UNITED STATES GOVERNMENT PRINTING OFFICE (GPO)

REQUIREMENTS DOCUMENT
(RD V3.0)

FOR THE

FUTURE DIGITAL SYSTEM (FDsys)

FINAL

October 18, 2006

FINAL

Document Change/Configuration Control Sheet

Document Title: FDsys Requirements Document (RD 3.0)

Date	Filename / version #	Author	Revision Description
10/16/2006	FDsys RD v3.0	PMO	System Requirements Document (RD 3.0), following System Requirements Review for release 1B
10/17/2006	FDsys RD v3.0	Zwaard	Added page numbers and text about deleted requirements.

Table of Contents

1.0 Introduction

This Requirements Document (RD V3.0) defines the requirements for the Future Digital System (FDsys) and is intended to communicate those requirements to the technical community who will build the system. These requirements are consistent with the U.S. Government Printing Office's (GPO) intent to implement FDsys in a series of incremental releases.

1.1 System Purpose

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

1.2 System Scope

FDsys is unparalleled in scope. Included in the FDsys will be all known Federal Government documents within the scope of GPO's Federal Depository Library Program (FDLP). This content will be entered into the system and then authenticated and catalogued according to GPO metadata and document creation standards. Content may include text and associated graphics, video, audio, and other forms of content that emerge. Content will be available for Web searching and Internet viewing, downloading and printing, and as document masters for conventional printing, on-demand printing, and other dissemination methods.

1.3 System Releases

Standing up FDsys is a complex system integration task, which will be rolled out in a series of releases. Each release includes improvements to both system capability and underlying infrastructure, and is built incrementally on those preceding it until the full range of capabilities is implemented.

2.0 Requirements

The requirements listed in this section are the result of a thorough analysis of the ideas proposed in the *Future Digital System ConOps* and revisions to *Requirements Document 2.1* as a result of the Systems Requirements Review for release 1B. This RD should be reviewed together with the *ConOps* Section 5.3: Description of Proposed System and *RD 2.1* for a complete understanding of the proposed system.

There are several levels of system requirements in each major system capability. Each subsection is hierarchical in nature; these relationships are reflected in the ID codes.

Several requirements in this list are marked "deleted." This is used to show that a requirement from *RD 2.1* has been removed because it was a duplicate of another requirement.

Each requirement is identified by the release in which we anticipate its implementation (Release 1B, 1C, 2, and 3) and its criticality to the system.

- Must: The system cannot adequately function without meeting this requirement. This requirement must be implemented in the release listed.
- Should: Functionality system users will expect. These requirements are desirable features that will be implemented in the release listed, whenever possible.
- Could: Additional functionality that is not critical to the system function or user experience.

2.1 Requirements List

Identification	Requirement	Release/ Criticality
3.2.1.2	**Requirements for System, General**	
3.2.1.2.1	The system shall provide for the use of internal and external open interfaces.	Release 1B; Must
3.2.1.2.1.1	The system may provide for the use of proprietary interfaces only when open interfaces are not available or do not meet system requirements.	Release 1B; Must
3.2.1.2.2	The system shall provide an architecture that allows preservation of content independent of any specific hardware and software that was used to produce them.	Release 1B; Must
3.2.1.2.3	The system shall use plug-in components that can be replaced with minimal impact to remaining components as workload and technology change.	Release 2; Must
3.2.1.2.4	The system shall accommodate changes in technologies and policies without requiring major re-engineering or design changes.	Release 1C; Must
3.2.1.2.4.1	The system shall support multiple user roles.	Release 1C; Must
3.2.1.2.4.2	The system shall support the assignment of one or more roles to a user.	Release 1C; Must

3.2.1.2.4.3	The system shall support the management of the functions permitted by a user role.	Release 1C; Must
3.2.1.2.4.4	The system shall prevent a user from performing a function unless the user possesses a user role permitting that function.	Release 1C; Must
3.2.1.2.4.5	The system shall support the capability to change key parameters affecting the operation of the system without redesigning the system.	Release 1C; Must
3.2.1.2.4.6	The system shall support the capability to accommodate changes in hardware technologies without requiring major reengineering or design changes.	Release 1C; Must
3.2.1.2.4.7	The system shall support the capability to accommodate changes in software technologies without requiring major reengineering or design changes.	Release 1C; Must
3.2.1.2.4.8	The system shall support the capability to accommodate changes in processes without requiring major reengineering or design changes.	Release 1C; Must
3.2.1.2.4.9	The system shall support the capability to accommodate changes in policies without requiring major reengineering or design changes.	Release 1C; Must
3.2.1.2.4.10	The system shall support the capability to accommodate changes in personnel without requiring major reengineering or design changes.	Release 1C; Must
3.2.1.2.4.11	The system shall support the capability to accommodate changes in system locations without requiring major reengineering or design changes.	Release 1C; Must
3.2.1.2.5	The system shall provide the capability to scale to 50 petabytes (TBR) of storage without requiring redesigning the system.	Release 1C; Must
3.2.1.2.6	The system shall have the ability to handle additional kinds of content over time, not limited to specific types that exist today.	Release 1B; Must
3.2.1.2.6.1	The system shall provide the ability to ingest content independently of its digital format.	Release 1B; Must
3.2.1.2.6.2	The system shall provide the ability to store content independently of its digital format.	Release 1B; Must
3.2.1.2.6.3	The system shall provide the ability to deliver content independently of its digital format.	Release 1B; Must
3.2.1.2.7	The system shall provide support for content management lifecycle processes for harvested, converted and deposited content.	Release 2; Must
3.2.1.2.8	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.	Release 2; Must
3.2.1.2.8.1	The system shall enable GPO to tailor content-based services to suit its customers' needs.	Release 3; Must
3.2.1.2.8.2	The system shall enable GPO to tailor content-based services to implement progressive improvements in business process.	Release 3; Must

3.2.1.2.9	The system shall assemble content and metadata files into content packages that are compliant with open standards.	Release 1B; Must
3.2.1.2.9.1	The system shall provide the capability for a content package to contain one binding file.	Release 1B; Must
3.2.1.2.9.2	The binding file of the content package shall be expressed in XML.	Release 1B; Must
3.2.1.2.9.3	The binding file of the content package shall contain an inventory of all the content files in the package.	Release 1B; Must
3.2.1.2.9.4	The binding file of the content package shall contain an inventory of all the metadata files in the package.	Release 1B; Must
3.2.1.2.9.5	The binding file of the content package shall contain the relationships between the content files and metadata files in the package.	Release 1B; Must
3.2.1.2.9.6	The system shall provide the capability for one or more metadata files to be related to each content file in a content package.	Release 1B; Must
3.2.1.2.9.7	The system shall provide the capability for each metadata file to be related to one or more content files in a content package.	Release 1B; Must
3.2.1.2.9.8	The system shall support the capability to transform the binding file of the content package into other formats.	Release 3; Must
3.2.1.2.10	The system shall be available for use at all GPO locations.	Release 1C; Must
3.2.1.2.12.10.1	The system is considered available when all critical system functions are operational.	Release 1C; Must
3.2.1.2.11	The system shall provide the capability to maintain required response times when there are 20,000 (TBR) concurrent users performing a mix of operations that represents peak time operational use.	Release 1C; Must
3.2.1.2.12	The system shall support an average peak time availability of 99.7%.	Release 1C; Must
3.2.1.2.12.1	Deleted.	
3.2.1.2.12.2	Deleted.	
3.2.1.2.13	The system shall provide a response to the user within 2 seconds of a user on the GPO intranet initiating an operation.	Release 1C; Must

3.2.2.2	**Requirements for Content Metadata**	
3.2.2.2.1	**Content Metadata Core Capabilities**	
3.2.2.2.1.1	The system shall have a central functionality which collects, edits, and shares content metadata among the broad functions of the system.	Release 1B; Must
3.2.2.2.1.1.1	The system shall allow authorized users to edit content metadata residing within a SIP.	Release 1B; Must
3.2.2.2.1.1.2	The system shall allow authorized users to edit content metadata residing within an AIP.	Release 1B; Must

3.2.2.2.1.1.3	The system shall allow authorized users to edit content metadata residing within an ACP.	Release 1B; Must
3.2.2.2.1.1.4	The system shall allow authorized users to edit content metadata residing within WIP.	Release 1B; Must
3.2.2.2.1.2	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.	Release 1B; Must
3.2.2.2.1.3	The system shall provide mechanisms to share content metadata and provide linkages and interoperability between extension schema and input standards.	Release 1B; Must
3.2.2.2.1.4	The Application Programmer Interfaces of the system shall be based on open standards	Release 1B; Must
3.2.2.2.1.5	The system shall provide the capability to link content metadata with system metadata.	Release 1B; Must
3.2.2.2.1.6	The system shall provide the capability to link content metadata with business process information.	Release 1B; Must

3.2.2.2.2	**Content Metadata Types**	
3.2.2.2.2.1	The system shall employ metadata which relates descriptive information related to a target digital object(s) and its associated content package.	Release 1B; Must
3.2.2.2.2.1.1	All metadata files shall be encoded in XML and conform to schema that are adopted by FDsys.	Release 1B; Must
3.2.2.2.2.2	The system shall employ metadata which relates representation information related to a target digital object(s) and its associated content package.	Release 1B; Must
3.2.2.2.2.3	The system shall employ metadata which relates administrative information related to a target digital object(s) and its associated content package.	Release 1B; Must
3.2.2.2.2.3.1	The system shall employ metadata which relates technical information related to a target digital object(s) and its associated content package.	Release 1B; Must
3.2.2.2.2.3.2	The system shall employ metadata which relates the structure of a target digital object(s) and its associated content package.	Release 1B; Must
3.2.2.2.2.3.2.1	The system shall employ publication-specific metadata (e.g., Federal Register, Code of Federal Regulations, United States Code, U.S. Reports).	Release 1C; Must
3.2.2.2.2.3.2.2	The system shall employ document-specific metadata (e.g., Congressional Bills, Congressional Reports, Congressional Documents, proposed rules, business cards, envelopes, agency strategic plans)	Release 1C; Must
3.2.2.2.2.3.3	The system shall employ metadata which relates the rights information of a target digital object(s) and its associated content package.	Release 1C; Must
3.2.2.2.2.3.4	The system shall employ metadata which relates the source information of a target digital object(s) and its associated content package.	Release 1B; Must

3.2.2.2.2.3.5	The system shall employ metadata which relates the provenance information of a target digital object(s) and its associated content package.	Release 1B; Must
3.2.2.2.2.4	The system shall employ metadata which relates the Preservation Description Information (PDI) of a target digital object(s) and its associated content package.	Release 1B; Must
3.2.2.2.2.5	The system shall employ metadata which relates the context of a digital object and relationship to other objects.	Release 1B; Must
3.2.2.2.2.6	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.	Release 1B; Must
3.2.2.2.2.7	The system shall employ metadata which describes and provides reference information about the digital object and its associated content package.	Release 1B; Must
3.2.2.2.2.8	The system shall employ metadata which relates packaging information related to a target digital object(s) and its associated content package.	Release 1B; Must

3.2.2.2.3	**Content Metadata Schema**	
3.2.2.2.3.1	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.	Release 1B; Must
3.2.2.2.3.2	In general, GPO shall refer to metadata schema rather than embed data elements in the METS wrapper.	Release 1B; Must
3.2.2.2.3.4	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible.	Release 2; Must
3.2.2.2.3.4.0.1	The system shall support the capability to employ additional established extension schema for expressing metadata in the future.	Release 2; Must
3.2.2.2.3.4.0.2	The system shall support the capability to translate metadata conforming to registered input standards to an XML representation for storage in the system.	Release 2; Must
3.2.2.2.3.4.0.3	The system shall have the capability to employ Dublin Core version 1.1 as an extension schema.	Release 1B; Must
3.2.2.2.3.4.0.4	The system shall have the capability to employ PREMIS version 1.0 as an extension schema.	Release 1B; Must
3.2.2.2.3.4.1	The system shall have the capability to employ Machine Readable Cataloging (MARC) as an input standard.	Release 1B; Must
3.2.2.2.3.4.2	The system shall have the capability to employ Metadata Object Description Schema (MODS) version 3.2 as an extension schema.	Release 1B; Must
3.2.2.2.3.4.3	The system shall support the capability to employ additional input standards for expressing metadata in the future.	Release 2; Must
3.2.2.2.3.4.4	The system shall have the capability to employ Encoded Archival Description (EAD) version 2002 as an extension DTD.	Release 2; Could

3.2.2.2.3.4.5	The system shall have the capability to employ Text Encoding Initiative (TEI) TEI P4 DTD as an extension DTD.	Release 2; Could
3.2.2.2.3.4.6	The system shall have the capability to employ Data Document Initiative (DDI) version 2.1 as an extension DTD.	Release 2; Could
3.2.2.2.3.4.7	The system shall have the capability to employ Federal Geographic Data Committee (FGDC) CSDGM Document Type Declaration as an extension DTD.	Release 2; Could
3.2.2.2.3.4.8	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including Premis.	Release 1C; Must
3.2.2.2.3.4.9	The system shall have the capability to employ MPEG 21 as an input standard.	Release 2; Should
3.2.2.2.3.4.10	The system shall have the capability to employ JPEG 2000 as an input standard.	Release 2; Should
3.2.2.2.3.4.11	The system shall have the capability to employ ONIX as an extension schema.	Release 2; Must
3.2.2.2.3.4.12	The system shall have the capability to employ MIX (NISO Metadata for Images) as an extension schema.	Release 1C; Must
3.2.2.2.3.5	The system shall employ a registry of extension schema and input standards in use.	Release 1C; Must
3.2.2.2.3.6	Authorized users shall have the capability to manage the registry of schema employed by the system.	Release 1C; Must
3.2.2.2.3.6.1	The system shall provide the capability for users to add new XML schemas to the Schema Registry,	Release 1C; Must
3.2.2.2.3.6.2	The system shall provide the capability for users to remove XML schemas from the Schema Registry,	Release 1C; Must
3.2.2.2.3.6.3	The system shall provide the capability for users to update XML schemas in the Schema Registry,	Release 1C; Must
3.2.2.2.3.6.4	The system shall allow users to add new XML DTDs to the Schema Registry,	Release 1C; Must
3.2.2.2.3.6.5	The system shall provide the capability for users to remove XML DTDs from the Schema Registry,	Release 1C; Must
3.2.2.2.3.6.6	The system shall provide the capability for users to update XML DTDs in the Schema Registry,	Release 1C; Must
3.2.2.2.3.7	Deleted.	
3.2.2.2.3.8	Deleted.	
3.2.2.2.3.8.1	The schema shall interact with METS.	Release 1C; Must
3.2.2.2.3.8.2	The schema shall map to specific function(s), content type, or content formats within the system.	Release 1C; Must
3.2.2.2.3.8.2.1	The schema shall map to specific function(s).	Release 1C; Must
3.2.2.2.3.8.2.2	The schema shall map to content type(s).	Release 1C; Must
3.2.2.2.3.8.2.3	The schema shall map to content format(s).	Release 1C; Must
3.2.2.2.3.8.3	Deleted.	
3.2.2.2.3.8.4	The schema shall not conflict with other schema in use by the system.	Release 1C; Must

3.2.2.2.3.9	The system shall provide the capability to add extension schema developed by GPO to the Schema Registry.	Release 1C; Must
3.2.2.2.3.10	Specific schema that will be used in each case shall be based on the specific needs of the target digital object(s) or content package [e.g., content type (text, audio, video, multi-type), metadata type (descriptive, technical, structural)].	Release 1C; Must

3.2.2.2.4	**Content Metadata Import and Export**	
3.2.2.2.4.1	The system shall have the capability to receive and record existing metadata from sources external to the system.	Release 3; Must
3.2.2.2.4.1.1	The system shall have the capability to receive existing MARC metadata from sources external to the system."	Release 2; Must
3.2.2.2.4.1.2	The system shall have the capability to record existing MARC metadata from sources external to the system."	Release 2; Must
3.2.2.2.4.1.3	The system shall have the capability to receive existing COSATI metadata from sources external to the system."	Release 3; Must
3.2.2.2.4.1.4	The system shall have the capability to record existing COSATI metadata from sources external to the system."	Release 3; Must
3.2.2.2.4.2	The system shall provide the capability to export metadata in the form of a DIP.	Release 1C; Must
3.2.2.2.4.2.1	The system shall provide the capability to export metadata from a single publication.	Release 1C; Must
3.2.2.2.4.2.1.1	The system shall provide the capability to export content along with metadata from a single publication.	Release 1C; Must
3.2.2.2.4.2.1.2	The system shall provide the capability to export metadata from one or more renditions of a single publication.	Release 1C; Must
3.2.2.2.4.2.1.3	The system shall provide the capability to export one or more metadata files from a single publication."	Release 1C; Must
3.2.2.2.4.2.2	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.	Release 1C; Must
3.2.2.2.4.2.2.1	The system shall provide the capability to export content along with metadata from multiple publications.	Release 1C; Must
3.2.2.2.4.2.2.2	The system shall provide the capability to export metadata from one or more renditions of multiple publications."	Release 1C; Must
3.2.2.2.4.2.2.3	The system shall provide the capability to export one or more metadata files from multiple publications."	Release 1C; Must
3.2.2.2.4.3	The system shall provide the capability to transform metadata from one standard to another prior to exporting it.	Release 2; Must

3.2.2.2.5	**Content Metadata Management**	
3.2.2.2.5.1	The system shall have the ability to manage metadata regardless of its source.	Release 1B; Must
3.2.2.2.5.2	The system shall have the ability to create metadata meeting the requirements of one or more schema.	Release 2; Must
3.2.2.2.5.2.1	The system shall provide the capability for an authorized user to enter metadata.	Release 1B; Must
3.2.2.2.5.2.2	The system shall provide the capability to transform metadata from one standard to another.	Release 2; Must
3.2.2.2.5.2.3	The system shall provide the capability to extract metadata from content.	Release 2; Must
3.2.2.2.5.3	The system shall provide the capability for GPO to designate metadata elements as mandatory.	Release 1B; Must
3.2.2.2.5.4	The system shall have the capability to automatically record in system metadata information about the actions performed by the system on content.	Release 1B; Must
3.2.2.2.5.5	The system shall have the capability to automatically record in BPI information about the actions performed by business processes on content.	Release 1B; Must
3.2.2.2.5.6	The system shall log all additions, deletions, and changes to content metadata within the system.	Release 1B; Must

3.2.3.1.2	**Requirements for SIP**	
3.2.3.1.2.1	**SIP - Deposited Content**	
3.2.3.1.2.1.1	The SIP for Deposited Content shall contain one or more renditions of the publication being submitted in the SIP.	Release 1B; Must
3.2.3.1.2.1.2	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.	Release 1B; Must

3.2.3.1.2.2	**SIP - Harvested Content**	
3.2.3.1.2.2.1	The SIP for Harvested Content shall contain zero or more rendition consisting of the original harvested digital objects.	Release 1B; Must
3.2.3.1.2.2.2	The metadata for harvested content in the SIP shall consist of representation information, documentation of harvest & transformation(s), submission level metadata for each rendition.	Release 2; Must
3.2.3.1.2.2.2.1	The metadata for harvested content in the SIP shall include information about the harvest process.	Release 2; Must

3.2.3.1.2.3	**SIP - Converted Content**	
3.2.3.1.2.3.1	The SIP for Converted Content shall contain, at a minimum, a rendition consisting of the digital object(s) as produced by the conversion process.	Release 1B; Must

3.2.3.1.2.3.2	The SIP for converted Content shall support the inclusion of representation information and metadata describing the conversion process for each rendition.	Release 1B; Must
3.2.3.1.2.3.2.1	The metadata for converted content in the SIP shall include full technical information on the conversion, as specified by NISO Z 39.87-2002.	Release 1B; Must

3.2.3.1.2.4	**Core SIP Requirements**	
3.2.3.1.2.4.1	A SIP shall contain one or more renditions of one publication.	Release 1B; Must
3.2.3.1.2.4.1.1	A SIP that describes a publication which only exists in tangible form shall contain a surrogate digital object that describes its tangible expression.	Release 1B; Must
3.2.3.1.2.4.1.2	A SIP shall have the capability to contain metadata indicating if the publication it contains is in scope for GPO's dissemination programs.	Release 1B; Must
3.2.3.1.2.4.1.3	Each rendition of a publication in a SIP shall be contained in its own subdirectory of the content directory.	Release 1B; Must
3.2.3.1.2.4.1.4	A rendition of a publication in a SIP shall contain one or more digital objects.	Release 1B; Must
3.2.3.1.2.4.1.5	A rendition of a publication in a SIP shall contain one or more subdirectories.	Release 1B; Must
3.2.3.1.2.4.1.6	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.	Release 1B; Must
3.2.3.1.2.4.1.7	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.	Release 1B; Must
3.2.3.1.2.4.1.8	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is in a screen optimized format.	Release 1B; Must
3.2.3.1.2.4.1.9	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is in a print optimized format.	Release 1B; Must
3.2.3.1.2.4.1.10	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is in a press optimized format.	Release 1B; Must
3.2.3.1.2.4.1.11	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is a complete representation of the publication.	Release 1B; Must
3.2.3.1.2.4.1.12	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.	Release 1B; Must
3.2.3.1.2.4.2	A SIP shall contain a METS file named sip.xml.	Release 1B; Must
3.2.3.1.2.4.2.1	The sip.xml file shall contain an inventory of all the content files in a SIP.	Release 1B; Must

3.2.3.1.2.4.2.2	The sip.xml file shall contain an inventory of all the metadata files in a SIP.	Release 1B; Must
3.2.3.1.2.4.2.3	The sip.xml file shall contain the relationships between the content files and metadata files in a SIP.	Release 1B; Must
3.2.3.1.2.4.2.4	The system shall provide the capability for one or more metadata files to be related to each content file in a SIP.	Release 1B; Must
3.2.3.1.2.4.2.5	The system shall provide the capability for each metadata file to be related to one or more content files in a SIP.	Release 1B; Must
3.2.3.1.2.4.3	A SIP shall contain one or more metadata files associated with the content.	Release 1B; Must
3.2.3.1.2.4.3.1	The system shall provide the capability to store an XML schema that describes the format of a content file in a SIP.	Release 1B; Must
3.2.3.1.2.4.3.2	The system shall provide the capability to store an XML DTD that describes the format of a content file in a SIP.	Release 1B; Must
3.2.3.1.2.4.4	Metadata files in a SIP shall be encoded in XML.	Release 1B; Must
3.2.3.1.2.4.4.1	Metadata files in a SIP shall conform to an XML Schema or XML DTD that is registered in the FDsys Metadata Schema Registry.	Release 1C; Must
3.2.3.1.2.4.5	The SIP specified in this document shall apply to all content types specified and accepted by FDsys: converted, deposited and harvested.	Release 2; Must
3.2.3.1.2.4.5.1	The SIP requirements shall apply to deposited content.	Release 1B; Must
3.2.3.1.2.4.5.2	The SIP requirements shall apply to converted content.	Release 1C; Must
3.2.3.1.2.4.5.3	The SIP requirements shall apply to harvested content.	Release 1C; Must

3.2.3.1.2.5	**Requirements for sip.xml File**	
3.2.3.1.2.5.1	The sip.xml file shall conform to the METS version 1.5.	Release 1B; Must
3.2.3.1.2.5.2	The sip.xml file shall conform to the GPO METS Profile version 1.0.	Release 1B; Must
3.2.3.1.2.5.3	Digital objects in the SIP shall be stored outside the sip.xml file.	Release 1B; Must
3.2.3.1.2.5.3.1	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.	Release 1B; Must
3.2.3.1.2.5.4	Metadata files in the SIP shall be stored outside the sip.xml file.	Release 1B; Must
3.2.3.1.2.5.4.1	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.	Release 1B; Must
3.2.3.1.2.5.5	Deleted.	

3.2.3.1.2.6	**Structural Layout for SIPs**	
3.2.3.1.2.6.1	The SIP shall contain the sip.xml at the top level of the SIP directory structure.	Release 1B; Must
3.2.3.1.2.6.1.1	The SIP shall contain a directory named content at the top level of the SIP directory structure.	Release 1B; Must
3.2.3.1.2.6.1.2	The SIP shall contain a directory named metadata at the top level of the SIP directory structure.	Release 1B; Must
3.2.3.1.2.6.2	The content files for each rendition of a publication in a SIP shall be placed in its own subdirectory under the content directory.	Release 1B; Must
3.2.3.1.2.6.2.0.1	The folder structure of the digital objects in a rendition folder shall be recorded in the sip.xml file.	Release 1B; Must
3.2.3.1.2.6.2.1	Deleted.	
3.2.3.1.2.6.3	All metadata files shall be placed in the metadata directory.	Release 1B; Must
3.2.3.1.2.6.3.1	The metadata files for each rendition of a publication in a SIP shall be placed in its own subdirectory under the metadata directory.	Release 1B; Must
3.2.3.1.2.6.3.1.1	The metadata subdirectory for a rendition shall have the same name as the content subdirectory for that rendition.	Release 1B; Must
3.2.3.1.2.6.4	A SIP shall contain a least one metadata file containing descriptive metadata for the publication that shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.6.4.1	The mandatory descriptive metadata file for a publication shall be stored in MODS format.	Release 1B; Must
3.2.3.1.2.6.4.2	The mandatory descriptive metadata file for a publication shall be located in the top level directory.	Release 1B; Must
3.2.3.1.2.6.5	Each rendition of a publication shall have one or more metadata files that include administrative metadata about the rendition.	Release 1B; Must
3.2.3.1.2.6.5.1	Each content file in a rendition shall have, at a minimum, a metadata file specifying the file format of the content file.	Release 1B; Must

3.2.3.1.2.7	**Packaging of SIPs**	
3.2.3.1.2.7.1	The system shall provide the capability to aggregate all the files and directories in a SIP into a single package.	Release 1B; Must
3.2.3.1.2.7.1.1	The system shall provide the capability to aggregate the SIP into a ZIP file.	Release 1C; Must
3.2.3.1.2.7.1.2	The system shall provide the capability to ingest into FDsys a SIP that is aggregated in a ZIP file.	Release 1C; Must
3.2.3.1.2.7.1.3	The system shall support the capability to aggregate the SIP into additional file formats in the future.	Release 3; Must
3.2.3.1.2.7.1.4	The system shall support the capability to ingest into FDsys a SIP that is aggregated in additional file formats in the future.	Release 3; Must

3.2.3.1.2.8	**SIP Descriptive Metadata Requirements**	
3.2.3.1.2.8.0.1	The system shall have the capability to store descriptive metadata in multiple extension schema and records in the SIP.	Release 1B; Must
3.2.3.1.2.8.0.1.1	The system shall have the capability to store descriptive metadata in ONIX format in the SIP.	Release 2; Must
3.2.3.1.2.8.0.1.2	The system shall have the capability to store descriptive metadata in Dublin Core format in the SIP.	Release 1B; Must
3.2.3.1.2.8.0.1.3	The system shall have the capability to store descriptive metadata in PREMIS format in the SIP.	Release 1B; Must
3.2.3.1.2.8.0.1.4	The system shall have the capability to store descriptive metadata in COSATI format in the SIP.	Release 3; Must
3.2.3.1.2.8.0.1.5	The system shall have the capability to store descriptive metadata in additional descriptive metadata formats in the future in the SIP.	Release 3; Must
3.2.3.1.2.8.1	The system shall employ descriptive metadata elements in the SIP in MODS version 3.1 format.	Release 1B; Must
3.2.3.1.2.8.2	The system shall allow all MODS elements to be stored in the MODS file in the SIP.	Release 1B; Must
3.2.3.1.2.8.2.1	The system shall allow all MODS sub-elements to be stored in the MODS file in the SIP.	Release 1B; Must
3.2.3.1.2.8.3	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.	Release 1B; Must
3.2.3.1.2.8.3.1	The OriginInfo:publisher MODS descriptive metadata element shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.2	The OriginInfo:dateIssued, Captured, Created, Modified, Valid, or Other MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.3	The Language MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.4	The Identifier MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.5	The Location MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.6	The PhysicalDescription:internetMediaType MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.7	The PhysicalDescription:digitalOrigin MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.8	The PhysicalDescription:extent MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.9	The TypeOfResource MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must
3.2.3.1.2.8.3.10	The RecordInfo MODS descriptive metadata elements shall be considered mandatory.	Release 1B; Must

3.2.3.1.2.9	**SIP Administrative Metadata Requirements**	

3.2.3.1.2.9.1	The system shall support the capability for the SIP to contain administrative metadata that conform to a METS extension schema.	Release 1B; Must
3.2.3.1.2.9.1.1	The SIP shall identify the extension schema to which each administrative metadata file conforms.	Release 1B; Must
3.2.3.1.2.9.1.2	The METS extension schema identified for an administrative metadata file in the SIP must be registered in the Metadata Registry.	Release 1B; Must
3.2.3.1.2.9.1.3	The system shall verify that each administrative metadata file in the SIP conforms to its identified METS extension schema.	Release 1B; Must
3.2.3.1.2.9.1.4	The system shall have the capability to include technical metadata about each rendition in the SIP.	Release 1B; Must
3.2.3.1.2.9.1.5	The system shall have the capability to include source metadata about each rendition in the SIP.	Release 1B; Must
3.2.3.1.2.9.1.6	The system shall have the capability to include rights metadata about each rendition in the SIP.	Release 1B; Must
3.2.3.1.2.9.1.7	The system shall have the capability to include provenance metadata about each rendition in the SIP.	Release 1B; Must
3.2.3.1.2.9.1.8	The system shall have the capability to include system metadata about each rendition in the SIP.	Release 1B; Must

3.2.3.2.2	**Requirements for AIP**	
3.2.3.2.2.1	**AIP Core Capabilities**	
3.2.3.2.2.1.1	An AIP shall contain one or more renditions of one publication.	Release 1B; Must
3.2.3.2.2.1.1.1	An AIP shall only be created for SIPs that contain a publication that is in scope for GPO's dissemination programs.	Release 2; Must
3.2.3.2.2.1.1.2	The AIP shall provide the capability to contain a rendition of the publication in the format in which it was created.	Release 1B; Must
3.2.3.2.2.1.1.3	The system shall provide the capability for authorized users to add renditions of a publication to an AIP.	Release 1B; Must
3.2.3.2.2.1.2	The AIP shall provide the capability to include more than one rendition of a publication.	Release 1B; Must
3.2.3.2.2.1.2.1	Each rendition of a publication in an AIP shall be contained in its own subdirectory of the content directory.	Release 1B; Must
3.2.3.2.2.1.2.2	A rendition of a publication in an AIP shall contain one or more files.	Release 1B; Must
3.2.3.2.2.1.2.3	A rendition of a publication in an AIP shall contain one or more subdirectories.	Release 1B; Must
3.2.3.2.2.1.2.4	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.	Release 1B; Must
3.2.3.2.2.1.2.5	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.	Release 1B; Must

3.2.3.2.2.1.2.6	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is in a screen optimized format.	Release 1B; Must
3.2.3.2.2.1.2.7	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is in a print optimized format.	Release 1B; Must
3.2.3.2.2.1.2.8	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is in a press optimized format.	Release 1B; Must
3.2.3.2.2.1.2.9	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is a complete representation of the publication.	Release 1B; Must
3.2.3.2.2.1.2.10	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.	Release 1B; Must
3.2.3.2.2.1.3	The AIP shall contain Representation Information metadata for every rendition of the publication in the AIP.	Release 1B; Must
3.2.3.2.2.1.4	The system shall support the creation of AIPs which are independent of any particular hardware and software component.	Release 1B; Must
3.2.3.2.2.1.4.1	The system shall provide the capability to add content to an AIP independent of the content's digital format.	Release 1B; Must
3.2.3.2.2.1.4.2	The system shall provide the capability to store content in an AIP independent of the content's digital format.	Release 1B; Must
3.2.3.2.2.1.4.3	The system shall provide the capability to deliver content stored in an AIP regardless of the content's digital format.	Release 1B; Must
3.2.3.2.2.1.5	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.	Release 1B; Must
3.2.3.2.2.1.5.1	The system shall provide the capability for authorized users to access AIPs for the purpose of executing preservation processes on AIPs.	Release 1B; Must
3.2.3.2.2.1.5.2	The system shall provide the capability for authorized users to access AIPs for the purpose of disseminating DIPs from AIPs.	Release 1B; Must
3.2.3.2.2.1.6	Deleted.	
3.2.3.2.2.1.7	An AIP shall contain a METS file named aip.xml.	Release 1B; Must
3.2.3.2.2.1.7.1	The aip.xml file shall contain an inventory of all the content files in an AIP.	Release 1B; Must
3.2.3.2.2.1.7.2	The aip.xml file shall contain an inventory of all the metadata files in an AIP.	Release 1B; Must
3.2.3.2.2.1.7.3	The aip.xml file shall contain the relationships between the content files and metadata files in an AIP.	Release 1B; Must

3.2.3.2.2.1.7.4	The system shall provide the capability for one or more metadata files to be related to each content file in an AIP.	Release 1B; Must
3.2.3.2.2.1.7.5	The system shall provide the capability for each metadata file to be related to one or more content files in an AIP.	Release 1B; Must
3.2.3.2.2.1.8	The AIP shall contain one or more metadata files associated with the content.	Release 1B; Must
3.2.3.2.2.1.8.1	The system shall provide the capability to store an XML schema that describes the format of a content file in an AIP.	Release 1B; Must
3.2.3.2.2.1.8.2	The system shall provide the capability to store an XML DTD that describes the format of a content file in an AIP.	Release 1B; Must

3.2.3.2.2.2	**Requirements for aip.xml File**	
3.2.3.2.2.2.1	The aip.xml file shall conform to the METS version 1.5.	Release 1B; Must
3.2.3.2.2.2.2	The aip.xml file shall conform to the GPO METS Profile version 1.0.	Release 1B; Must
3.2.3.2.2.2.3	Digital objects in the AIP shall be stored outside the aip.xml file.	Release 1B; Must
3.2.3.2.2.2.3.1	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.	Release 1B; Must
3.2.3.2.2.2.4	Metadata files in the AIP shall be stored outside the aip.xml file.	Release 1B; Must
3.2.3.2.2.2.4.1	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.	Release 1B; Must
3.2.3.2.2.2.5	A metadata file must be associated with one or more digital objects inside the aip.xml file.	Release 1B; Must

3.2.3.2.2.3	**Structural Layout for AIPs**	
3.2.3.2.2.3.1	The AIP shall contain the aip.xml at the top level of the AIP directory structure.	Release 1B; Must
3.2.3.2.2.3.1.1	The SIP shall contain a directory named content at the top level of the AIP directory structure.	Release 1B; Must
3.2.3.2.2.3.1.2	The AIP shall contain a directory named metadata at the top level of the AIP directory structure.	Release 1B; Must
3.2.3.2.2.3.2	The content files for each rendition of a publication in an AIP shall be placed in its own subdirectory under the content directory.	Release 1B; Must
3.2.3.2.2.3.2.0.1	The hierarchical structure of the digital objects in a rendition folder shall be recorded in the aip.xml file.	Release 1B; Must
3.2.3.2.2.3.2.1	Deleted.	
3.2.3.2.2.3.3	All metadata files shall be placed in the metadata directory.	Release 1B; Must

3.2.3.2.2.3.3.1	The metadata files for each rendition of a publication in an AIP shall be placed in its own subdirectory under the metadata directory.	Release 1B; Must
3.2.3.2.2.3.3.1.1	The metadata subdirectory for a rendition shall have the same name as the content subdirectory for that rendition.	Release 1B; Must
3.2.3.2.2.3.4	Each content file in a rendition shall have, at a minimum, a metadata file specifying technical parameters of the content file.	Release 1B; Must

3.2.3.2.2.4	**AIP Metadata**	
3.2.3.2.2.4.1	Metadata files in a SIP shall be encoded in XML.	Release 1B; Must
3.2.3.2.2.4.1.0.1	Metadata files in an AIP shall conform to an XML Schema or XML DTD that is registered in the FDsys Metadata Schema Registry.	Release 1C; Must
3.2.3.2.2.4.3	The AIP shall include preservation metadata to record preservation processes, from ingest into the repository through disposal.	Release 1C; Must
3.2.3.2.2.4.4	The system shall store descriptive metadata elements in the AIP in MODS version 3.1 format.	Release 1B; Must
3.2.3.2.2.4.4.0.1	The system shall have the capability to store descriptive metadata in ONIX format in the AIP.	Release 2; Must
3.2.3.2.2.4.4.0.2	The system shall have the capability to store descriptive metadata in Dublin Core format in the AIP.	Release 1B; Must
3.2.3.2.2.4.4.0.3	The system shall have the capability to store descriptive metadata in PREMIS format in the AIP.	Release 1B; Must
3.2.3.2.2.4.4.0.4	The system shall have the capability to store descriptive metadata in COSATI format in the AIP.	Release 3; Must
3.2.3.2.2.4.4.0.5	The system shall have the capability to store descriptive metadata in MODS format in the AIP.	Release 1B; Must
3.2.3.2.2.4.4.0.6	The system shall have the capability to store descriptive metadata in additional descriptive metadata formats in the future in the AIP.	Release 3; Must
3.2.3.2.2.4.4.1	The AIP shall incorporate all descriptive metadata elements from the SIP.	Release 1B; Must
3.2.3.2.2.4.5	The AIP shall include metadata that expresses Preservation Description Information (PDI) according to the PREMIS Data Dictionary and extension schema which implement it.	Release 1C; Must
3.2.3.2.2.4.6	The system shall support the capability for the AIP to contain administrative metadata that conform to a METS extension schema.	Release 1B; Must
3.2.3.2.2.4.6.0.1	The AIP shall identify the METS extension schema to which each administrative metadata file conforms.	Release 1B; Must
3.2.3.2.2.4.6.0.2	The METS extension schema identified for an administrative metadata file in the AIP must be registered in the Metadata Registry.	Release 1B; Must
3.2.3.2.2.4.6.0.3	The system shall verify that each administrative metadata file in the AIP conforms to its identified METS extension schema.	Release 1B; Must

3.2.3.2.2.4.6.0.4	The AIP shall have the capability to include Preservation Description Information (PDI) about each rendition included in the AIP.	Release 1B; Must
3.2.3.2.2.4.6.0.5	The system shall have the capability to include technical metadata about each rendition in the AIP.	Release 1B; Must
3.2.3.2.2.4.6.0.6	The system shall have the capability to include source metadata about each rendition in the AIP.	Release 1C; Must
3.2.3.2.2.4.6.0.7	The system shall have the capability to include rights metadata about each rendition in the AIP.	Release 1B; Must
3.2.3.2.2.4.6.0.8	The system shall have the capability to include provenance metadata about each rendition in the AIP.	Release 1B; Must

3.2.3.2.2.5	**AIP Unique ID**	
3.2.3.2.2.5.1	The AIP shall include the unique identification number assigned to the content in the SIP.	Release 1B; Must

3.2.3.3.2	**Requirements for ACP**	
3.2.3.3.2.1	**ACP Core Capabilities**	
3.2.3.3.2.1.1	An ACP shall contain copies of one or more renditions of one publication.	Release 1C; Must
3.2.3.3.2.1.1.1	The system shall provide the capability for authorized users to add renditions of a publication to an ACP.	Release 1C; Must
3.2.3.3.2.1.1.2	The ACP shall have the capability to be retained in the system for period of time as is indicated in metadata.	Release 1C; Must
3.2.3.3.2.1.1.3	The system shall provide the user the capability to alter the length of time to retain an ACP in the system.	Release 2; Must
3.2.3.3.2.1.1.4	The system shall provide the capability for an authorized user to transform renditions of ACPs.	Release 2; Must
3.2.3.3.2.1.1.5	The system shall create an ACP from its corresponding AIP when the AIP is accessed at a rate more than a user configurable frequency.	Release 2; Must
3.2.3.3.2.1.2	The ACP shall have the capability to include the following:	Release 1C; Must
3.2.3.3.2.1.2.1	The ACP shall have the capability to include renditions of publications that are not in scope of GPO's dissemination programs.	Release 1C; Must
3.2.3.3.2.1.2.2	The ACP shall have the capability to include renditions derived from AIP renditions.	Release 1C; Must
3.2.3.3.2.1.2.3	The system shall create one or more access derivative renditions for an ACP if its corresponding AIP has no access derivative renditions.	Release 2; Must
3.2.3.3.2.1.2.4	Deleted.	
3.2.3.3.2.1.3	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.	Release 1C; Must
3.2.3.3.2.1.4	The ACP shall have the capability to include all digital objects included in its corresponding AIP.	Release 1C; Must

3.2.3.3.2.1.5	The ACP shall contain a copy of the metadata files for each rendition which was copied from its corresponding AIP.	Release 1C; Must
3.2.3.3.2.1.6	The access time for an ACP shall be as less than or equal to the access time for its corresponding AIP.	Release 1C; Must
3.2.3.3.2.1.7	The ACP shall have the capability to replicate the structural layout of an AIP.	Release 1C; Could
3.2.3.3.2.1.8	Deleted.	
3.2.3.3.2.1.9	Deleted.	
3.2.3.3.2.1.10	The ACP shall have the capability to be linked to one AIP, known as its corresponding AIP.	Release 1C; Must
3.2.3.3.2.1.11	The ACP shall have the capability to include copies of one or more renditions from its corresponding AIP.	Release 1C; Must
3.2.3.3.2.1.11.1	The ACP shall include copies of renditions from its corresponding AIP based on business rules.	Release 1C; Must
3.2.3.3.2.1.11.2	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are screen optimized renditions.	Release 1C; Must
3.2.3.3.2.1.11.3	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are press optimized renditions.	Release 1C; Must
3.2.3.3.2.1.11.4	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are print optimized renditions.	Release 1C; Must

3.2.3.3.2.2	**ACP Binding Metadata File**	
3.2.3.3.2.2.1	An ACP shall have the capability to contain a METS file named acp.xml.	Release 1C; Must
3.2.3.3.2.2.1.1	The acp.xml file shall conform to the METS version 1.5.	Release 1C; Must
3.2.3.3.2.2.1.1.1	The acp.xml file shall conform to the GPO METS Profile version 1.0.	Release 1C; Must
3.2.3.3.2.2.1.2	Digital objects in the ACP shall be stored outside the acp.xml file.	Release 1C; Must
3.2.3.3.2.2.1.3	The system must provide the capability to include metadata files as required to support access and delivery	Release 1C; Must
3.2.3.3.2.2.1.4	The system shall provide the capability to associate metadata files with one or more digital objects in the ACP.	Release 1C; Must

3.2.3.3.2.3	**ACP Metadata**	
3.2.3.3.2.3.1	Metadata files in an ACP shall be encoded in XML.	Release 1C; Must
3.2.3.3.2.3.2	Deleted.	
3.2.3.3.2.3.3	The system shall provide the capability to add structural and descriptive metadata for digital objects at a level of granularity that facilitates access.	Release 1C; Must

3.2.3.3.2.3.4	Deleted.	
3.2.3.3.2.3.5	The system shall have the capability to use descriptive metadata extension schema to support access to publications.	Release 1C; Must
3.2.3.3.2.3.5.1	The system shall provide the capability to use descriptive metadata in MODS format to support access to publications.	Release 1B; Must
3.2.3.3.2.3.5.2	The system shall provide the capability to use descriptive metadata in ONIX format to support access to publications.	Release 2; Must
3.2.3.3.2.3.5.3	The system shall provide the capability to use descriptive metadata in Dublin Core format to support access to publications.	Release 1B; Must
3.2.3.3.2.3.5.4	The system shall provide the capability to use descriptive metadata in PREMIS format to support access to publications.	Release 1B; Must
3.2.3.3.2.3.5.5	The system shall provide the capability to use descriptive metadata in COSATI format to support access to publications.	Release 3; Must
3.2.3.3.2.3.5.6	The system shall support the capability to use additional descriptive metadata formats in the future to support access to publications.	Release 3; Must
3.2.3.3.2.3.6	The ACP shall have the capability to include mandatory descriptive metadata elements from the AIP and SIP.	Release 1C; Must
3.2.3.3.2.3.7	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.	Release 1C; Must
3.2.3.3.2.3.8	The ACP shall contain administrative metadata that conform to a METS extension schema	Release 1C; Must
3.2.3.3.2.3.8.1	The ACP shall identify the METS extension schema to which each administrative metadata file conforms.	Release 1C; Must
3.2.3.3.2.3.8.2	The METS extension schema identified for an administrative metadata file in the ACP shall be registered in the Metadata Registry.	Release 1C; Must
3.2.3.3.2.3.8.3	The system shall verify that each administrative metadata file in the ACP conforms to its identified METS extension schema.	Release 1C; Must
3.2.3.3.2.3.8.4	The system shall have the capability to include technical metadata about each rendition in the ACP.	Release 1C; Must
3.2.3.3.2.3.8.5	The system shall have the capability to include source metadata about each rendition in the ACP.	Release 1C; Must
3.2.3.3.2.3.8.6	The system shall have the capability to include rights metadata about each rendition in the ACP.	Release 1C; Must
3.2.3.3.2.3.8.7	The system shall have the capability to include provenance metadata about each rendition in the ACP.	Release 1C; Must
3.2.3.3.2.3.9	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.	Release 1C; Must

3.2.3.3.2.3.10	The ACP shall have the capability to include the unique ID assigned to the SIP and AIP in metadata.	Release 1C; Must

3.2.3.4.2	Requirements for DIP	
3.2.3.4.2.1	**DIP Core Capabilities**	
3.2.3.4.2.1.1	The system shall create a DIP in response to a user request for a publication.	Release 1B; Must
3.2.3.4.2.1.1.1	A DIP shall provide the capability to contain copies of one or more renditions of one publication.	Release 1B; Must
3.2.3.4.2.1.1.2	A DIP shall provide the capability to contain copies of the metadata about each rendition it contains.	Release 1B; Must
3.2.3.4.2.1.1.3	The system shall copy content and metadata to a DIP from the publication's ACP.	Release 1B; Must
3.2.3.4.2.1.1.4	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.	Release 1B; Must
3.2.3.4.2.1.1.5	The system shall provide the capability to generate screen optimized versions of renditions for inclusion in the DIP.	Release 1C; Must
3.2.3.4.2.1.1.6	A DIP created for a service provider shall have the capability to contain the order information for the publication.	Release 1C; Must
3.2.3.4.2.1.2	The DIP shall have the capability to include transient copies of digital objects that are optimized for delivery from the system.	Release 1B; Must
3.2.3.4.2.1.3	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.	Release 1B; Must
3.2.3.4.2.1.4	The DIP shall have the capability to refer to or embed one or more metadata files associated with the content.	Release 1B; Must
3.2.3.4.2.1.5	The DIP shall have the capability to refer to or embed one or more digital objects associated with metadata.	Release 1B; Must
3.2.3.4.2.1.6	The system shall provide the capability to deliver DIPs that only include content metadata.	Release 1B; Must
3.2.3.4.2.1.7	The DIP shall have the capability to be an exact replica of the AIP.	Release 1B; Must
3.2.3.4.2.1.8	The DIP Metadata shall have the capability to include descriptive, structural, technical, administrative, and packaging metadata necessary for delivery from the system.	Release 1B; Must
3.2.3.4.2.1.8.1	The DIP Metadata shall have the capability to include descriptive metadata necessary for delivery from the system.	Release 1B; Must
3.2.3.4.2.1.8.2	The DIP Metadata shall have the capability to include structural metadata necessary for delivery from the system.	Release 1B; Must

3.2.3.4.2.1.8.3	The DIP Metadata shall have the capability to include technical metadata necessary for delivery from the system.	Release 1B; Must
3.2.3.4.2.1.8.4	The DIP Metadata shall have the capability to include administrative metadata necessary for delivery from the system.	Release 1B; Must
3.2.3.4.2.1.8.5	The DIP Metadata shall have the capability to include packaging metadata necessary for delivery from the system.	Release 1B; Must
3.2.3.4.2.1.8.6	The DIP Metadata shall have the capability to include system metadata necessary for delivery from the system.	Release 1B; Must
3.2.3.4.2.1.9	Deleted.	
3.2.3.4.2.1.10	The system shall have the capability to package DIPs in such a way to facilitate delivery.	Release 1C; Must

3.2.3.4.2.2	**DIP Binding Metadata File**	
3.2.3.4.2.2.1	A DIP shall provide the capability to contain a METS file named dip.xml.	Release 1B; Must
3.2.3.4.2.2.1.1	The dip.xml file shall conform to the METS version 1.5.	Release 1B; Must
3.2.3.4.2.2.1.1.1	The dip.xml file shall conform to the GPO METS Profile version 1.0.	Release 1B; Must
3.2.3.4.2.2.1.2	The system shall provide the capability to embed or refer to digital objects (e.g., XML, OCR-ed text) as required to support delivery.	Release 1B; Must
3.2.3.4.2.2.1.3	The system shall provide the capability to embed or refer to metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support delivery.	Release 1B; Must
3.2.3.4.2.2.1.4	The system shall provide the capability to associate content metadata files with one or more digital objects in the DIP.	Release 1B; Must

3.2.3.4.2.3	**DIP Metadata**	
3.2.3.4.2.3.1	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.	Release 1B; Must
3.2.3.4.2.3.2	Deleted.	
3.2.3.4.2.3.3	The DIP shall have the capability to include mandatory descriptive metadata elements from the SIP, ACP, and AIP.	Release 1B; Must
3.2.3.4.2.3.4	The system shall provide the capability to copy descriptive metadata to a DIP.	Release 1B; Must
3.2.3.4.2.3.4.1	The system shall provide the capability to copy descriptive metadata in MODS format to a DIP.	Release 1B; Must
3.2.3.4.2.3.4.2	The system shall provide the capability to copy descriptive metadata in ONIX format to a DIP.	Release 2; Must
3.2.3.4.2.3.4.3	The system shall provide the capability to copy descriptive metadata in Dublin Core format to a DIP.	Release 2; Must

3.2.3.4.2.3.4.4	The system shall provide the capability to copy descriptive metadata in PREMIS format to a DIP.	Release 2; Must
3.2.3.4.2.3.4.5	The system shall provide the capability to copy descriptive metadata in COSATI format to a DIP.	Release 3; Must
3.2.3.4.2.3.4.6	The system shall support the capability to copy additional descriptive metadata formats to the DIP in the future.	Release 3; Must
3.2.3.4.2.3.5	Deleted.	
3.2.3.4.2.3.6	Deleted.	
3.2.3.4.2.3.7	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.	Release 1B; Must
3.2.3.4.2.3.8	The system shall provide the capability to include information generated as a result of Content Originator ordering.	Release 1B; Must
3.2.3.4.2.3.9	The system shall provide the capability to include information generated as a result of a user request.	Release 1B; Must
3.2.3.4.2.3.10	The DIP shall have the capability to include the unique ID for any content or metadata being delivered in the DIP.	Release 1C; Must
3.2.3.4.2.3.11	The system shall provide the capability to support the Open Archives Initiative Metadata Harvesting Protocol version TBD.	Release 3; Must

3.2.4.1.1	**Requirements for Pre-ingest Processes**	
3.2.4.1.1.1	**Pre-ingest Processing**	
3.2.4.1.1.1.0.1	The system shall have the capability to read registered metadata schema to extract metadata for use by the system.	Release 1B; Must
3.2.4.1.1.1.1	The system shall accept content from Content Originators.	Release 1B; Must
3.2.4.1.1.1.2	The system shall accept jobs from Content Originator ordering.	Release 1B; Must
3.2.4.1.1.1.3	The system shall accept deposited content created without using style tools.	Release 1B; Must
3.2.4.1.1.1.4	The system shall accept deposited content created using style tools.	Release 2; Could / Release 3; Must
3.2.4.1.1.1.5	The system shall accept converted content.	Release 1B; Must
3.2.4.1.1.1.6	The system shall accept harvested content.	Release 1B; Must
3.2.4.1.1.1.7	The system shall have the capability to apply version control.	Release 1B; Must
3.2.4.1.1.1.8	The system shall detect duplicate content in the system and notify authorized users.	Release 1C; Must
3.2.4.1.1.1.8.1	The system shall determine if the version of content is already in the system, using, at a minimum: Version Information, bibliographic information, authentication information, content (e.g., hashes)	Release 1B; Must

3.2.4.1.1.1.8.1.1	The system shall determine if the version of content is already in the system using version information.	Release 1B; Must
3.2.4.1.1.1.8.1.2	The system shall determine if the version of content is already in the system using bibliographic information.	Release 1B; Must
3.2.4.1.1.1.8.1.3	The system shall determine if the version of content is already in the system based on its content.	Release 1B; Must
3.2.4.1.1.1.8.1.4	The system shall have the capability to detect near duplicate documents.	Release 3; Must
3.2.4.1.1.1.8.2	The system shall have the capability to reject duplicate content.	Release 1B; Must
3.2.4.1.1.1.8.2.1	The system shall notify users when duplicate content is detected.	Release 1B; Must
3.2.4.1.1.1.8.2.2	The system shall notify users when near duplicate content is detected.	Release 3; Must
3.2.4.1.1.1.9	The system shall have the capability to store content in WIP before job order information is received.	Release 1B; Must
3.2.4.1.1.1.10	The system shall have the capability to assign a unique ID to content.	Release 1B; Must
3.2.4.1.1.1.10.1	The system shall have the capability to assign a unique ID to content packages.	Release 1B; Must
3.2.4.1.1.1.10.2	The system shall have the capability to assign a unique ID to digital objects.	Release 1B; Must
3.2.4.1.1.1.11	The system shall have the capability to assign a unique ID to jobs.	Release 1B; Must
3.2.4.1.1.1.12	The system shall populate the Identifier field in the corresponding MODS record with the content unique ID.	Release 1B; Must
3.2.4.1.1.1.13	The system shall link related jobs, business process information (BPI), and content.	Release 1B; Must
3.2.4.1.1.1.14	The system shall allow Content Evaluators to make scope determinations.	Release 1B; Must
3.2.4.1.1.1.15	The system shall have the capability to perform integrity checking.	Release 1B; Must
3.2.4.1.1.1.16	The system shall have the capability to apply a digital time stamp to content.	Release 1B; Must
3.2.4.1.1.1.17	The system shall have the capability to perform accessibility assessments.	Release 2; Must
3.2.4.1.1.1.17.1	The system shall have the capability to allow users to manually perform 508 accessibility assessments on content.	Release 1B; Must
3.2.4.1.1.1.17.2	The system shall have the capability to automatically perform 508 accessibility assessments on content.	Release 2; Must
3.2.4.1.1.1.18	The system shall have the capability to support the creation of a pre-ingest bundle (PIB).	Release 1C; Must
3.2.4.1.1.1.19	The system shall have the capability to accept modified DIPs from the Service Provider after publisher approval.	Release 1C; Must

3.2.4.1.1.1.20	The system shall have the capability to accept modified PIBs from the Service Provider after publisher approval.	Release 1C; Must
3.2.4.1.1.1.21	The system shall accept publisher approval information for SIP creation.	Release 1B; Must
3.2.4.1.1.1.22	The system shall have the capability to assemble content and metadata to create SIPs.	Release 1B; Must
3.2.4.1.1.1.23	The system shall have the capability to create a log of all transactions and activities.	Release 1B; Must

3.2.4.2.1	Requirements for Ingest Processing	
3.2.4.2.1.1	**Ingest Processing Core Capabilities**	
3.2.4.2.1.1.1	Ingest processing performs the following functions:	Release 1B; Must
3.2.4.2.1.1.1.1	Accept and validate SIPs	Release 1B; Must
3.2.4.2.1.1.1.1.1	Ingest processing shall accept SIPs.	Release 1B; Must
3.2.4.2.1.1.1.1.2	Ingest Processing shall validate SIPs.	Release 1B; Must
3.2.4.2.1.1.1.2	Ingest processing shall have the capability to create AIPs from SIPs.	Release 1B; Must
3.2.4.2.1.1.1.3	Ingest Processing shall have the capability to create ACPs from SIPs.	Release 1B; Must
3.2.4.2.1.1.1.4	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.	Release 1B; Must

3.2.4.2.1.2	**Ingest Processing**	
3.2.4.2.1.2.0.1	The system shall have the capability to transform textual content metadata into XML.	Release 2; Must
3.2.4.2.1.2.0.2	The system shall support the capability to conform to future requirements for SIP validation.	Release 3; Must
3.2.4.2.1.2.1	The system shall allow authorized users to submit content to ingest once content has been approved for release by the publisher.	Release 1B; Must
3.2.4.2.1.2.1.1	The system shall provide a prompt to confirm that the user intends to submit the SIP to ingest.	Release 1B; Should
3.2.4.2.1.2.2	The system shall validate that SIPs conform to requirements for a system compliant SIP.	Release 1B; Must
3.2.4.2.1.2.2.1	The system shall verify that the SIP includes all mandatory metadata elements.	Release 1B; Must
3.2.4.2.1.2.2.2	The system shall verify that the METS file is valid.	Release 1B; Must
3.2.4.2.1.2.2.3	The system shall verify that at least one digital object is present.	Release 1B; Must
3.2.4.2.1.2.2.4	Deleted.	
3.2.4.2.1.2.3	The system shall provide the capability to reject non-conforming SIPs.	Release 1B; Must
3.2.4.2.1.2.3.1	The system shall direct exceptions to authorized users.	Release 1B; Must

3.2.4.2.1.2.3.1.1	The system shall provide the capability for authorized users to process SIPs to conform to SIP validation.	Release 1B; Must
3.2.4.2.1.2.4	The system shall provide the capability to notify users that a SIP is nonconforming.	Release 1B; Must
3.2.4.2.1.2.5	The system shall provide the capability to notify users of the reasons a SIP is nonconforming.	Release 1B; Must
3.2.4.2.1.2.6	The system shall verify the file format of a digital object by a means other than mime type or file extension.	Release 1C; Must
3.2.4.2.1.2.7	The system shall have the capability to verify content integrity (e.g., checksum).	Release 1B; Must
3.2.4.2.1.2.8	Deleted.	
3.2.4.2.1.2.9	Deleted.	
3.2.4.2.1.2.10	The system shall have the capability to create a log of all transactions and activities.	Release 1B; Must

3.2.4.3.2	**Requirements for Preservation Processing**	
3.2.4.3.2.1	**Preservation Processing Core Capabilities**	
3.2.4.3.2.1.1	The system shall have the ability to store AIPs in a preservation repository environment.	Release 1B; Must
3.2.4.3.2.1.1.1	AIPs shall remain free from corruption and remain accessible as GPO undergoes changes in information technology and infrastructure.	Release 1B; Must
3.2.4.3.2.1.1.1.1	AIPs shall remain free from corruption as GPO undergoes changes in information technology and infrastructure.	Release 1B; Must
3.2.4.3.2.1.1.1.2	AIPs shall remain accessible as GPO undergoes changes in information technology and infrastructure.	Release 1B; Must
3.2.4.3.2.1.2	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.	Release 2; Must
3.2.4.3.2.1.2.1	Deleted.	
3.2.4.3.2.1.3	The system shall maintain the integrity of content throughout preservation processes.	Release 2; Must
3.2.4.3.2.1.3.1	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	Release 2; Must
3.2.4.3.2.1.4	The system shall preserve essential behaviors of digital content when a digital object goes through a preservation process.	Release 2; Must
3.2.4.3.2.1.4.1	The system shall maintain content functionality associated with content presentation when a digital object goes through a preservation process.	Release 2; Must
3.2.4.3.2.1.5	The system shall preserve significant properties and attributes of digital content as a digital object goes through a preservation process.	Release 2; Must

3.2.4.3.2.1.5.1	The system shall maintain content structure when a digital object goes through a preservation process	Release 2; Must
3.2.4.3.2.1.5.2	The system shall maintain content structure when a digital object goes through a preservation process.	Release 2; Must
3.2.4.3.2.1.5.3	The system shall maintain hyperlinks to content within the target document when a digital object goes through a preservation process.	Release 2; Must
3.2.4.3.2.1.5.3.1	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.	Release 2; Must
3.2.4.3.2.1.6	Deleted.	
3.2.4.3.2.1.6.1	The system shall have the capability to produce DIPs which are interoperable with other OAIS-based repositories.	Release 1C; Could / Release 2; Must
3.2.4.3.2.1.7	The system shall be capable of scheduling or executing preservation processes on individual AIPs or on selected groups of archival content.	Release 2; Must
3.2.4.3.2.1.7.1	The system shall be capable of scheduling preservation processes on individual AIPs.	Release 2; Must
3.2.4.3.2.1.7.2	The system shall be capable of scheduling preservation processes on selected groups of archival content.	Release 2; Must
3.2.4.3.2.1.7.3	The system shall be capable of executing preservation processes on individual AIPs.	Release 2; Must
3.2.4.3.2.1.7.4	The system shall be capable of executing preservation processes on selected groups of archival content.	Release 2; Must

3.2.4.3.2.2	**Preservation Processing**	
3.2.4.3.2.2.0.1	The system shall have the capability to transform digital object(s) into a digital object of another format.	Release 3; Must
3.2.4.3.2.2.1	The system shall have the ability to migrate data to formats other than those in which the files were created or received.	Release 2; Must
3.2.4.3.2.2.1.1	The system shall support the transformation of Quark digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.1.1	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.	Release 2; Must
3.2.4.3.2.2.1.1.2	The system shall support the transformation of Quark digital objects into HTML digital objects.	Release 2; Must
3.2.4.3.2.2.1.1.3	The system shall support the transformation of Quark digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.1.4	The system shall support the transformation of Quark digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.1.5	The system shall support the transformation of Quark digital objects into PDF digital objects.	Release 2; Must

3.2.4.3.2.2.1.1.13	The system shall support the ability to set parameters of the output file of the transformation (resolution, color depth, etc).	Release 2; Must
3.2.4.3.2.2.1.1	The system shall ensure that the files resulting from migrations will be in a format free of proprietary restrictions to the possible extent.	Release 1C; Should / Release 2; Must
3.2.4.3.2.2.1.2	The system shall support the transformation of InDesign digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.2.1	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.	Release 2; Must
3.2.4.3.2.2.1.2.2	The system shall support the transformation of InDesign digital objects into HTML digital objects.	Release 2; Must
3.2.4.3.2.2.1.2.3	The system shall support the transformation of InDesign digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.2.4	The system shall support the transformation of InDesign digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.2.5	The system shall support the transformation of InDesign digital objects into PDF digital objects.	Release 2; Must
3.2.4.3.2.2.1.2	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.	Release 2; Must
3.2.4.3.2.2.1.3	The system shall support the transformation of Microsoft Word digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.3.1	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.	Release 2; Must
3.2.4.3.2.2.1.3.2	The system shall support the transformation of Microsoft Word digital objects into HTML digital objects.	Release 2; Must
3.2.4.3.2.2.1.3.3	The system shall support the transformation of Microsoft Word digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.3.4	The system shall support the transformation of Microsoft Word digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.3.5	The system shall support the transformation of Microsoft Word digital objects into PDF digital objects.	Release 2; Must
3.2.4.3.2.2.1.3.6	The system shall support the transformation of Microsoft Word digital objects into Open Document digital objects.	Release 2; Must
3.2.4.3.2.2.1.4	The system shall support the transformation of Microsoft Excel digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.4.1	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.	Release 2; Must

3.2.4.3.2.2.1.4.2	The system shall support the transformation of Microsoft Excel digital objects into HTML digital objects.	Release 2; Must
3.2.4.3.2.2.1.4.3	The system shall support the transformation of Microsoft Excel digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.4.4	The system shall support the transformation of Microsoft Excel digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.4.5	The system shall support the transformation of Microsoft Excel digital objects into PDF digital objects.	Release 2; Must
3.2.4.3.2.2.1.4.6	The system shall support the transformation of Microsoft Excel digital objects into Open Document digital objects.	Release 2; Must
3.2.4.3.2.2.1.4	The system shall have the ability to produce notification of incomplete or unsuccessful migrations.	Release 2; Must
3.2.4.3.2.2.1.4.1	The system shall have the ability to identify incomplete or unsuccessful migrations.	Release 2; Must
3.2.4.3.2.2.1.4.2	The system shall have the ability to produce notification of incomplete or unsuccessful migrations.	Release 2; Must
3.2.4.3.2.2.1.5	The system shall support the transformation of Microsoft PowerPoint digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.5.1	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.	Release 2; Must
3.2.4.3.2.2.1.5.2	The system shall support the transformation of Microsoft PowerPoint digital objects into HTML digital objects.	Release 2; Must
3.2.4.3.2.2.1.5.3	The system shall support the transformation of Microsoft PowerPoint digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.5.4	The system shall support the transformation of Microsoft PowerPoint digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.5.5	The system shall support the transformation of Microsoft PowerPoint digital objects into PDF digital objects.	Release 2; Must
3.2.4.3.2.2.1.5.6	The system shall support the transformation of Microsoft PowerPoint digital objects into Open Document digital objects.	Release 2; Must
3.2.4.3.2.2.1.6	The system shall support the transformation of PDF digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.6.1	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.	Release 2; Must
3.2.4.3.2.2.1.6.2	The system shall support the transformation of PDF digital objects into HTML digital objects.	Release 2; Must

3.2.4.3.2.2.1.6.3	The system shall support the transformation of PDF digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.6.4	The system shall support the transformation of PDF digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.6.5	The system shall support the transformation of HTML digital objects into PDF digital objects.	Release 2; Must
3.2.4.3.2.2.1.6.6	The system shall support the transformation of HTML digital objects into XHTML digital objects.	Release 2; Must
3.2.4.3.2.2.1.7	The system shall support the transformation of HTML digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.7.1	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.	Release 2; Must
3.2.4.3.2.2.1.7.2	The system shall support the transformation of HTML digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.7.3	The system shall support the transformation of HTML digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.8	The system shall support the transformation of TIFF digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.8.1	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.	Release 2; Must
3.2.4.3.2.2.1.8.2	The system shall support the transformation of the full text index of any TIFF digital object into an ASCII digital object.	Release 2; Must
3.2.4.3.2.2.1.8.3	The system shall support the transformation of the full text index of any TIFF digital object into an XML digital object.	Release 2; Must
3.2.4.3.2.2.1.8.5	The system shall support the transformation of the full text index of any TIFF digital object into an HTML digital object.	Release 2; Must
3.2.4.3.2.2.1.8.6	The system shall support the transformation a TIFF digital object into a JPG digital object.	Release 2; Must
3.2.4.3.2.2.1.8.4	The system shall support the transformation of the full text index of any TIFF digital object into an PDF digital object.	Release 2; Must
3.2.4.3.2.2.1.9	The system shall provide an interface to integrate transforming technologies as required.	Release 1B; Must
3.2.4.3.2.2.1.10	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.	Release 2; Must
3.2.4.3.2.2.1.11	Where formats containing images are transformed to XML the placement of said images, if any, will be stored in the new format	Release 2; Must
3.2.4.3.2.2.1.12	The system shall support the transformation of WordPerfect digital objects as defined below:	Release 2; Must

3.2.4.3.2.2.1.12.1	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.	Release 2; Must
3.2.4.3.2.2.1.12.2	The system shall support the transformation of WordPerfect digital objects into Microsoft Word digital objects.	Release 2; Must
3.2.4.3.2.2.1.12.3	The system shall support the transformation of WordPerfect digital objects into HTML digital objects.	Release 2; Must
3.2.4.3.2.2.1.12.4	The system shall support the transformation of WordPerfect digital objects into ASCII digital objects.	Release 2; Must
3.2.4.3.2.2.1.12.5	The system shall support the transformation of WordPerfect digital objects into XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.12.6	The system shall support the transformation of WordPerfect digital objects into PDF digital objects.	Release 2; Must
3.2.4.3.2.2.1.14	The system shall support the transformation of EPS digital objects as defined below:	Release 2; Must
3.2.4.3.2.2.1.14.1	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.	Release 2; Must
3.2.4.3.2.2.1.14.2	The system shall support the transformation of the full text index of any EPS digital object into an ASCII digital object	Release 2; Must
3.2.4.3.2.2.1.14.3	The system shall support the transformation of the full text index of any EPS digital object into an XML digital object	Release 2; Must
3.2.4.3.2.2.1.14.5	The system shall support the transformation of the full text index of any EPS digital object into an HTML digital object	Release 2; Must
3.2.4.3.2.2.1.14.4	The system shall support the transformation of the full text index of any EPS digital object into an PDF digital object	Release 2; Must
3.2.4.3.2.2.1.15	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.	Release 2; Must
3.2.4.3.2.2.1.16	The system shall support the transformation of XML as defined below:	Release 2; Must
3.2.4.3.2.2.1.16.1	The system shall support the transformation of XML digital objects into other registered XML digital objects.	Release 2; Must
3.2.4.3.2.2.1.16.2	The system shall support the transformation of XML metadata into other registered XML metadata.	Release 2; Must
3.2.4.3.2.2.1.16.3	The system shall support the transformation of system metadata into other registered XML metadata.	Release 2; Must
3.2.4.3.2.2.1.17	The system shall have the capability to perform transformations without deleting the content that has been acted upon.	Release 2; Must

3.2.4.3.2.2.1.18	The system shall provide the capability to apply quality metrics to format transformations.	Release 2; Must
3.2.4.3.2.2.2	The system shall have the ability to preserve bit streams of digital objects of content as submitted by refreshment.	Release 1C; Must
3.2.4.3.2.2.2.1	The system shall have the ability to verify that the refreshed file is authentic and faithful.	Release 1C; Must
3.2.4.3.2.2.2.2	The system shall provide logs that record the results of refreshment processes.	Release 1C; Must
3.2.4.3.2.2.2.3	The system shall have the ability to notify users of incomplete or unsuccessful refreshment processes.	Release 1C; Must
3.2.4.3.2.2.2.3.1	The system shall have the ability to identify incomplete or unsuccessful refreshments processes.	Release 1C; Must
3.2.4.3.2.2.2.3.2	The system shall have the ability to produce notification of incomplete or unsuccessful refreshments processes.	Release 1C; Must
3.2.4.3.2.2.3	The system shall have the ability to support emulation to preserve access to content.	Release 2; Must
3.2.4.3.2.2.3.1	The system shall have the ability to verify that the emulated file retains specified attributes and behaviors, i.e. is authentic and faithful.	Release 2; Must
3.2.4.3.2.2.4	The system shall support the transformation of AIPs into ACPs.	Release 2; Must
3.2.4.3.2.2.5	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.	Release 2; Must

3.2.4.3.2.3	**Preservation Processing - Assessment**	
3.2.4.3.2.3.1	The system shall have the ability to assess ingested content and determine preservation processes based on the assessments.	Release 2; Must
3.2.4.3.2.3.1.1	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.	Release 2; Must
3.2.4.3.2.3.1.2	There shall be no limit set on the number or frequency of assessments.	Release 2; Must
3.2.4.3.2.3.1.3	The system shall have the ability to re-assess content stored in the system.	Release 2; Must
3.2.4.3.2.3.2	The system shall present a range of options to the Service Specialist for decision if the system is unable to make a determination.	Release 3; Could

3.2.4.3.2.4	**Preservation Processing - Administration**	
3.2.4.3.2.4.1	The system shall support scheduling the automatic execution of preservation processes.	Release 2; Must
3.2.4.3.2.4.2	The system shall support batch Content Preservation of content.	Release 2; Must

3.2.4.3.2.4.3	The system shall support Content Preservation on an item-by-item basis.	Release 2; Must
3.2.4.3.2.4.4	The system shall maintain an audit trail of preservation processes.	Release 2; Must
3.2.4.3.2.4.5	The system shall support the ability for authorized users to request preservation processes.	Release 2; Must

3.2.4.3.2.5	**Preservation Processing - Storage**	
3.2.4.3.2.5.1	The system shall provide a digital archival repository environment which is based on open-standards architecture.	Release 1C; Must
3.2.4.3.2.5.1.1	The repository environment shall keep AIPs separate from working or production copies.	Release 1C; Must
3.2.4.3.2.5.1.2	The system shall ensure that when content in AIP is changed, the content in the ACP is changed.	Release 1C; Must
3.2.4.3.2.5.1.3	The system shall maintain one on more backups of the repository environment consistent with the overall FDsys storage requirements.	Release 1C; Must

3.2.4.3.2.6	**Preservation Processing - Metadata**	
3.2.4.3.2.6.1	The system shall capture or generate metadata which specifies the relationship of files resulting from preservation processes to their predecessors.	Release 2; Must
3.2.4.3.2.6.2	The system shall employ metadata for preservation which is compliant with the emerging standard developed by the PREMIS working group.	Release 1C; Must
3.2.4.3.2.6.3	The system shall employ schema for facilitating preservation metadata processes compliant with those developed by the PREMIS working group.	Release 1C; Must

3.2.4.3.2.7	**Preservation Processing - Security**	
3.2.4.3.2.7.1	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).	Release 2; Must

3.2.4.4.2	**Requirements for Unique Identifier**	
3.2.4.4.2.0.1.2	The system shall allow an authorized user to apply a new level of granularity to content without affecting previously applied levels.	Release 1C; Must
3.2.4.4.2.0.1.3	The system shall assign unique IDs.	Release 1B; Must
3.2.4.4.2.0.1.4	Unique ID shall be human-readable.	Release 1B; Must
3.2.4.4.2.0.1.5	Unique ID shall be expressible in XML ID.	Release 1B; Must
3.2.4.4.2.0.1.6	Unique ID shall be an alphanumeric identifier (ANI).	Release 1B; Must
3.2.4.4.2.0.1.7	The system shall allow for the pre-assignment of unique IDs to external entities.	Release 1B; Must
3.2.4.4.2.0.1.8	The system shall only accept unique IDs created by the system.	Release 1B; Must

3.2.4.4.2.0.1.9	The system shall provide the capability to apply unique IDs to digital objects.	Release 1B; Must
3.2.4.4.2.0.1.10	Unique ID characters shall include numbers 0-9 and letters A – Z (minus I and O).	Release 1B; Must
3.2.4.4.2.0.1.11	Unique ID shall be stored in Metadata.	Release 1B; Must
3.2.4.4.2.0.1.12	Unique ID shall be unique.	Release 1B; Must

3.2.4.4.2.1	**Unique ID Core Capabilities**	
3.2.4.4.2.1.0.1	The system shall support granularity of any content based on the natural granularity boundaries of that content.	Release 2; Must
3.2.4.4.2.1.0.1.2	The system shall support granularity of GPO Access content referenced in 7.4.2.2.4.b based on the natural granularity boundaries of that content.	Release 1C; Must
3.2.4.4.2.1.1	The system shall allow GPO to define the level of granularity that content can be retrieved at.	Release 1B; Must
3.2.4.4.2.1.1.0.1	The system shall have the capability for a user to decide the level of granularity that should be applied to a publication.	Release 1C; Must
3.2.4.4.2.1.1.0.1.1	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).	Release 1C; Must
3.2.4.4.2.1.1.0.2	The system shall allow elements to be retrieved by at all levels of granularity	Release 1C; Must
3.2.4.4.2.1.1.1	The system shall support granularity to the level of a publication.	Release 1B; Must
3.2.4.4.2.1.1.2	The system shall support granularity down to the level of any paragraph in a publication.	Release 1C; Should / Release 2; Must
3.2.4.4.2.1.1.3	The system shall support granularity down to the level of any individual graphic	Release 1C; Must
3.2.4.4.2.1.1.4	The system shall support granularity down to the level of any embedded graphical element in a publication	Release 1C; Should / Release 2; Must
3.2.4.4.2.1.1.5	The system shall support granularity down to the level of any video in its entirety.	Release 1C; Must
3.2.4.4.2.1.1.6	The system shall support granularity down to the level of any segment of any video.	Release 3; Must
3.2.4.4.2.1.1.7	The system shall support granularity down to the level of any audio in its entirety.	Release 1C; Must
3.2.4.4.2.1.1.8	The system shall support granularity down to the level of any segment of any audio.	Release 3; Should
3.2.4.4.2.1.2	Deleted.	
3.2.4.4.2.1.2.1	Deleted.	
3.2.4.4.2.1.2.2	Deleted.	
3.2.4.4.2.1.2.3	Deleted.	
3.2.4.4.2.1.2.4	Deleted.	

3.2.4.4.2.1.2.5	The system shall provide the capability to support 10 trillion Digital Objects without redesigning the system.	Release 1C; Must
3.2.4.4.2.1.3	Deleted.	
3.2.4.4.2.1.3.1	Deleted.	
3.2.4.4.2.1.3.2	Deleted.	
3.2.4.4.2.1.4	Deleted.	
3.2.4.4.2.1.5	Deleted.	

3.2.4.4.2.2	**Job ID**	
3.2.4.4.2.2.1	The system shall create and assign a unique ID for each job.	Release 1B; Must
3.2.4.4.2.2.2.1	The system shall provide the capability to assign unique IDs to Content Originator orders of content jobs.	Release 1B; Must
3.2.4.4.2.2.2.2	The system shall provide the capability to assign unique IDs to Content Originator orders of service jobs.	Release 1B; Must
3.2.4.4.2.2.2.3	The system shall provide the capability to assign unique IDs to non-Content Originator order related jobs.	Release 1B; Must
3.2.4.4.2.2.3	The system shall not re-use Job unique IDs.	Release 1B; Must

3.2.4.4.2.3	**Content Package ID**	
3.2.4.4.2.3.1	The system shall create and assign a unique ID for each Content Package.	Release 1B; Must
3.2.4.4.2.3.1.1	The system shall create and assign a unique ID to each SIP.	Release 1B; Must
3.2.4.4.2.3.1.2	The system shall create and assign a unique ID to each AIP.	Release 1B; Must
3.2.4.4.2.3.1.2.1	The AIP shall inherit the unique ID from the SIP if an ACP is not created.	Release 1B; Must
3.2.4.4.2.3.1.2.2	The ACP shall inherit the unique ID from the SIP if an AIP is not created.	Release 1B; Must
3.2.4.4.2.3.1.3	The system shall create and assign a unique ID to each ACP.	Release 1B; Must
3.2.4.4.2.3.1.4	Deleted.	
3.2.4.4.2.3.2	Content Package unique IDs shall be unique.	Release 1B; Must
3.2.4.4.2.3.3	The system shall record package unique ID's in metadata.	Release 1B; Must

3.2.4.4.2.4	**Interface for Unique ID**	
3.2.4.4.2.4.1	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.	Release 1B; Must
3.2.4.4.2.4.1.0.1	The system shall allow the capability for an authorized user to input a unique ID.	Release 1B; Must

3.2.4.4.2.4.1.0.2	The system shall allow the capability for an authorized user to retrieve content and information about the content associated with a unique ID.	Release 1B; Must
3.2.4.4.2.4.1.0.3	The system shall allow the capability for an authorized user to input an agency supplied ID.	Release 1B; Must
3.2.4.4.2.4.1.0.4	The system shall allow the capability for an authorized user to retrieve content and information about the content associated with an agency supplied ID.	Release 1B; Must
3.2.4.4.2.4.1.1	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).	Release 1B; Must

3.2.4.5.2	Requirements for Persistent Name	
3.2.4.5.2.1	**Persistent Name Core Capabilities**	
3.2.4.5.2.1.1	The system shall assign persistent names to all in-scope published versions during access processing.	Release 1C; Must
3.2.4.5.2.1.1.1	Persistent name shall not conflict with other identifiers within FDsys.	Release 1C; Must
3.2.4.5.2.1.2	The system shall comply with the following standards and best practices pertaining to persistent naming.	Release 1C; Must
3.2.4.5.2.1.2.1	“Persistent Identification: A Key Component Of An E-Government Infrastructure.” CENDI Persistent Identification Task Group (March 10, 2004)	Release 1C; Must
3.2.4.5.2.1.2.2	Interagency Committee on Government Information Recommendations to the Office of Management and Budget (December 17, 2004)	Release 1C; Must
3.2.4.5.2.1.2.3	RFC 1737 Functional Requirements for Uniform Resource Names (December 1994)	Release 1C; Must
3.2.4.5.2.1.2.4	RFC 2141 URN Syntax (May 1997)	Release 1C; Must
3.2.4.5.2.1.2.5	RFC 2396 – Uniform Resource Identifiers (URI): Generic Syntax (August 1998)	Release 1C; Must
3.2.4.5.2.1.3	The system shall support interoperability across different naming systems to allow one system to access a resource within another.	Release 3; Should
3.2.4.5.2.1.4	The system shall accommodate OpenURL syntax to enable federated searching.	Release 3; Must
3.2.4.5.2.1.5	The system shall support the persistent name supplied by GPO as the definitive persistent name.	Release 1C; Must
3.2.4.5.2.1.5.1	The system shall allow GPO to elect other systems or agencies to become recognized GPO naming authorities.	Release 1C; Must
3.2.4.5.2.1.6	The system shall assign persistent names that are location independent.	Release 1C; Must
3.2.4.5.2.1.7	The system shall assign persistent names that are protocol independent.	Release 3; Must
3.2.4.5.2.1.8	Persistent names shall be unique.	Release 1C; Must

3.2.4.5.2.1.9	The system shall have the capability to assign intelligent persistent names.	Release 1C; Must
3.2.4.5.2.1.9.1	The system shall have the capability to assign predictable persistent names.	Release 1C; Must
3.2.4.5.2.1.10	The system shall have the capability to assign non-intelligent persistent names.	Release 1C; Could
3.2.4.5.2.1.11	Deleted.	
3.2.4.5.2.1.12	The system shall have the capability to record the date and time of persistent name creation.	Release 1C; Must
3.2.4.5.2.1.12.1	Date and time of the persistent name creation shall be recorded in metadata.	Release 1C; Must
3.2.4.5.2.1.13	The system shall have the capability to create reports about persistent name management.	Release 2; Could
3.2.4.5.2.1.14	The system shall resolve legacy existing GPO naming schemes.	Release 1C; Must
3.2.4.5.2.1.14.1	The system shall resolve existing PURLs.	Release 1C; Must
3.2.4.5.2.1.14.2	The system shall resolve existing URLS that were constructed using GetDoc.	Release 1C; Must
3.2.4.5.2.1.14.3	The system shall resolve existing URLS that were constructed using GetPage.	Release 1C; Must
3.2.4.5.2.1.14.4	The system shall resolve existing URLS that were constructed using GetCFR.	Release 1C; Must
3.2.4.5.2.1.15	The system shall support one persistent name per AIP.	Release 1C; Must

3.2.4.5.2.2	**Persistent Name Resolution**	
3.2.4.5.2.2.1	The system shall use a resolution system to locate and provide access to content with persistent names.	Release 1C; Must
3.2.4.5.2.2.1.1	The resolution process shall resolve an assigned name into a resource or the resource metadata.	Release 1C; Must
3.2.4.5.2.2.1.2	The resolution process shall allow for persistent name recognition within standard browsers.	Release 1C; Must
3.2.4.5.2.2.2	The system shall have the capability to support distributed persistent naming and resolution at the local and global level.	Release 1C; Must
3.2.4.5.2.2.3	The system shall support resolution of a single persistent name to multiple distributed locations.	Release 1C; Should
3.2.4.5.2.2.3.1	The system shall be able to identify and resolve to multiple identical copies of a resource at multiple locations through a single persistent name.	Release 1C; Should
3.2.4.5.2.2.4	The system shall support resolution of a single persistent name to multiple content versions.	Release 1C; Should
3.2.4.5.2.2.4.1	The system shall determine the most appropriate rendition based on attributes of the request.	Release 1C; Should

3.2.4.5.2.3	**Persistent Name Metadata**	
3.2.4.5.2.3.1	The system shall record persistent names associated with content.	Release 1C; Must

3.2.4.5.2.3.2	The system shall record existing persistent names associated with content.	Release 1C; Must
3.2.4.5.2.3.3	The system shall provide the capability to associate metadata with the persistent name	Release 1C; Must

3.2.4.6.2	**Requirements for Authentication**	
3.2.4.6.2.1	**Authentication Core Capabilities**	
3.2.4.6.2.1.1	The system shall provide the capability to certify content as authentic.	Release 1C; Must
3.2.4.6.2.1.1.0.1	The system shall provide the capability to use passwords to verify the identity of authorized users.	Release 1B; Must
3.2.4.6.2.1.1.0.2	The system shall provide the capability to use PKI certificates to verify the identity of authorized users.	Release 1C; Must
3.2.4.6.2.1.1.0.3	The system shall provide the capability to verify the authorization level of authorized users to perform requested functions.	Release 1B; Must
3.2.4.6.2.1.1.0.4	The system shall provide the capability to validate credentials (e.g. digital certificate) of authorized users.	Release 1C; Must
3.2.4.6.2.1.1.1	Deleted.	
3.2.4.6.2.1.1.2	Deleted.	
3.2.4.6.2.1.2	The system shall provide the capability to certify content as official.	Release 2; Must
3.2.4.6.2.1.2.1	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 will record information about this designation (intended use) in metadata.	Release 1C; Must
3.2.4.6.2.1.3	The system shall provide the capability to certify content at levels of granularity defined by GPO.	Release 2; Must
3.2.4.6.2.1.4	The system shall provide the capability to convey certification by means of an integrity mark.	Release 1C; Must
3.2.4.6.2.1.5	The system shall provide the capability to use GPO's Public Key Infrastructure (PKI).	Release 1C; Must
3.2.4.6.2.1.6	Deleted.	
3.2.4.6.2.1.7	Deleted.	
3.2.4.6.2.1.8	The system shall provide the capability to use public key cryptography, digital certificates, encryption or other widely accepted information security mechanisms for providing authentication services within FDsys.	Release 1C; Must

3.2.4.6.2.2	**Authentication - Content Pre-ingest and Ingest**	
3.2.4.6.2.2.1	The system must provide the capability to verify and validate the authenticity, integrity, and official status of deposited content.	Release 2; Must

3.2.4.6.2.2.1.0.1	The system shall provide the capability to validate the authenticity of deposited content.	Release 2; Must
3.2.4.6.2.2.1.0.2	The system shall provide the capability to validate the integrity of deposited content.	Release 2; Must
3.2.4.6.2.2.1.0.3	The system shall provide the capability to validate the official status of deposited content.	Release 2; Must
3.2.4.6.2.2.1.1	The system shall verify the identity and authority of authorized users.	Release 2; Must
3.2.4.6.2.2.1.2	Valid proof of the user’s identity shall be logged by the system.	Release 2; Must
3.2.4.6.2.2.1.3	The source (e.g., OriginInfo:publisher) of the deposited content shall be recorded in metadata.	Release 1B; Must
3.2.4.6.2.2.1.4	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.	Release 2; Must
3.2.4.6.2.2.1.4.1	The system shall validate that deposited content has not been altered in an unauthorized manner during transmission from the authorized user to the system.	Release 2; Must
3.2.4.6.2.2.1.4.2	The system shall validate that deposited content has not been destroyed in an unauthorized manner during transmission from the authorized user to the system.	Release 2; Must
3.2.4.6.2.2.1.4.3	The system shall record information about deposited content integrity in metadata.	Release 2; Must
3.2.4.6.2.2.1.5	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.	Release 1C; Must
3.2.4.6.2.2.1.5.1	The system shall verify that the content sender is, in fact, the party who claimed to have sent the content.	Release 1C; Must
3.2.4.6.2.2.1.5.2	The system shall verify that the content recipient is, in fact, the party who claimed to have received the content.	Release 1C; Must
3.2.4.6.2.2.1.5.3	The system shall record content sender and recipient information in metadata.	Release 1C; Must
3.2.4.6.2.2.1.6	The system shall have the capability to record intended use in metadata.	Release 2; Must
3.2.4.6.2.2.1.7	The system shall have the capability to use PKI for the establishment of a trust model for deposited content.	Release 2; Must
3.2.4.6.2.2.2	The system must provide the capability to verify and validate the authenticity, integrity, and official status of harvested content.	Release 2; Must
3.2.4.6.2.2.2.0.1	The system shall provide the capability to validate the authenticity of harvested content.	Release 2; Must
3.2.4.6.2.2.2.0.2	The system shall provide the capability to validate the integrity of harvested content.	Release 2; Must
3.2.4.6.2.2.2.0.3	The system shall provide the capability to validate the official status of harvested content.	Release 2; Must

3.2.4.6.2.2.2.1	The system shall examine harvested content for the purpose of verifying the source of the harvested content.	Release 1C; Must
3.2.4.6.2.2.2.2	The source (e.g., OriginInfo:publisher) of harvested content shall be recorded in metadata.	Release 1C; Must
3.2.4.6.2.2.2.3	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.	Release 1C; Must
3.2.4.6.2.2.2.3.1	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.	Release 1C; Must
3.2.4.6.2.2.2.3.2	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.	Release 1C; Must
3.2.4.6.2.2.2.3.3	The system shall record information about the harvested content integrity in metadata.	Release 1C; Must
3.2.4.6.2.2.3	The system must provide the capability to verify and validate the authenticity, integrity, and official status of converted content.	Release 2; Must
3.2.4.6.2.2.3.0.1	The system shall provide the capability to validate the authenticity of converted content.	Release 2; Must
3.2.4.6.2.2.3.0.2	The system shall provide the capability to validate the integrity of converted content.	Release 2; Must
3.2.4.6.2.2.3.0.3	The system shall provide the capability to validate the official status of converted content.	Release 2; Must
3.2.4.6.2.2.3.1	The source (e.g., OriginInfo:publisher) of converted content shall be recorded in metadata.	Release 1B; Must
3.2.4.6.2.2.3.2	The source (e.g., OriginInfo:publisher) of tangible content that was used to create the converted content shall be recorded in metadata.	Release 1B; Must
3.2.4.6.2.2.3.3	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.	Release 2; Must
3.2.4.6.2.2.3.3.1	The system shall validate that converted content has not been altered in an unauthorized manner during transmission to the system.	Release 2; Must
3.2.4.6.2.2.3.3.2	The system shall validate that converted content has not been destroyed in an unauthorized manner during transmission to the system.	Release 2; Must
3.2.4.6.2.2.3.3.3	The system shall record information about converted content integrity in metadata.	Release 2; Must
3.2.4.6.2.2.3.4	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.	Release 2; Must

3.2.4.6.2.2.3.4.1	The system shall verify that the sender is, in fact, the party who claimed to have sent the converted content.	Release 2; Must
3.2.4.6.2.2.3.4.2	The system shall verify that the recipient is, in fact, the party who claimed to have received the converted content.	Release 2; Must
3.2.4.6.2.2.3.4.3	The system shall record the sender and the recipient information in metadata.	Release 2; Must
3.2.4.6.2.2.3.5	The system shall have the capability to record intended use in metadata.	Release 1B; Must
3.2.4.6.2.2.3.6	The system shall have the capability to use PKI for the establishment of a trust model for converted content.	Release 2; Must
3.2.4.6.2.2.4	The system shall provide the capability to recognize and validate integrity marks at pre-ingest.	Release 2; Must
3.2.4.6.2.2.4.0.1	The system shall provide the capability to recognize integrity marks at pre-ingest.	Release 2; Must
3.2.4.6.2.2.4.0.2	The system shall provide the capability to validate integrity marks at pre-ingest.	Release 2; Must
3.2.4.6.2.2.4.1	The system shall have the capability to retain integrity marks in accordance with GPO business rules.	Release 2; Must
3.2.4.6.2.2.4.2	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 record in metadata that a digital signature was present and make this information available to End Users.	Release 1C; Must
3.2.4.6.2.2.4.2.1	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.	Release 1C; Must
3.2.4.6.2.2.4.2.2	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.	Release 1C; Must
3.2.4.6.2.2.5	The system shall provide the capability to process encrypted files at pre-ingest.	Release 1C; Could / Release 2; Must
3.2.4.6.2.2.6	The system shall record chain of custody information.	Release 2; Must
3.2.4.6.2.2.6.1	Chain of custody information shall be recorded in metadata.	Release 2; Must
3.2.4.6.2.2.6.2	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.	Release 2; Must

3.2.4.6.2.2.6.2.1	The system shall have the ability to gather Distinguished Name information from integrity marks for use as part of the chain of custody.	Release 2; Must
3.2.4.6.2.2.6.2.2	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.	Release 2; Must
3.2.4.6.2.2.6.2.3	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.	Release 2; Must
3.2.4.6.2.2.6.2.4	The system shall have the capability to record chain of custody in WIP.	Release 2; Must
3.2.4.6.2.2.6.2.5	The system shall have the ability to gather chain of custody from content metadata when it is not available from integrity marks.	Release 2; Must
3.2.4.6.2.2.6.2.6	The system shall update chain of custody information in metadata at ingest.	Release 1C; Must
3.2.4.6.2.2.7	The system shall provide the capability to perform redundancy checking (e.g., checksum) on content at ingest.	Release 2; Must
3.2.4.6.2.2.7.1	The system shall provide the capability to record checksum type and value in metadata.	Release 1C; Must
3.2.4.6.2.2.7.1.1	The system shall provide the capability to record checksum type in metadata.	Release 1C; Must
3.2.4.6.2.2.7.1.2	The system shall provide the capability to record checksum value in metadata.	Release 1C; Must
3.2.4.6.2.2.8	The system shall provide the capability to apply a digital timestamp to content at ingest.	Release 1C; Must
3.2.4.6.2.2.9	Deleted.	

3.2.4.6.2.3	**Authentication - User Credentials**	
3.2.4.6.2.3.1	Deleted.	
3.2.4.6.2.3.1.1	Deleted.	
3.2.4.6.2.3.2	Deleted.	

3.2.4.6.2.4	**Authentication - Content Integrity**	
3.2.4.6.2.4.1	The system must provide the capability to maintain content integrity by ensuring that content has not been altered or destroyed in an unauthorized manner.	Release 1B; Must
3.2.4.6.2.4.1.0.1	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.	Release 1B; Must
3.2.4.6.2.4.1.0.2	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.	Release 1B; Must

3.2.4.6.2.4.1.0.3	The system shall have the capability to ensure integrity of content within the system at a definable frequency.	Release 1B; Must
3.2.4.6.2.4.1.0.4	The system shall have the capability to ensure integrity of work in progress content.	Release 1B; Must
3.2.4.6.2.4.2	Deleted.	
3.2.4.6.2.4.2.2	Deleted.	
3.2.4.6.2.4.2.3	The system shall not allow critical transaction and system log files to be adjusted by any unauthorized party.	Release 1B; Must
3.2.4.6.2.4.2.3.1	The system shall not allow critical transaction files to be adjusted by any unauthorized party.	Release 1B; Must
3.2.4.6.2.4.2.3.2	The system shall not allow system log files to be adjusted by any unauthorized party.	Release 1B; Must
3.2.4.6.2.4.2.4	The system shall have the capability to certify integrity of content during backup and other system processes.	Release 1B; Must
3.2.4.6.2.4.3	The system shall certify integrity of pre-ingested and ingested content.	Release 2; Must
3.2.4.6.2.4.3.0.1	The system shall certify integrity of pre-ingested content.	Release 2; Must
3.2.4.6.2.4.3.0.2	The system shall certify integrity of ingested content.	Release 2; Must
3.2.4.6.2.4.3.1	Content integrity shall be maintained during transmission from the Content Originator to the system.	Release 1C; Must
3.2.4.6.2.4.3.2	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.	Release 2; Must
3.2.4.6.2.4.4	The system shall have the capability to certify integrity of delivered content.	Release 2; Must
3.2.4.6.2.4.4.1	The system shall have the capability to apply a cryptographic digital signature, in accordance with IETF RFC 3447, to content delivered from the system.	Release 2; Must
3.2.4.6.2.4.4.2	The system shall have the capability to verify that the electronic content is valid, uncorrupted, and free of malicious code.	Release 2; Must
3.2.4.6.2.4.4.2.1	The system shall have the capability to verify that the electronic content is valid.	Release 2; Must
3.2.4.6.2.4.4.2.2	The system shall have the capability to verify that the electronic content is uncorrupted.	Release 2; Must
3.2.4.6.2.4.4.2.3	The system shall have the capability to verify that the electronic content is free of malicious code.	Release 2; Must
3.2.4.6.2.4.5	The system shall provide the capability to provide notification that a change has occurred to content within the system.	Release 2; Must

3.2.4.6.2.4.5.1	The system shall provide the capability to notify designated users if content has been altered or destroyed in an unauthorized manner.	Release 2; Must
3.2.4.6.2.4.5.1.1	The system shall provide the capability to notify designated users if content has been altered in an unauthorized manner.	Release 2; Must
3.2.4.6.2.4.5.1.2	The system shall provide the capability to notify designated users if content has been destroyed in an unauthorized manner.	Release 2; Must
3.2.4.6.2.4.5.2	The system shall provide the capability to notify designated users if content has been altered or destroyed in an authorized manner.	Release 2; Must
3.2.4.6.2.4.5.2.1	The system shall provide the capability to notify designated users if content has been altered in an authorized manner.	Release 2; Must
3.2.4.6.2.4.5.2.2	The system shall provide the capability to notify designated users if content has been destroyed in an authorized manner.	Release 2; Must
3.2.4.6.2.4.5.3	The system shall provide the capability to notify designated users when changes were made to content.	Release 2; Must
3.2.4.6.2.4.5.4	The system shall provide the capability to notify designated users where changes were made to content.	Release 2; Must
3.2.4.6.2.4.5.5	The system shall provide the capability to notify designated users by whom changes were made to content.	Release 2; Must
3.2.4.6.2.4.5.6	The system shall provide the capability to notify designated users what changes were made to content.	Release 2; Must
3.2.4.6.2.4.5.7	The system shall log changes to content in metadata.	Release 2; Must
3.2.4.6.2.4.6	The system shall provide the capability of demonstrating continued integrity of content packages when authorized changes are made (such as to the metadata).	Release 2; Must

3.2.4.6.2.5	**Authentication - Time Stamps**	
3.2.4.6.2.5.1	The system shall support digital time stamping.	Release 1C; Must
3.2.4.6.2.5.2	The system shall provide the capability to provide date and time verification.	Release 2; Must
3.2.4.6.2.5.3	The system shall be flexible enough to provide date and time verification through various mechanisms including a time certification authority, network server, or the signer’s system.	Release 2; Must
3.2.4.6.2.5.3.1	The system shall be flexible enough to provide date and time verification through a time certification authority.	Release 2; Must
3.2.4.6.2.5.3.2	The system shall be flexible enough to provide date and time verification through a network time server.	Release 2; Must

3.2.4.6.2.5.3.3	The system shall be flexible enough to provide date and time verification through the signer's system.	Release 2; Must

3.2.4.6.2.6	**Authentication - Integrity Marks**	
3.2.4.6.2.6.1	The system shall support the use of integrity marks.	Release 2; Must
3.2.4.6.2.6.2	Integrity marks shall include certification information.	Release 2; Must
3.2.4.6.2.6.3	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).	Release 2; Must
3.2.4.6.2.6.4	The system shall support the capability to manually add integrity marks to content.	Release 2; Could
3.2.4.6.2.6.5	The system shall support the capability to automatically add integrity marks to content.	Release 2; Must
3.2.4.6.2.6.6	The system shall support the use of visible integrity marks.	Release 2; Must
3.2.4.6.2.6.7	The system shall support the use of invisible integrity marks.	Release 1C; Could / Release 2; Must
3.2.4.6.2.6.8	The system shall provide flexibility regarding where the integrity mark is applied through automated and manual processes.	Release 2; Must
3.2.4.6.2.6.8.1	The system shall provide flexibility regarding where the integrity mark is applied through automated processes.	Release 2; Must
3.2.4.6.2.6.8.2	The system shall provide flexibility regarding where the integrity mark is applied through manual processes.	Release 2; Must
3.2.4.6.2.6.9	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.	Release 2; Must
3.2.4.6.2.6.10	The system shall support the application of multiple integrity marks on the same content.	Release 2; Must
3.2.4.6.2.6.11	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.	Release 2; Must

3.2.4.6.2.7	**Authentication - Content Delivery**	
3.2.4.6.2.7.1	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.	Release 2; Must
3.2.4.6.2.7.1.1	The system shall provide the capability for users to validate the authenticity of the content packages that are delivered from the system.	Release 2; Must
3.2.4.6.2.7.1.2	The system shall provide the capability for users to validate the integrity of the content packages that are delivered from the system.	Release 2; Must

3.2.4.6.2.7.1.3	The system shall provide the capability for users to validate the official status of the content packages that are delivered from the system.	Release 2; Must
3.2.4.6.2.7.2	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.	Release 2; Must
3.2.4.6.2.7.2.1	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of electronic presentation.	Release 2; Must
3.2.4.6.2.7.2.2	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.	Release 2; Must
3.2.4.6.2.7.2.3	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of digital media.	Release 2; Must
3.2.4.6.2.7.2.4	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.	Release 1C; Must
3.2.4.6.2.7.2.5	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.	Release 1C; Must
3.2.4.6.2.7.3	Where public key cryptography and digital certificates are used to create a digital signature integrity mark on delivered content the following shall apply:	Release 2; Must
3.2.4.6.2.7.3.1	The integrity mark shall provide the capability to include the GPO Seal of Authenticity logo if the digital signature is a visible digital signature.	Release 2; Could
3.2.4.6.2.7.3.2	The integrity mark shall include certification information.	Release 2; Must
3.2.4.6.2.7.3.2.1	The integrity mark shall include the name of the certifying organization.	Release 2; Must
3.2.4.6.2.7.3.2.2	The integrity mark shall include the date on the signer's digital certificate.	Release 2; Must
3.2.4.6.2.7.3.2.3	The integrity mark shall include the digital time stamp.	Release 2; Must
3.2.4.6.2.7.3.2.4	The integrity mark shall include the public key value of the signer.	Release 2; Must
3.2.4.6.2.7.3.2.5	The integrity mark shall include identification of the hash algorithm used.	Release 2; Must
3.2.4.6.2.7.3.2.6	The integrity mark shall include the reason for signing.	Release 2; Must
3.2.4.6.2.7.3.2.7	The integrity mark shall include the signer's location.	Release 2; Must
3.2.4.6.2.7.3.2.8	The integrity mark shall include the signer's contact information.	Release 2; Must
3.2.4.6.2.7.3.2.9	The integrity mark shall include the name of the entity that certified the content.	Release 2; Must
3.2.4.6.2.7.3.2.10	The integrity mark shall include the expiration date of the digital certificate used to sign the content.	Release 2; Must

3.2.4.6.2.7.3.2.11	The integrity mark shall be flexible enough to include additional, GPO-defined certification information.	Release 2; Must
3.2.4.6.2.7.3.3	The values for the integrity mark fields shall be extracted from the digital certificate that was used to create the digital signature.	Release 2; Must
3.2.4.6.2.7.3.4	The system shall provide the flexibility to add new fields to the integrity mark.	Release 2; Must
3.2.4.6.2.7.3.5	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.	Release 2; Must
3.2.4.6.2.7.3.5.1	The system shall have the capability to confirm that the digital certificate that was used to create the digital signature is valid and accurate.	Release 2; Must
3.2.4.6.2.7.3.5.2	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.	Release 2; Must
3.2.4.6.2.7.3.6	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.	Release 2; Must
3.2.4.6.2.7.3.6.1	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.	Release 2; Must
3.2.4.6.2.7.3.6.2	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.	Release 2; Must
3.2.4.6.2.7.3.7	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.	Release 2; Must
3.2.4.6.2.7.3.7.1	The digital signature shall include the date and time that the digital signature was applied to content.	Release 2; Must
3.2.4.6.2.7.3.7.2	The digital signature shall include the expiration date of the digital certificate.	Release 2; Must
3.2.4.6.2.7.3.8	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.	Release 1C; Should / Release 2; Must
3.2.4.6.2.7.3.8.1	Non-revoked certificates shall display a valid status regardless of the expiration date of the digital certificate.	Release 1C; Should / Release 2; Must
3.2.4.6.2.7.3.8.2	The validity of the digital certificate shall be based on the certificate validity at the time and date the content was digitally signed.	Release 1C; Should / Release 2; Must

3.2.4.6.2.7.3.9	For electronic presentation, validation shall be done automatically without End User intervention.	Release 1C; Should / Release 2; Must

3.2.4.6.2.8	**Re-authentication of Content**	
3.2.4.6.2.8.1	The system shall provide the capability to re-authenticate content that has already been authenticated (e.g., expired certificate).	Release 1B; Could / Release 2; Must
3.2.4.6.2.8.2	The system shall provide the capability to notify GPO System Administrators when content needs to be re-authenticated.	Release 1B; Could / Release 2; Must
3.2.4.6.2.8.3	The system shall provide the capability for GPO to change or revoke the authentication status of content.	Release 1B; Must

3.2.4.6.2.9	**Authentication Standards/Best Practices**	
3.2.4.6.2.9.1	Deleted.	
3.2.4.6.2.9.2	Deleted.	
3.2.4.6.2.9.3	Deleted.	
3.2.4.6.2.9.4	Deleted.	
3.2.4.6.2.9.5	Deleted.	
3.2.4.6.2.9.6	Deleted.	
3.2.4.6.2.9.7	Deleted.	
3.2.4.6.2.9.7.1	Deleted.	
3.2.4.6.2.9.8	Deleted.	
3.2.4.6.2.9.9	Deleted.	
3.2.4.6.2.9.10	Deleted.	
3.2.4.6.2.9.11	Deleted.	
3.2.4.6.2.9.12	Deleted.	
3.2.4.6.2.9.13	Deleted.	
3.2.4.6.2.9.14	Deleted.	
3.2.4.6.2.9.15	Deleted.	
3.2.4.6.2.9.16	Deleted.	
3.2.4.6.2.9.17	Deleted.	
3.2.4.6.2.9.18	Deleted.	
3.2.4.6.2.9.19	Deleted.	
3.2.4.6.2.9.20	Deleted.	

3.2.4.6.2.10	**Authentication Records Management**	
3.2.4.6.2.10.1	The system shall create administrative records of authentication processes.	Release 2; Must
3.2.4.6.2.10.2	The system shall create transaction records of administrative processes.	Release 2; Must
3.2.4.6.2.10.3	The system shall support an audit capability for content certification.	Release 2; Must

3.2.4.6.2.10.4	The system shall support an audit capability for content validation.	Release 2; Must
3.2.4.6.2.10.5	The system shall comply with GPO and Federal records management policies.	Release 2; Must
3.2.4.6.2.10.5.1	The system shall comply with GPO records management policies, as document in GPO Publication 840.7.	Release 2; Must
3.2.4.6.2.10.5.2	The system shall comply with Federal records management policies (e.g., NARA's Records Management Guidance for Agencies Implementing Electronic Signature Technologies, 2000).	Release 2; Must

3.2.4.6.2.11	**Authentication Metadata**	
3.2.4.6.2.11.1	The system shall provide the capability to include authentication and certification information in metadata.	Release 2; Must
3.2.4.6.2.11.1.1	The system shall provide the capability to include authenticity information in metadata.	Release 2; Must
3.2.4.6.2.11.1.1.1	Authenticity metadata shall have the capability to include the source of deposited, harvested, and converted content.	Release 2; Must
3.2.4.6.2.11.1.1.2	Authenticity metadata shall have the capability to include the Content Originator identity and authority to publish deposited content.	Release 2; Must
3.2.4.6.2.11.1.1.3	Authenticity metadata shall have the capability to include the source of tangible content that was used to create converted content.	Release 2; Must
3.2.4.6.2.11.1.1.4	Authenticity metadata shall have the capability to include the chain of custody information excluding information about End User chain of custody.	Release 2; Must
3.2.4.6.2.11.1.2	The system shall provide the capability to include integrity information in metadata.	Release 2; Must
3.2.4.6.2.11.1.2.1	Integrity metadata shall have the capability to include information about any pre-ingest and ingest integrity checks for transmission to the system.	Release 2; Must
3.2.4.6.2.11.1.2.2	Integrity metadata shall have the capability to include information about any integrity checks within the system.	Release 2; Must
3.2.4.6.2.11.1.2.3	Integrity metadata shall have the capability to include information about changes that are made.	Release 2; Must
3.2.4.6.2.11.1.2.4	Integrity metadata shall have the capability to include information about who makes a change.	Release 2; Must
3.2.4.6.2.11.1.2.5	Integrity metadata shall have the capability to include information about where a change is made.	Release 2; Must
3.2.4.6.2.11.1.2.6	Integrity metadata shall have the capability to include information about when a change is made.	Release 2; Must
3.2.4.6.2.11.1.3	The system shall provide the capability to include non-repudiation information in metadata.	Release 2; Must
3.2.4.6.2.11.1.3.1	Non-repudiation metadata shall have the capability to include the sender's identity and proof.	Release 2; Must

3.2.4.6.2.11.1.3.2	Non-repudiation metadata shall have the capability to include the recipient's identity and proof.	Release 2; Must
3.2.4.6.2.11.1.4	The system shall provide the capability to include intended use information in metadata.	Release 2; Must
3.2.4.6.2.11.1.4.1	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.	Release 2; Must
3.2.4.6.2.11.1.4.2	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.	Release 2; Must
3.2.4.6.2.11.1.4.3	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.	Release 2; Must

3.2.4.7.2	Requirements for Version Control	
3.2.4.7.2.1	**Version Control Core Capabilities**	
3.2.4.7.2.1.1	Deleted.	
3.2.4.7.2.1.1.1	Deleted.	
3.2.4.7.2.1.2	Deleted.	
3.2.4.7.2.1.2.1	Deleted.	
3.2.4.7.2.1.3	The system shall allow authorized users to input, view, and manage version information.	Release 1C; Must
3.2.4.7.2.1.3.1	The system shall allow authorized users to input, view, and manage version information.	Release 1C; Must
3.2.4.7.2.1.3.1.1	The system shall allow authorized users to input version information.	Release 1C; Must
3.2.4.7.2.1.3.1.2	The system shall allow authorized users to view version information.	Release 1C; Must
3.2.4.7.2.1.3.1.3	The system shall allow authorized users to manage version information.	Release 1C; Must
3.2.4.7.2.1.3.2	The system shall allow authorized users to input, view, and manage version identifiers.	Release 1C; Must
3.2.4.7.2.1.3.2.1	The system shall allow authorized users to input version identifiers.	Release 1C; Must
3.2.4.7.2.1.3.2.2	The system shall allow authorized users to view version identifiers.	Release 1C; Must
3.2.4.7.2.1.3.2.3	The system shall allow authorized users to manage version identifiers.	Release 1C; Must
3.2.4.7.2.1.4	The system shall have the capability to alert authorized users when duplicate content is rejected.	Release 1C; Should / Release 2; Must
3.2.4.7.2.1.5	The system shall log all version history.	Release 2; Must
3.2.4.7.2.1.5.1	The version history log shall be incorporated into the package's metadata.	Release 2; Must
3.2.4.7.2.1.6	The system shall provide the capability to apply version control to work in progress content.	Release 1B; Could / Release 1C; Should / Release 2; Must

3.2.4.7.2.1.6.1	The system shall provide the capability to maintain configuration control of content in a WIP.	Release 1B; Could / Release 1C; Should / Release 2; Must
3.2.4.7.2.1.6.2	The system shall provide the capability to maintain configuration control of metadata in a WIP.	Release 1B; Could / Release 1C; Should / Release 2; Must
3.2.4.7.2.1.6.3	The system shall provide the capability to maintain configuration control of BPI in a WIP.	Release 1B; Could / Release 1C; Should / Release 2; Must

3.2.4.7.2.2	**Version Triggers**	
3.2.4.7.2.2.1	The system shall apply rules for version triggers.	Release 2; Must
3.2.4.7.2.2.1.1	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.	Release 2; Must
3.2.4.7.2.2.1.2	Authorized users shall be able to modify rules for version triggers.	Release 2; Must
3.2.4.7.2.2.2	The system shall detect the following version triggers.	Release 2; Must
3.2.4.7.2.2.2.1	Modifications to content	Release 2; Must
3.2.4.7.2.2.2.2	Changes to the “last updated” date provided within the document	Release 2; Must
3.2.4.7.2.2.2.3	Changes to a flat date provided within the document	Release 2; Must
3.2.4.7.2.2.2.4	Changes to a publication’s title	Release 2; Must
3.2.4.7.2.2.2.5	Changes to a publication’s edition statement and/or metadata	Release 2; Must
3.2.4.7.2.2.2.6	Changes in the issuing agency of a publication	Release 2; Must
3.2.4.7.2.2.2.7	Changes in file size or format	Release 2; Must
3.2.4.7.2.2.2.8	Changes in the publication’s numbering scheme	Release 2; Must
3.2.4.7.2.2.2.9	Notification of the publisher (i.e., issuing agency)	Release 2; Must
3.2.4.7.2.2.3	The system shall provide the capability to notify users when version triggers have been activated.	Release 2; Must
3.2.4.7.2.2.3.1	Deleted.	
3.2.4.7.2.2.4	The system shall provide the capability to notify designated authorized users when a version cannot be determined.	Release 2; Must

3.2.4.7.2.3	**Version Detection**	
3.2.4.7.2.3.1	The system shall determine if version identifiers are present in content packages.	Release 2; Must
3.2.4.7.2.3.1.1	Version identifiers shall be stored in metadata.	Release 1C; Must

3.2.4.7.2.4	**Version Metadata**	
3.2.4.7.2.4.1	The system shall express version information in metadata.	Release 1C; Must
3.2.4.7.2.4.1.1	The system shall update the metadata to indicate changes to attributes.	Release 1C; Must
3.2.4.7.2.4.2	The system shall record chain of custody information in metadata .	Release 1C; Must

3.2.4.7.2.5	**Version Relationships**	
3.2.4.7.2.5.1	The system shall determine and record relationships between versions.	Release 2; Must
3.2.4.7.2.5.1.1	The system shall establish links to related documents identified through version information in metadata.	Release 2; Must
3.2.4.7.2.5.1.2	The system shall make links to related documents permanently available.	Release 2; Must
3.2.4.7.2.5.1.3	The system shall be able to render relationship information so that it is human-readable.	Release 2; Must

3.2.4.7.2.6	**Version Notification**	
3.2.4.7.2.6.1	The system shall have the capability to notify users which version of content they are accessing.	Release 2; Must
3.2.4.7.2.6.1.1	The system shall have the capability to notify users of the number of available versions of selected content.	Release 2; Must
3.2.4.7.2.6.1.2	The system shall have the capability to notify users that they are not viewing the latest available version of selected content.	Release 2; Must
3.2.4.7.2.6.1.3	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.	Release 2; Must
3.2.4.7.2.6.1.4	The system shall have the capability for users to view the difference in the content between versions.	Release 3; Must
3.2.4.7.2.6.1.5	The system shall have the capability to notify users that access to a version is restricted.	Release 2; Must

3.2.5.1.2	**Requirements for Workflow**	
3.2.5.1.2.1	**Workflow Core Capabilities**	
3.2.5.1.2.1.1	The system shall provide the capability to define workflows.	Release 1B; Must
3.2.5.1.2.1.1.1	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.	Release 1B; Must
3.2.5.1.2.1.1.2	The system shall provide the capability to validate workflow definitions against the established schema.	Release 1B; Must
3.2.5.1.2.1.2	The system shall provide the capability to create new versions of workflow definitions.	Release 1B; Must
3.2.5.1.2.1.3	The system shall provide the capability to test new versions of workflow definitions without interfering with any existing workflow instances.	Release 1B; Must
3.2.5.1.2.1.4	The system shall provide the capability to place new versions of workflow definitions into production.	Release 1B; Must

3.2.5.1.2.1.4.1	The system shall provide the capability to deploy newly developed or modified workflow definitions without interfering with existing workflow instances.	Release 1B; Must
3.2.5.1.2.1.5	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.	Release 1B; Must
3.2.5.1.2.1.5.1	The system shall provide the capability to revert to previous workflow definitions without interfering with existing workflow instances.	Release 1B; Must
3.2.5.1.2.1.5.2	The system shall provide the capability to revert to previous workflow definitions without interfering with other non-completed instances of workflows.	Release 1B; Must
3.2.5.1.2.1.6	The system shall provide the capability to manage business rules.	Release 1B; Must
3.2.5.1.2.1.6.1	The workflow-related business rules shall be configurable by the user to control the order in which the rules are applied.	Release 2; Must
3.2.5.1.2.1.7	The system shall provide the capability to manage manual activities.	Release 1B; Must
3.2.5.1.2.1.8	The system shall provide the capability to manage automated activities.	Release 2; Must
3.2.5.1.2.1.9	The system shall provide the capability to assign comments on jobs/activities.	Release 1B; Must
3.2.5.1.2.1.9.1	The system shall provide the capability to assign optional comments on jobs.	Release 1B; Must
3.2.5.1.2.1.9.2	The system shall provide the capability to assign optional comments on activities.	Release 1B; Must
3.2.5.1.2.1.9.3	The system shall provide the capability to assign optional comments on workflow instances.	Release 1B; Must
3.2.5.1.2.1.10	The system shall prevent the loss of workflow data.	Release 1B; Must
3.2.5.1.2.1.10.1	The system shall replicate workflow data to failover location(s).	Release 1C; Must
3.2.5.1.2.1.10.2	The system shall allow the frequency of backup processes to be controlled by the user.	Release 1C; Must
3.2.5.1.2.1.10.2.1	The system shall allow the backup processes to be controlled automatically or manually.	Release 2; Must
3.2.5.1.2.1.10.3	The system shall backup all necessary data required to retrieve workflow data to its original state in the event of a system failure.	Release 1C; Must
3.2.5.1.2.1.10.4	The system shall perform workflow backup processes without interruption to users.	Release 1C; Must
3.2.5.1.2.1.11	The system shall store information related to workflows in BPI.	Release 1B; Must
3.2.5.1.2.1.11.1	The system shall store information about workflows in BPI.	Release 1B; Must
3.2.5.1.2.1.11.2	The system shall store information about jobs in BPI.	Release 1B; Must
3.2.5.1.2.1.11.3	The system shall store information about activities in BPI.	Release 1B; Must

3.2.5.1.2.2	**Workflow - Control of Execution**	
3.2.5.1.2.2.1	The system shall provide the capability to control the execution of workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.1	The system shall provide the capability to assign priorities to workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.2	The system shall provide the capability to schedule for manual and automated activities.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.2.1.2.1	The system shall provide the capability to assign deadlines for jobs/activities.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.2.1.2.1.1	The system shall provide the capability to assign deadlines for jobs.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.2.1.2.1.2	The system shall provide the capability to assign deadlines for activities.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.2.1.2.2	The system shall provide the capability to assign estimated completion times for jobs/activities.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.2.1.2.2.1	The system shall provide the capability to assign estimated completion times for jobs.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.2.1.2.2.2	The system shall provide the capability to assign estimated completion times for activities.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.2.1.3	The system shall provide the capability to assign human resources to manual activities.	Release 1C; Could
3.2.5.1.2.2.1.4	The system shall provide the capability to suspend activities/workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.4.1	The system shall provide the capability to suspend activities.	Release 1B; Must
3.2.5.1.2.2.1.4.2	The system shall provide the capability to suspend workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.5	The system shall provide the capability to resume activities/workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.5.1	The system shall provide the capability to resume activities.	Release 1B; Must
3.2.5.1.2.2.1.5.2	The system shall provide the capability to resume workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.6	The system shall provide the capability to cancel activities/workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.6.1	The system shall provide the capability to cancel activities.	Release 1B; Must
3.2.5.1.2.2.1.6.2	The system shall provide the capability to cancel workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.7	The system shall provide the capability to log activities.	Release 1B; Must
3.2.5.1.2.2.1.7.1	The system shall provide the capability to log activity start time.	Release 1B; Must
3.2.5.1.2.2.1.7.2	The system shall provide the capability to log activity end time.	Release 1B; Must
3.2.5.1.2.2.1.7.3	The system shall provide the capability to log the person(s) performing the activity.	Release 1B; Must
3.2.5.1.2.2.1.7.4	The system shall provide the capability to log the resources associated with an activity .	Release 1B; Must

3.2.5.1.2.2.1.8	The system shall provide the capability to manage lists of workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.8.1	The system shall provide the capability for a user to view lists of workflow instances.	Release 1B; Must
3.2.5.1.2.2.1.8.2	The system shall provide the capability for a user to assign lists of workflow instances to other users.	Release 1B; Must
3.2.5.1.2.2.1.9	The system shall provide the capability to perform actions on a batch of workflow instances.	Release 2; Must
3.2.5.1.2.2.2	The system shall provide the capability to control the execution of jobs.	Release 1B; Must
3.2.5.1.2.2.2.1	The system shall provide the capability to assign priorities to jobs.	Release 1C; Should
3.2.5.1.2.2.2.1.1	The priority of a job shall be inherited by workflow instances associated with the job.	Release 1C; Should
3.2.5.1.2.2.2.2	The system shall provide the capability to suspend and resume jobs.	Release 1B; Must
3.2.5.1.2.2.2.2.1	The system shall provide the capability to suspend jobs.	Release 1B; Must
3.2.5.1.2.2.2.2.2	The system shall provide the capability to resume jobs.	Release 1B; Must
3.2.5.1.2.2.2.3	The system shall provide the capability to cancel a job.	Release 1B; Must
3.2.5.1.2.2.2.4	The system shall provide the capability to adjust the priority of a job at any time.	Release 2; Must
3.2.5.1.2.2.2.4.1	The system shall provide the capability to adjust the priority of a job manually or automatically.	Release 2; Must
3.2.5.1.2.2.2.5	The system shall provide the capability to log jobs.	Release 1B; Must
3.2.5.1.2.2.2.6	The system shall provide the capability to manage work lists of jobs.	Release 1B; Must
3.2.5.1.2.2.2.7	The system shall provide the capability to perform actions on a batch of jobs.	Release 2; Must

3.2.5.1.2.3	**Workflow - Monitoring**	
3.2.5.1.2.3.1	The system shall provide a monitoring tool for all workflow instances.	Release 1B; Must
3.2.5.1.2.3.1.1	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.	Release 1C; Must
3.2.5.1.2.3.1.1.1	The monitoring tool shall provide the capability to see how many instances of a workflow exist.	Release 1C; Must
3.2.5.1.2.3.1.1.2	The monitoring tool shall provide the capability to see the status of the workflow instances.	Release 1C; Must
3.2.5.1.2.3.1.2	The monitoring tool shall provide the capability for the user to customize views.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.3.1.3	The monitoring tool shall provide the capability to save customized views for future use.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.3.1.4	The monitoring tool shall provide the capability for users to monitor processing history of workflow instances.	Release 1B; Must

3.2.5.1.2.3.1.4.1	The monitoring tool shall provide the capability for users to monitor processing history over a specified time period.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.3.1.5	The monitoring tool shall report throughput, delay, load, and additional performance measures in the future.	Release 2; Must
3.2.5.1.2.3.1.5.1	The monitoring tool shall report the throughput for workflow instances.	Release 1C; Must
3.2.5.1.2.3.1.5.2	The monitoring tool shall report any delays for workflow instances.	Release 1C; Must
3.2.5.1.2.3.1.5.3	The monitoring tool shall report the loads for workflow instances.	Release 1C; Must
3.2.5.1.2.3.1.5.4	The monitoring tool shall report additional performance measures in the future.	Release 2; Must
3.2.5.1.2.3.2	The system shall provide the capability for users to monitor jobs or a list of jobs.	Release 1B; Must
3.2.5.1.2.3.2.0.1	The system shall provide the capability for users to monitor jobs.	Release 1B; Must
3.2.5.1.2.3.2.0.2	The system shall provide the capability for users to monitor a list of jobs.	Release 1B; Must
3.2.5.1.2.3.2.1	The system shall provide the capability for users to monitor a batch of jobs.	Release 1B; Must
3.2.5.1.2.3.2.2	The system shall provide the capability to monitor planned, scheduled and actual times for selected jobs.	Release 2; Must
3.2.5.1.2.3.2.2.1	The system shall provide the capability to monitor planned times for selected jobs.	Release 2; Must
3.2.5.1.2.3.2.2.2	The system shall provide the capability to monitor scheduled times for selected jobs.	Release 2; Must
3.2.5.1.2.3.2.2.3	The system shall provide the capability to monitor actual times for selected jobs.	Release 2; Must
3.2.5.1.2.3.2.3	The system shall provide the capability to group jobs with a defined status.	Release 1B; Must
3.2.5.1.2.3.3	The system shall provide the capability for users to monitor workflow instances or a list of workflow instances.	Release 1B; Must
3.2.5.1.2.3.3.0.1	The system shall provide the capability for users to monitor workflow instances.	Release 1B; Must
3.2.5.1.2.3.3.0.2	The system shall provide the capability for users to monitor workflow instances or a list of workflow instances.	Release 1B; Must
3.2.5.1.2.3.3.1	The system shall provide the capability for users to monitor a batch of workflow instances.	Release 1B; Must
3.2.5.1.2.3.3.2	The system shall provide the capability to monitor planned, scheduled and actual times for selected workflow instances.	Release 2; Must
3.2.5.1.2.3.3.2.1	The system shall provide the capability to monitor planned times for selected workflow instances.	Release 2; Must
3.2.5.1.2.3.3.2.2	The system shall provide the capability to monitor scheduled times for selected workflow instances.	Release 2; Must

3.2.5.1.2.3.3.2.3	The system shall provide the capability to monitor actual times for selected workflow instances.	Release 2; Must
3.2.5.1.2.3.3.3	The system shall provide the capability to group workflow instances with a defined status.	Release 2; Must

3.2.5.1.2.4	**Workflow - Resource Requirements**	
3.2.5.1.2.4.1	The system shall provide the capability to estimate resource requirements associated with internal workflow.	Release 1B; Could / Release 1C; Must
3.2.5.1.2.4.2	The system shall provide the capability to estimate resource requirements associated with external workflow.	Release 1C; Could / Release 2; Must
3.2.5.1.2.4.3	The system shall provide the capability to estimate resource requirements for automated and manual activities.	Release 1C; Could / Release 2; Must
3.2.5.1.2.4.3.1	The system shall provide the capability to estimate resource requirements for automated activities.	Release 1C; Could / Release 2; Must
3.2.5.1.2.4.3.2	The system shall provide the capability to estimate resource requirements for manual activities.	Release 1C; Could / Release 2; Must

3.2.5.1.2.5	**Workflow - Notification**	
3.2.5.1.2.5.1	The system shall provide the capability to associate notifications with workflows.	Release 1B; Must
3.2.5.1.2.5.2	The system shall provide the capability to manage notifications attached to workflows.	Release 1B; Must
3.2.5.1.2.5.3	The system shall send notifications via e-mail, the user's screen, and additional methods in the future.	Release 2; Must
3.2.5.1.2.5.3.1	The system shall send notifications via e-mail.	Release 1B; Must
3.2.5.1.2.5.3.2	The system shall send notifications via the user’s screen.	Release 1B; Must
3.2.5.1.2.5.3.3	The system shall send notifications via additional methods in the future.	Release 2; Must
3.2.5.1.2.5.4	The system shall provide the capability to configure the list of recipients of notifications.	Release 1B; Must
3.2.5.1.2.5.5	The system shall provide the capability to escalate notifications.	Release 3; Should

3.2.5.1.2.6	**Workflow - Security**	
3.2.5.1.2.6.1	The system shall provide the capability to have security controls on workflow activities.	Release 1B; Must
3.2.5.1.2.6.1.1	The security control (allow or deny actions) shall be rule based.	Release 2; Must
3.2.5.1.2.6.1.2	Manual activities in the workflows shall be assigned with one or more security rules.	Release 2; Must

3.2.5.1.2.7	**Workflow - Interface**	

3.2.5.1.2.7.1	The system shall provide a Graphical User Interface (GUI) edit tool to manage workflow definitions and executions.	Release 1B; Must
3.2.5.1.2.7.2	The Monitoring Tool shall contain a GUI for all workflow monitoring capabilities.	Release 1B; Must

3.2.5.2.2	Requirements for Storage Management	
3.2.5.2.2.1	**Storage Core Capabilities**	
3.2.5.2.2.1.1	The system shall support retrieval of data from online storage at error rates of TBR.	Release 1B; Must
3.2.5.2.2.1.2	The system shall be capable of providing a secure repository environment for all storage.	Release 1C; Must
3.2.5.2.2.1.2.1	Near-line storage media shall preserve data integrity and quality for no less than 10 years in a data center environment.	Release 1C; Must
3.2.5.2.2.1.2.2	Each data center in the system shall be housed in a facility protected by physical security measures.	Release 1C; Must
3.2.5.2.2.1.2.3	Each data center in the system shall be protected from power failures for the time required to safely power down all system components.	Release 1C; Must
3.2.5.2.2.1.2.4	Each data center in the system shall be equipped with power failure sensors capable of notifying users when grid power has failed.	Release 1C; Must
3.2.5.2.2.1.2.5	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.	Release 1C; Must
3.2.5.2.2.1.2.6	Each data center in the system shall be equipped with environment sensors capable of notifying users when out of tolerance conditions are imminent.	Release 1C; Must
3.2.5.2.2.1.3	The system shall support the capability to include multiple storage classes.	Release 1C; Must
3.2.5.2.2.1.3.1	The system shall support the capability to add additional storage classes in the future without a major redesign.	Release 1C; Must
3.2.5.2.2.1.3.2	The system shall support the capability to transparently migrate data from one storage class to another based on system policies.	Release 1C; Must
3.2.5.2.2.1.3.3	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.	Release 1C; Must
3.2.5.2.2.1.3.4	The system shall support the capability for authorized users to set storage policies for selected content packages.	Release 1C; Must

3.2.5.2.2.2	**Content Delivery Network Storage**	
3.2.5.2.2.2.1	The system shall have the capability to store data dynamically in external Content Delivery Networks (CDN) based on hit rate/criticality of content.	Release 2; Must
3.2.5.2.2.2.1.0.1	The system shall support the capability for authorized users to designate data for storage in a Content Delivery Network.	Release 1C; Must
3.2.5.2.2.2.1.1	Deleted.	
3.2.5.2.2.2.1.2	Deleted.	
3.2.5.2.2.2.2	The system shall have the capability to utilize external storage Service Providers.	Release 1C; Must
3.2.5.2.2.2.3	Deleted.	
3.2.5.2.2.2.4	Deleted.	
3.2.5.2.2.2.5	Deleted.	
3.2.5.2.2.2.6	Deleted.	
3.2.5.2.2.2.7	Deleted.	
3.2.5.2.2.2.7.1	Deleted.	
3.2.5.2.2.2.8	Deleted.	
3.2.5.2.2.2.8.1	Deleted.	
3.2.5.2.2.2.9	Deleted.	

3.2.5.2.2.3	**Networked Moderate Performance Storage**	
3.2.5.2.2.3.1	Deleted.	
3.2.5.2.2.3.2	Deleted.	
3.2.5.2.2.3.3	Deleted.	
3.2.5.2.2.3.4	Deleted.	
3.2.5.2.2.3.5	Deleted.	

3.2.5.2.2.4	**Low Criticality- Low Cost Storage**	
3.2.5.2.2.4.1	Deleted.	
3.2.5.2.2.4.2	Deleted.	
3.2.5.2.2.4.3	Deleted.	
3.2.5.2.2.4.4	Deleted.	
3.2.5.2.2.4.5	Deleted.	

3.2.5.2.2.5	**Failover Storage**	
3.2.5.2.2.5.1	Failover Storage shall provide the fault tolerance required to allow the system to survive a localized disaster.	Release 1C; Must
3.2.5.2.2.5.2	Failover Storage shall be able to reconstitute and switch-over to alternate systems at a remote site in the event of local catastrophic damage.	Release 1C; Must
3.2.5.2.2.5.2.0.1	The system shall replicate all system data to a disaster recovery site.	Release 1C; Must

3.2.5.2.2.5.2.1	Failover Storage shall allow the switchover to redundant components via either user action or automatic in case of failure.	Release 1C; Must
3.2.5.2.2.5.2.1.1	Failover Storage shall allow the switchover to redundant components via user action.	Release 1C; Must
3.2.5.2.2.5.2.1.2	Failover Storage shall allow the switchover to redundant components automatically in case of failure.	Release 1C; Must
3.2.5.2.2.5.2.2	The system shall replicate all content packages to a disaster recovery site.	Release 1C; Must
3.2.5.2.2.5.2.3	The system shall replicate all BPI to a disaster recovery site.	Release 1C; Must
3.2.5.2.2.5.2.4	In the event of a disaster, a complete switchover shall be complete within 15 minutes of initiation. (TBS)	Release 1C; Must
3.2.5.2.2.5.3	Deleted.	
3.2.5.2.2.5.4	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).	Release 1C; Must

3.2.5.2.2.6	**Backup Retrieval Media Storage**	
3.2.5.2.2.6.1	Back-up Retrieval Media Storage shall be able to accomplish periodic backup on mass removable storage media.	Release 1B; Must
3.2.5.2.2.6.1.1	Back-up Retrieval Media Storage shall allow users to manage periodic backup schedules.	Release 1B; Must
3.2.5.2.2.6.1.2	Back-up Retrieval Media Storage shall allow backups on multiple types of mass removable storage media.	Release 1C; Must
3.2.5.2.2.6.2	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.	Release 1B; Must
3.2.5.2.2.6.2.1	Back-up Retrieval Media Storage shall allow users to manage which data is listed as critical.	Release 1C; Must
3.2.5.2.2.6.2.2	Back-up Retrieval Media Storage shall allow users to manage the backup schedule.	Release 1B; Must
3.2.5.2.2.6.2.3	Back-up Retrieval Media Storage shall not interfere with current system processes.	Release 1B; Must
3.2.5.2.2.6.3	Deleted.	
3.2.5.2.2.6.4	Back-up Retrieval Media Storage shall support mirroring the write data in cache as a method of data protection.	Release 1C; Must
3.2.5.2.2.6.4.1	Back-up Retrieval Media Storage shall allow users to manage which data should be backed up.	Release 1C; Must
3.2.5.2.2.6.5	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.	Release 3; Must

3.2.5.2.2.6.5.1	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.	Release 3; Must
3.2.5.2.2.6.6	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.	Release 1C; Must

3.2.5.2.2.7	**Mid-term Archival Storage**	
3.2.5.2.2.7.1	Deleted.	
3.2.5.2.2.7.2	Deleted.	

3.2.5.2.2.8	**Long-term Permanent Archival Storage**	
3.2.5.2.2.8.1	Long-term Permanent Archival Storage shall have off-line storage and indexing capability for multiple Petabytes of data.	Release 1C; Must
3.2.5.2.2.8.2	Long-term Permanent Archival Storage shall have a remote storage site over 600 miles from the main GPO facility.	Release 1C; Must
3.2.5.2.2.8.3	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., 70° F, 60% Humidity).	Release 3; Must

3.2.5.2.2.9	**Functional Data Storage**	
3.2.5.2.2.9.1	Work In Progress (WIP) Storage	Release 1C; Must
3.2.5.2.2.9.1.0.1	The average access time for WIPs shall be 2 seconds or less.	Release 1C; Must
3.2.5.2.2.9.1.0.2	WIPs shall be protected from unauthorized alteration by user actions.	Release 1C; Must
3.2.5.2.2.9.1.1	Deleted.	
3.2.5.2.2.9.1.2	Deleted.	
3.2.5.2.2.9.1.3	Deleted.	
3.2.5.2.2.9.1.4	Deleted.	
3.2.5.2.2.9.1.5	WIP Storage shall contain both content and metadata.	Release 1C; Must
3.2.5.2.2.9.2	Archival Information Package (AIP) Storage	Release 1C; Must
3.2.5.2.2.9.2.0.1	The system shall write all AIPs to archival media for off site storage.	Release 1C; Must
3.2.5.2.2.9.2.0.2	The average access time for SIPs after submission to the system shall be 2 seconds or less.	Release 1C; Must
3.2.5.2.2.9.2.0.3	The average access time for AIPs stored in on line storage shall be 2 seconds or less.	Release 1C; Must
3.2.5.2.2.9.2.0.4	The average access time for AIPs stored in near line storage shall be 24 hours (TBS) or less.	Release 1C; Must
3.2.5.2.2.9.2.0.5	SIPs shall be protected from unauthorized alteration by user actions.	Release 1C; Must

3.2.5.2.2.9.2.0.6	AIPs shall be protected from unauthorized alteration by user actions.	Release 1C; Must
3.2.5.2.2.9.2.1	Deleted.	
3.2.5.2.2.9.2.2	Deleted.	
3.2.5.2.2.9.2.3	Deleted.	
3.2.5.2.2.9.2.4	Deleted.	
3.2.5.2.2.9.2.5	AIP Storage shall exist in isolation of other system stores.	Release 1C; Must
3.2.5.2.2.9.2.6	The system shall support the capability to migrate AIP content to future storage technologies.	Release 1C; Must
3.2.5.2.2.9.2.7	AIP Storage shall contain both content and metadata.	Release 1C; Must
3.2.5.2.2.9.3	Access Content Storage (ACS)	Release 1C; Must
3.2.5.2.2.9.3.0.1	The average access time for ACPs shall be 2 seconds or less.	Release 1C; Must
3.2.5.2.2.9.3.0.2	ACPs shall be protected from unauthorized alteration by user actions.	Release 1C; Must
3.2.5.2.2.9.3.1	Deleted.	
3.2.5.2.2.9.3.2	Deleted.	
3.2.5.2.2.9.3.3	Deleted.	
3.2.5.2.2.9.3.4	Deleted.	
3.2.5.2.2.9.3.5	Deleted.	
3.2.5.2.2.9.3.6	Deleted.	
3.2.5.2.2.9.3.7	Deleted.	
3.2.5.2.2.9.3.8	ACS shall contain both content and metadata.	Release 1C; Must
3.2.5.2.2.9.4	Business Process information (BPI) Storage.	Release 1C; Must
3.2.5.2.2.9.4.0.1	The average access time for BPI shall be 2 seconds or less.	Release 1C; Must
3.2.5.2.2.9.4.0.2	BPI shall be protected from unauthorized alteration by user actions.	Release 1C; Must
3.2.5.2.2.9.4.1	Deleted.	
3.2.5.2.2.9.4.2	Deleted.	
3.2.5.2.2.9.4.3	Deleted.	
3.2.5.2.2.9.4.4	Deleted.	
3.2.5.2.2.9.4.5	Deleted.	
3.2.5.2.2.9.4.6	BPS shall contain Failover Storage.	Release 1C; Must
3.2.5.2.2.9.4.7	Deleted.	

3.2.5.2.2.10	**Storage System Standards**	
3.2.5.2.2.10.1	The system shall integrate with Unix and Windows based Directory Services (Lightweight Directory Access Protocol, Active Directory), and role based access.	Release 1B; Must
3.2.5.2.2.10.1.1	The system shall integrate with Lightweight Directory Access Protocol (LDAP).	Release 1B; Must

3.2.5.2.2.10.1.2	The system shall control access to data in storage based on the user's role.	Release 1C; Must
3.2.5.2.2.10.1.3	The system shall prefer the use of Lightweight Directory Access Protocol over Active Directory wherever possible.	Release 1C; Must
3.2.5.2.2.10.2	The system shall be able to ingest files stored on disk systems connected directly to the system.	Release 2; Must
3.2.5.2.2.10.2.1	The system shall provide the capability to read files stored in common operating system formats.	Release 2; Must
3.2.5.2.2.10.2.1.1	The system shall be able to ingest files stored in a FAT filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.2	The system shall be able to ingest files stored in a FAT32 filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.3	The system shall be able to ingest files stored in a VFAT filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.4	The system shall be able to ingest files stored in a NTFS filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.5	The system shall be able to ingest files stored in a HPFS filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.6	The system shall be able to ingest files stored in a EXT2 filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.7	The system shall be able to ingest files stored in a EXT3 filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.8	The system shall be able to ingest files stored in a EXT4 filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.9	The system shall be able to ingest files stored in a HFS Plus filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.10	The system shall be able to ingest files stored in a JFS2 filesystem.	Release 2; Must
3.2.5.2.2.10.2.1.11	The system shall be able to ingest files stored in a UFS filesystem.	Release 2; Must
3.2.5.2.2.10.3	The system shall utilize common Redundant Array of Independent Disks (RAID) Disk Data Format (DDF) architecture.	Release 1C; Must
3.2.5.2.2.10.4	The system shall conform to commonly used, industry standard protocols.	Release 2; Must
3.2.5.2.2.10.4.1	The system shall support the capability to interface with industry standard protocols.	Release 2; Must
3.2.5.2.2.10.4.2	The system shall use industry standard protocols when there is one that meets the system requirements.	Release 2; Must
3.2.5.2.2.10.4.3	The system shall use of non-standard protocols only when there is no industry standard that meets the system requirements.	Release 2; Must
3.2.5.2.2.10.5	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.	Release 1C; Must
3.2.5.2.2.10.5.1	The system shall allow interaction with management information bases (MIB) via SNMP.	Release 1C; Must

3.2.5.2.2.10.5.2	The system shall conform to or interoperate within Object-based Storage Device (OSD) specification.	Release 1C; Must
3.2.5.2.2.10.6	The system storage shall support ANSI INCITS 388-2004 Storage Management Initiative Specification.	Release 2; Must
3.2.5.2.2.10.7	The system back-up tapes shall conform to Linear Tape-Open (LTO) standard.	Release 1C; Must

3.2.5.2.2.11	**Storage - Monitoring**	
3.2.5.2.2.11.1	The system shall provide the capability to monitor the health of system components in real time.	Release 1C; Must
3.2.5.2.2.11.1.1	The system shall monitor the health of the network components in real-time.	Release 1C; Must
3.2.5.2.2.11.1.2	The system shall monitor the health of the system applications in real-time.	Release 1C; Must
3.2.5.2.2.11.1.3	The system shall monitor the health of the storage components in real-time.	Release 1C; Must
3.2.5.2.2.11.1.4	The system monitor the health of the processing components in real-time.	Release 1C; Must
3.2.5.2.2.11.1.5	The system shall monitor the health of the operating system in real-time.	Release 1C; Must
3.2.5.2.2.11.2	The system shall provide the capability for the user to configure the upper and lower bounds for system parameters being monitored.	Release 1C; Must
3.2.5.2.2.11.3	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.	Release 1C; Must
3.2.5.2.2.11.3.0.1	The system shall send a notification to users when a performance problem is detected.	Release 1C; Must
3.2.5.2.2.11.3.0.2	The system shall send a notification to users when a failure condition is detected.	Release 1C; Must
3.2.5.2.2.11.3.0.3	The system shall send a notification to users when a failure is impending.	Release 1C; Must
3.2.5.2.2.11.3.1	The system shall send notifications to appropriate user screen, e-mail, and via additional methods in the future.	Release 2; Must
3.2.5.2.2.11.3.1.1	The system shall send notifications to the appropriate user screen.	Release 1C; Must
3.2.5.2.2.11.3.1.2	The system shall send notifications to the appropriate e-mail.	Release 1C; Must
3.2.5.2.2.11.3.1.3	The system shall send notifications via additional methods in the future.	Release 2; Must
3.2.5.2.2.11.3.2	The system shall allow the users to configure the problem severity level that triggers a user notification.	Release 1C; Must
3.2.5.2.2.11.4	The system shall have the capability to monitor real-time performance of the system in terms of service levels.	Release 1C; Must
3.2.5.2.2.11.5	The system shall provide storage usage metrics that allow projection of future storage needs.	Release 3; Must

3.2.5.2.2.11.6	The system shall monitor a Service Level Agreement for an externally hosted data store.	Release 1C; Must
3.2.5.2.2.11.7	The system shall allow users to reconfigure RAID levels without vendor assistance.	Release 2; Must

3.2.5.2.2.12	**Storage - Preventive Action**	
3.2.5.2.2.12.1	The system shall automatically allocate stand-by drives to replace drives that have failed.	Release 1C; Must
3.2.5.2.2.12.2	The system shall have the ability to allow hot swapping of components should a failure condition be detected.	Release 1C; Must
3.2.5.2.2.12.2.1	The system shall provide the capability to hot swap power supplies when a power supply has failed.	Release 1C; Must
3.2.5.2.2.12.2.2	The system shall provide the capability to hot swap cooling fans when a cooling fan has failed.	Release 1C; Must
3.2.5.2.2.12.2.3	The system shall provide the capability to hot swap disk drives in disk storage systems when a disk drive has failed.	Release 1C; Must
3.2.5.2.2.12.2.4	The system shall provide the capability to hot swap blade servers when a blade server has failed.	Release 1C; Must
3.2.5.2.2.12.3	The system shall have the ability to dynamically move data to improve system performance.	Release 1C; Must
3.2.5.2.2.12.4	The storage systems shall provide the capability to upgrade controller microcode without shutting down the storage system.	Release 2; Must

3.2.5.2.2.13	**Storage - Data Integrity**	
3.2.5.2.2.13.1	The system shall allow for securing of partitions.	Release 1C; Must
3.2.5.2.2.13.2	The system shall allow encryption of logical content.	Release 1C; Must
3.2.5.2.2.13.3	Deleted.	

3.2.5.2.2.14	**Storage - Allocation**	
3.2.5.2.2.14.1	The system shall support the management of heterogeneous storage architectures (e.g. direct attached storage (DAS), network attached storage (NAS), storage area network (SAN)).	Release 1C; Must
3.2.5.2.2.14.2	The system shall provide the capability to automatically allocate additional storage when a user configurable threshold is crossed.	Release 1C; Must
3.2.5.2.2.14.3	The system shall be able to manage any infrastructure storage device attached to the system.	Release 1C; Must
3.2.5.2.2.14.4	The system shall allow both manual and automated compression of data at various compression levels for infrequently accessed data.	Release 1C; Must
3.2.5.2.2.14.5	The system shall provide the capability to allocate storage on new devices after they have been identified by the system and formatted for use.	Release 1C; Must

3.2.5.3.2	Requirements for Security	
3.2.5.3.2.1	**Security - System User Authentication**	
3.2.5.3.2.1.1	The system shall have the capability to authenticate users based on a unique user identity.	Release 1B; Must
3.2.5.3.2.1.1.1	The system shall authenticate system and security administrators.	Release 1B; Must
3.2.5.3.2.1.1.1.1	The system shall authenticate system administrators.	Release 1B; Must
3.2.5.3.2.1.1.1.2	The system shall authenticate security administrators.	Release 1B; Must
3.2.5.3.2.1.1.1.1	The system shall support user ID and password authentication.	Release 1B; Must
3.2.5.3.2.1.1.1.2	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).	Release 1C; Must
3.2.5.3.2.1.1.1.3	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).	Release 1C; Must
3.2.5.3.2.1.2	The system shall permit users to create a unique user identity for access to the system.	Release 1B; Must
3.2.5.3.2.1.2.1	The system shall enforce uniqueness of user identity so that no two users can use the exact same identity.	Release 1B; Must
3.2.5.3.2.1.2.2	The system shall be capable of Identity Management system functionality to facilitate provisioning of user identities for users and system administrators.	Release 1B; Must
3.2.5.3.2.1.2.2.1	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.	Release 2; Must
3.2.5.3.2.1.2.2.1.1	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.	Release 2; Must
3.2.5.3.2.1.2.2.1.2	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.	Release 1C; Must
3.2.5.3.2.1.2.3	A user shall only be allowed to manage attributes associated with their own user identity.	Release 1C; Must
3.2.5.3.2.1.3	The system shall display a message to users if they fail to authenticate.	Release 1B; Must
3.2.5.3.2.1.4	The system shall permit access to a default workbench for public End Users, which does not require them to login.	Release 1B; Must
3.2.5.3.2.1.5	Deleted.	

3.2.5.3.2.1.6	The system shall comply with GPO and Federal authentication policies.	Release 1C; Must
3.2.5.3.2.1.6.1	The system shall comply with GPO authentication policies specified in P825.33.	Release 1C; Must
3.2.5.3.2.1.6.2	The system shall comply with Federal authentication policies.	Release 1C; Must
3.2.5.3.2.1.7	The system shall have the capability to support up to 2048-bit RSA public/private key generation (asymmetric algorithm).	Release 1C; Must

3.2.5.3.2.2	**Security - User Access Control**	
3.2.5.3.2.2.1	The system shall have the capability to arbitrate access based on a role-based access model driven by policy.	Release 1C; Must
3.2.5.3.2.2.1.1	The system shall permit authorized system administrators to create and assign customized roles.	Release 1C; Must
3.2.5.3.2.2.1.1.1	The system shall permit authorized system administrators to create customized roles.	Release 1C; Must
3.2.5.3.2.2.1.1.2	The system shall permit authorized system administrators to assign customized roles.	Release 1C; Must
3.2.5.3.2.2.1.1.1	The system shall provide access control limitations to support data mining .	Release 2; Must
3.2.5.3.2.2.1.2	The system shall allow authorized system administrators to assign and customize roles for access to system data objects and transactions.	Release 1C; Must
3.2.5.3.2.2.1.2.1	The system shall allow authorized system administrators to assign roles for access to system data objects and transactions.	Release 1C; Must
3.2.5.3.2.2.1.2.2	The system shall allow authorized system administrators to customize roles for access to system data objects and transactions.	Release 1C; Must
3.2.5.3.2.2.1.3	The system shall allow the use of standards based LDAP technology for the role based access model.	Release 1B; Must
3.2.5.3.2.2.2	The system shall manage user accounts.	Release 1B; Must
3.2.5.3.2.2.3	The system shall provide the capability to create user accounts.	Release 1B; Must
3.2.5.3.2.2.3.1	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.	Release 1B; Must
3.2.5.3.2.2.4	The system shall provide the capability to access user accounts.	Release 1B; Must
3.2.5.3.2.2.5	The system shall provide the capability to delete user accounts.	Release 1B; Must
3.2.5.3.2.2.6	The system shall provide the capability to suspend user accounts.	Release 1C; Must
3.2.5.3.2.2.7	The system shall provide the capability to reactivate suspended user accounts.	Release 1C; Must
3.2.5.3.2.2.8	The system shall provide the capability for the renewal of user registrations.	Release 1C; Must

3.2.5.3.2.2.9	The system shall have the capability to expire user accounts.	Release 1C; Must
3.2.5.3.2.2.10	The system shall provide the capability for users to cancel their accounts.	Release 1C; Must
3.2.5.3.2.2.11	The system shall provide the capability for users to update their account information.	Release 1C; Must
3.2.5.3.2.2.12	The system shall provide a means to ensure that users cannot view or modify information of other users unless authorized.	Release 1B; Must
3.2.5.3.2.2.12.1	The system shall provide a means to ensure that users cannot view information of other users unless authorized.	Release 1B; Must
3.2.5.3.2.2.12.2	The system shall provide a means to ensure that users cannot modify information of other users unless authorized.	Release 1B; Must
3.2.5.3.2.2.13	The system shall securely store personal information (e.g. user names and passwords).	Release 1B; Must
3.2.5.3.2.2.14	The system shall provide the capability for authorized users to manage (add, modify, delete) information.	Release 1B; Must
3.2.5.3.2.2.15	The system shall have the capability to provide secure interfaces for FDsys operations.	Release 1C; Must

3.2.5.3.2.3	**Security - Capture and Analysis of Audit Logs**	
3.2.5.3.2.3.1	The system shall keep an audit log of all transactions in the system.	Release 1C; Must
3.2.5.3.2.3.1.1	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.	Release 1C; Must
3.2.5.3.2.3.1.1.1	Audit logs shall contain logged events which each contain the date the event occurred.	Release 1C; Must
3.2.5.3.2.3.1.1.2	Audit logs shall contain logged events which each contain the time the event occurred.	Release 1C; Must
3.2.5.3.2.3.1.1.3	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.	Release 1C; Must
3.2.5.3.2.3.1.1.4	Audit logs shall contain logged events which each contain a classification of the event by the event source.	Release 1C; Must
3.2.5.3.2.3.1.1.5	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.	Release 1C; Must
3.2.5.3.2.3.1.1.6	Audit logs shall contain logged events which each contain a number identifying the particular event type.	Release 1C; Must
3.2.5.3.2.3.1.2	Audit logs shall contain a description of the event.	Release 1C; Must

3.2.5.3.2.3.1.2.1	Audit logs shall contain a description of the event containing the user name of the user on whose behalf the event occurred.	Release 1C; Must
3.2.5.3.2.3.1.2.2	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.	Release 1C; Must
3.2.5.3.2.3.1.2.3	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.	Release 1C; Must
3.2.5.3.2.3.1.2.4	Audit logs shall contain a description of the event containing information about infrequent significant events that describe successful operations of major server services.	Release 1C; Must
3.2.5.3.2.3.1.2.5	Audit logs shall contain a description of the event containing warnings, events that are not necessarily significant, but that indicate possible future problems.	Release 1C; Must
3.2.5.3.2.3.1.2.6	Audit logs shall contain a description of the event containing an audit of the security access attempts that were successful.	Release 1C; Must
3.2.5.3.2.3.1.2.7	Audit logs shall contain a description of the event containing an audit of the security access attempts that failed.	Release 1C; Must
3.2.5.3.2.3.1.3	Audit logs shall contain additional data fields where binary data can be displayed in bytes or words.	Release 2; Must
3.2.5.3.2.3.1.4	The system shall maintain a system log containing events logged by the system components.	Release 1B; Must
3.2.5.3.2.3.1.4.1	The system shall allow system logs to be viewed by all authorized users.	Release 1B; Must
3.2.5.3.2.3.1.5	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.	Release 1C; Must
3.2.5.3.2.3.1.5.1	The system shall maintain a security log containing logon attempts (both valid and invalid).	Release 1C; Must
3.2.5.3.2.3.1.5.2	The system shall maintain a security log containing events related to resource use, such as creating, opening, or deleting files or other objects.	Release 1C; Must
3.2.5.3.2.3.1.5.1	The system shall allow security logs to be viewed by all authorized users.	Release 1C; Must
3.2.5.3.2.3.1.6	The system shall maintain an application log containing events logged by applications.	Release 1C; Must
3.2.5.3.2.3.1.6.1	The system shall allow applications logs to be viewed by all authorized users.	Release 1C; Must
3.2.5.3.2.3.1.7	The system shall have an Audit Log manager for system administrator functions.	Release 1C; Must
3.2.5.3.2.3.1.7.1	The Audit Log manager shall be searchable.	Release 1C; Must
3.2.5.3.2.3.1.8	The system shall have the capability to reconstruct complete transactions.	Release 1C; Must
3.2.5.3.2.3.1.9	The system shall keep an audit log of user ordering (request) transactions.	Release 1C; Must

3.2.5.3.2.3.1.10	The system shall keep an audit log of system administration transactions.	Release 1C; Must
3.2.5.3.2.3.1.11	The system shall keep an audit log of security administrator transactions.	Release 1C; Must
3.2.5.3.2.3.1.12	The system shall keep an audit log of system access rights.	Release 1C; Must
3.2.5.3.2.3.1.13	The system shall keep an audit log of preservation processes.	Release 1C; Must
3.2.5.3.2.3.1.14.1	The system shall keep an audit log of deposited content activities.	Release 1C; Must
3.2.5.3.2.3.1.14.2	The system shall keep an audit log of harvested content activities.	Release 1C; Must
3.2.5.3.2.3.1.14.3	The system shall keep an audit log of converted content activities.	Release 1C; Must
3.2.5.3.2.3.1.15	The system shall keep an audit log of Content Originator ordering activities.	Release 1C; Must
3.2.5.3.2.3.1.16	The system shall keep an audit log of content authentication activities.	Release 1C; Must
3.2.5.3.2.3.1.17	The system shall keep an audit log of version control activities.	Release 1C; Must
3.2.5.3.2.3.1.18	The system shall keep an audit log of cataloging activities.	Release 1C; Must
3.2.5.3.2.3.1.19	The system shall keep an audit log of support activities (e.g., support status).	Release 1C; Must
3.2.5.3.2.3.1.20	The system shall keep an audit log for data mining.	Release 2; Must
3.2.5.3.2.3.2	The system shall have the capability to maintain integrity of audit logs.	Release 1C; Must
3.2.5.3.2.3.2.1	The system shall protect the audit log from unauthorized user modification.	Release 1C; Must
3.2.5.3.2.3.2.2	The system shall detect user attempts to edit audit logs.	Release 1C; Must
3.2.5.3.2.3.3	The system shall keep an audit log of attempts to access the system.	Release 1C; Must
3.2.5.3.2.3.3.1	The system shall keep an audit log of any detected breaches of security policy.	Release 1C; Must
3.2.5.3.2.3.4	The system shall keep and store audit logs (e.g. audit trails) and utilize records management processes on these stores.	Release 1C; Must
3.2.5.3.2.3.4.0.1	The system shall keep audit logs (e.g. audit trails) per GPO P825.33.	Release 1C; Must
3.2.5.3.2.3.4.0.2	The system shall store audit logs (e.g. audit trails) per GPO P825.33.	Release 1C; Must
3.2.5.3.2.3.4.0.3	The system shall utilize records management processes on audit log stores.	Release 1C; Must
3.2.5.3.2.3.4.1	The system shall save audit logs as specified in GPO Publication 825.33.	Release 1C; Must

3.2.5.3.2.4	**Security - User Privacy**	

3.2.5.3.2.4.1	The system shall support the capability of maintaining user privacy in accordance with GPO's privacy policy and Federal privacy laws and regulations.	Release 1C; Must
3.2.5.3.2.4.1.1	The system shall conform to guidelines set forth in GPO Publication 825.33.	Release 1C; Must
3.2.5.3.2.4.1.2	The system shall support compliance outlined in Title 5 USC Sec. 552a (Records maintained on individuals).	Release 1C; Must
3.2.5.3.2.4.1.3	The system shall support the capability of maintaining access privacy (e.g., Search, Request).	Release 1C; Must
3.2.5.3.2.4.1.4	The system shall support the capability of maintaining support privacy (e.g., user identity).	Release 1C; Must
3.2.5.3.2.4.1.5	The system shall support the capability of maintaining Content Originator ordering privacy.	Release 1C; Must
3.2.5.3.2.4.1.6	The system shall provide measures that preclude a single authorized administrator from listing an end user's orders.	Release 1C; Must

3.2.5.3.2.5	**Security - Confidentiality**	
3.2.5.3.2.5.1	The system shall support the capability of maintaining confidentiality of user data (e.g., passwords).	Release 1B; Must
3.2.5.3.2.5.1.1	The system shall have the capability to provide confidentiality of user data, including user authentication data exchanged through external interfaces.	Release 1C; Must
3.2.5.3.2.5.1.1.1.1	Deleted.	
3.2.5.3.2.5.1.1.1.2	Deleted.	
3.2.5.3.2.5.1.1.2	The system shall use a minimum 128 bit key length for all symmetric encryption operations.	Release 1C; Must
3.2.5.3.2.5.1.2	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).	Release 1B; Must
3.2.5.3.2.5.2	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.	Release 1C; Must
3.2.5.3.2.5.2.1	The system shall provide a method of encrypting FDsys content and system data, when required by authorized system administrators.	Release 1C; Must
3.2.5.3.2.5.2.1.1	The system shall provide a method of encrypting FDsys content, when required by authorized system administrators.	Release 1C; Must
3.2.5.3.2.5.2.1.2	The system shall provide a method of encrypting FDsys system data, when required by authorized system administrators.	Release 1C; Must

3.2.5.3.2.6	**Security Administration**	

3.2.5.3.2.6.1	The system shall provide an administrative graphical user interface to perform user administration and security administration.	Release 1C; Must
3.2.5.3.2.6.1.1	The system shall provide an administrative graphical user interface to perform user administration.	Release 1C; Must
3.2.5.3.2.6.1.2	The system shall provide an administrative graphical user interface to perform security administration.	Release 1C; Must
3.2.5.3.2.6.2	The system shall have the capability for authorized security administrators to set and maintain system security policy.	Release 1C; Must
3.2.5.3.2.6.2.0.1	The system shall have the capability for authorized security administrators to set system security policy.	Release 1C; Must
3.2.5.3.2.6.2.1	System security policy parameters shall include the capability to support various authentication methods.	Release 1C; Must
3.2.5.3.2.6.2.1.1	System security policy parameters shall include authorized user authentication methods.	Release 1C; Must
3.2.5.3.2.6.2.1.2	System security policy parameters shall include administrator authentication methods.	Release 1C; Must
3.2.5.3.2.6.2.1.3	System security policy parameters shall include minimum passwords lengths.	Release 1C; Must
3.2.5.3.2.6.2.1.4	System security policy parameters shall include authorized encryption algorithms.	Release 1C; Must
3.2.5.3.2.6.2.1.5	The system shall be flexible enough to incorporate additional, GPO-defined system security policy parameters.	Release 1C; Must
3.2.5.3.2.6.2.2	The system shall have the capability for authorized security administrators to maintain system security policy.	Release 1C; Must
3.2.5.3.2.6.3	The system shall provide the capability for authorized security administrators to monitor system security policy settings and policy enforcement.	Release 1C; Must
3.2.5.3.2.6.3.1	The system shall provide the capability for authorized security administrators to monitor system security policy settings.	Release 1C; Must
3.2.5.3.2.6.3.2	The system shall provide the capability for authorized security administrators to monitor system security policy enforcement.	Release 1C; Must
3.2.5.3.2.6.4	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)).	Release 1C; Must
3.2.5.3.2.6.4.1	The system shall have the capability to enforce the separation of functions through assigned roles.	Release 1C; Must
3.2.5.3.2.6.4.2	The system shall provide the capability to partition security administration into logical elements such that security administrators can be assigned accordingly.	Release 1C; Must
3.2.5.3.2.6.4.3	The system shall provide the capability to limit security administrator’s authority to assigned logical elements.	Release 1C; Must

3.2.5.3.2.7	**Security - Availability**	
3.2.5.3.2.7.1	The system shall provide appropriate backup and redundant components to ensure availability to meet customer and GPO needs.	Release 1C; Must
3.2.5.3.2.7.1.0.1	The system shall provide appropriate backup components to ensure availability to meet customer and GPO needs.	Release 1C; Must
3.2.5.3.2.7.1.0.2	The system shall provide appropriate redundant components to ensure availability to meet customer and GPO needs.	Release 1C; Must
3.2.5.3.2.7.1.1	The system shall be operational in the event of disaster situations with minimal business interruption to business functions.	Release 1C; Must
3.2.5.3.2.7.1.1.1	The system shall return to normal operations post-disaster.	Release 1C; Must
3.2.5.3.2.7.1.2	The system shall adhere to GPO's Continuity of Operations (COOP) plans.	Release 1C; Must
3.2.5.3.2.7.1.2.1	The system shall adhere to system development guidelines set forth in Office of Management and Budget Circular A-130.	Release 1C; Must
3.2.5.3.2.7.1.2.2	The system shall adhere to guidelines set forth in Federal Preparedness Circular 65.	Release 1C; Must
3.2.5.3.2.7.1.3	The system shall have appropriate failover components.	Release 1C; Must
3.2.5.3.2.7.1.4	The system shall be operational at appropriate GPO alternate facilities.	Release 1C; Must
3.2.5.3.2.7.1.5	The system shall back up system applications and data at a frequency as determined by business requirements.	Release 1C; Must
3.2.5.3.2.7.1.5.1	The system shall back up system applications at a frequency as determined by business requirements.	Release 1C; Must
3.2.5.3.2.7.1.5.2	The system shall back up system data at a frequency as determined by business requirements.	Release 1C; Must
3.2.5.3.2.7.1.5.1	The system applications and data shall be backed up at off-site storage location.	Release 1C; Must
3.2.5.3.2.7.1.5.1.1	The system applications shall be backed up at off-site storage location.	Release 1C; Must
3.2.5.3.2.7.1.5.1.2	The system data shall be backed up at off-site storage location.	Release 1C; Must
3.2.5.3.2.7.1.6	The system shall interface with designated GPO Service Providers (e.g. Oracle).	Release 1C; Must
3.2.5.3.2.7.1.7	The system shall maintain data integrity during backup processing.	Release 1B; Must
3.2.5.3.2.7.1.8	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.	Release 1B; Must
3.2.5.3.2.7.1.9	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.	Release 1C; Must

3.2.5.3.2.7.1.9.1	Mutually authenticated, high speed connection between GPO offices and hosting site shall be utilized.	Release 1C; Must
3.2.5.3.2.7.1.9.2	Encrypted connection using industry standard IPSEC Virtual Private Network (VPN) and strong (128 bit key minimum) encryption shall be utilized.	Release 1C; Must

3.2.5.3.2.8	**Security - Integrity**	
3.2.5.3.2.8.1	The system shall have the capability to assure integrity of business process information (BPI).	Release 1C; Must
3.2.5.3.2.8.2	The system shall check content for malicious code (e.g., worms and viruses) prior to ingest to maintain integrity.	Release 1B; Must
3.2.5.3.2.8.2.0.1	The system shall utilize GPO virus scanner technology.	Release 1B; Must
3.2.5.3.2.8.2.1	If malicious code is detected in content, it shall be placed into a quarantine area for GPO inspection.	Release 1B; Must

3.2.5.3.2.9	**Security Standards**	
3.2.5.3.2.9.1	The system shall have the capability to support the following industry integrity standards.	Release 1C; Must
3.2.5.3.2.9.1.1	The system shall have the capability to support the RSA Digital Signature in accordance with IETF RFC 3447.	Release 1C; Must
3.2.5.3.2.9.1.2	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #1 standards.	Release 1C; Must
3.2.5.3.2.9.1.3	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #7 standards.	Release 1C; Must
3.2.5.3.2.9.1.4	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #11 standards.	Release 1C; Must
3.2.5.3.2.9.1.5	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #12 standards.	Release 1C; Must
3.2.5.3.2.9.1.6	The system shall have the capability to support the International Telephone Union (ITU) X.509 v3 standard for certificate format.	Release 1C; Must
3.2.5.3.2.9.1.7	The system shall have the capability to support the IETF Public Key Infrastructure Exchange (PKIX) X.509 v3 standards for certificate compatibility.	Release 1C; Must
3.2.5.3.2.9.1.8	The system shall have the capability to support the Keyed-Hash Message Authentication Code (HMAC) standard as specified in FIPS Pub 198.	Release 1C; Must
3.2.5.3.2.9.1.9	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.	Release 1C; Must
3.2.5.3.2.9.1.10	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-1 standard.	Release 1C; Must

3.2.5.3.2.9.1.11	The system must shall the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-256 standard.	Release 1C; Must
3.2.5.3.2.9.1.12	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-384 standard.	Release 1C; Must
3.2.5.3.2.9.1.13	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-512 standard.	Release 1C; Must
3.2.5.3.2.9.1.14	The system shall have the capability to support the XML Digital Signature standards defined in RFC 3275 and XMLDSIG.	Release 1C; Must
3.2.5.3.2.9.2	The system shall have the capability to support the following confidentiality standards.	Release 1C; Must
3.2.5.3.2.9.2.1	The system shall have the capability to support the FIPS 197 Advanced Encryption Standard (AES).	Release 1C; Must
3.2.5.3.2.9.2.2	The system shall have the capability to support the ANSI X9.52 Triple Data Encryption Standard (TDES).	Release 1C; Must
3.2.5.3.2.9.2.3	The system shall have the capability to support the Secure Sockets Layer (SSL) version 3 / Transport Layer Security (TLS) standards per the guidelines in NIST SP 800-52.	Release 1C; Must
3.2.5.3.2.9.2.4	The system shall have the capability to comply with FIPS 140-2.	Release 1C; Must
3.2.5.3.2.9.2.5	The system shall have the capability to support the W3C XML Encryption standard XMLENC.	Release 1C; Must
3.2.5.3.2.9.3	The system shall have the capability to support the following access control standards.	Release 1C; Must
3.2.5.3.2.9.3.1	The system shall have the capability to support the Lightweight Directory Access Protocol (LDAP) Internet Engineering Task Force (IETF) Request for Comments (RFC) 2251.	Release 1C; Must
3.2.5.3.2.9.3.2	The system shall have the capability to support the International Telephone Union (ITU) X.500 standards.	Release 1C; Must
3.2.5.3.2.9.3.3	The system shall have the capability to support the Security and Access Markup Language (SAML) version 2 standard as specified by OASIS.	Release 1C; Must

3.2.5.4.2	**Requirements for Enterprise Service Bus**	
3.2.5.4.2.1	**ESB Core Capabilities**	
3.2.5.4.2.1.1	The system shall provide the capability to interoperate with services or applications deployed in different hardware and software platforms.	Release 1C; Must
3.2.5.4.2.1.1.0.1	The ESB shall support interoperability with Java Enterprise Edition (JEE).	Release 1B; Must
3.2.5.4.2.1.1.0.2	The ESB shall support interoperability with .Net.	Release 1C; Must
3.2.5.4.2.1.1.0.3	The ESB shall support interoperability with Web Services.	Release 1B; Must

3.2.5.4.2.1.1.0.4	The ESB shall support interoperability with Java Message Service (JMS).	Release 1B; Must
3.2.5.4.2.1.1.1	The ESB shall support common operating systems.	Release 1B; Must
3.2.5.4.2.1.1.1.1	The ESB shall support Microsoft Windows Server 2003.	Release 1B; Must
3.2.5.4.2.1.1.1.2	The ESB shall support Red Hat Enterprise Advanced Server 2.1.	Release 1B; Must
3.2.5.4.2.1.1.2	The ESB shall support application programmer interfaces in common programming languages.	Release 1C; Must
3.2.5.4.2.1.1.2.1	The ESB shall support application programmer interfaces in C.	Release 1B; Must
3.2.5.4.2.1.1.2.2	The ESB shall support application programmer interfaces in C++.	Release 1B; Must
3.2.5.4.2.1.1.2.3	The ESB shall support application programmer interfaces in Java.	Release 1B; Must
3.2.5.4.2.1.1.2.4	The ESB shall support application programmer interfaces in C#.	Release 1C; Must
3.2.5.4.2.1.2	The system shall support the ability to authenticate applications and services and control which applications can invoke a service.	Release 2; Must
3.2.5.4.2.1.2.1	The system shall support the capability to authenticate internal processes attempting to invoke a service provided by the system.	Release 2; Must
3.2.5.4.2.1.2.2	The system shall support the capability to authenticate external processes attempting to invoke a service provided by the system.	Release 2; Must
3.2.5.4.2.1.3	The system shall provide the capability to integrate newly developed (or acquired) services or applications (e.g. ILS, Oracle).	Release 1C; Must
3.2.5.4.2.1.3.1	The system shall provide the capability to integrate with Oracle applications and services.	Release 1C; Must
3.2.5.4.2.1.4	The system shall provide the capability to integrate existing (or legacy) services or applications.	Release 1B; Must
3.2.5.4.2.1.4.1	The system shall provide the capability to integrate with the ILS.	Release 1B; Must
3.2.5.4.2.1.5	The system shall provide the capability to coordinate and manage services or applications in the form of enterprise business processes.	Release 1C; Must
3.2.5.4.2.1.6	The system shall provide the capability to support synchronous and asynchronous communications between services or applications.	Release 1C; Must
3.2.5.4.2.1.6.0.1	The system shall provide the capability to support synchronous communications between services or applications.	Release 1B; Must
3.2.5.4.2.1.6.0.2	The system shall provide the capability to support asynchronous communications between services or applications.	Release 1C; Must
3.2.5.4.2.1.6.0.3	The system shall provide the capability to support reliable communications between services or applications.	Release 1C; Must

3.2.5.4.2.1.6.0.4	The system shall provide the capability to specify the quality of service for communications between services or applications.	Release 1C; Must
3.2.5.4.2.1.6.1	The system shall provide the capability to queue communications between services and applications.	Release 1C; Must
3.2.5.4.2.1.7	The system shall provide the capability to run process transactions.	Release 1C; Must
3.2.5.4.2.1.7.1	The system shall provide the capability to manage process transactions declaratively via system configurations.	Release 1C; Must
3.2.5.4.2.1.7.1.1	The system shall provide the capability to manage process transactions declaratively using a GUI.	Release 1C; Must
3.2.5.4.2.1.7.1.2	The system shall provide the capability to store process transactions configuration information in XML.	Release 1C; Must
3.2.5.4.2.1.7.2	The system shall provide the capability to execute pre-defined process transactions.	Release 1C; Must
3.2.5.4.2.1.7.3	The system shall provide the capability to manually commit and roll back process transactions.	Release 1C; Must
3.2.5.4.2.1.8	The system shall provide the capability to create communications between services or applications, internal or external, in XML form with published schemas.	Release 1C; Must
3.2.5.4.2.1.8.1	The system shall provide the capability to validate communications against the appropriate published schema.	Release 1C; Must
3.2.5.4.2.1.8.2	The system shall provide the capability to transform communications to different published schemas.	Release 1C; Must
3.2.5.4.2.1.9	The system shall provide the capability to perform XML document-based routing between services or applications.	Release 1B; Must
3.2.5.4.2.1.10	The system shall provide the capability to support incremental implementations.	Release 1C; Must
3.2.5.4.2.1.10.1	The ESB shall support the capability to deploy services without disrupting system operations.	Release 1C; Must
3.2.5.4.2.1.10.2	The ESB shall support the capability to undeploy services without disrupting system operations that do not rely on the service which is being undeployed.	Release 1C; Must
3.2.5.4.2.1.10.3	The ESB shall support the capability to deploy applications without disrupting system operations.	Release 1C; Must
3.2.5.4.2.1.10.4	The ESB shall support the capability to undeploy applications without disrupting system operations that do not rely on the application which is being undeployed.	Release 1C; Must
3.2.5.4.2.1.11	The system shall provide the capability to support exception handling.	Release 1C; Must
3.2.5.4.2.1.11.1	The system shall provide the capability to generate compensating transactions for exceptions where possible.	Release 3; Should
3.2.5.4.2.1.12	The system shall store information related to the ESB in metadata.	Release 1B; Must

3.2.5.4.2.1.12.1	The system shall store information about schemas in metadata.	Release 1C; Must
3.2.5.4.2.1.12.1.1	The ESB shall support WSDL.	Release 1B; Must
3.2.5.4.2.1.12.1.2	The ESB shall support WS-Security.	Release 1C; Must
3.2.5.4.2.1.12.1.3	The ESB shall support WS-Reliability or WS-Reliable Messaging	Release 1C; Must
3.2.5.4.2.1.12.2	The system shall store information about transactional operations in metadata.	Release 1B; Must
3.2.5.4.2.1.12.2.1	The system shall support the capability to record information about transactions in logs.	Release 1B; Must
3.2.5.4.2.1.12.3	The system shall store information about communications in metadata.	Release 1B; Must
3.2.5.4.2.1.12.3.1	The system shall support the capability to record information about message traffic in logs.	Release 1B; Must
3.2.5.4.2.1.12.4	The system shall store information about business processes in metadata.	Release 1B; Must
3.2.5.4.2.1.12.4.1	The system shall support the capability to record information about business process execution in logs.	Release 1B; Must

3.2.5.4.2.2	**ESB Configuration**	
3.2.5.4.2.2.1	The system shall provide the capability to perform integration configurations.	Release 1C; Must
3.2.5.4.2.2.1.0.1	The system shall provide the capability to manage integration configurations using a GUI.	Release 1C; Must
3.2.5.4.2.2.1.1	The system shall provide the capability to perform integration configurations in XML.	Release 1C; Must
3.2.5.4.2.2.1.1.1	The system shall provide the capability to store integration configuration information in XML.	Release 1C; Must
3.2.5.4.2.2.2	The system shall provide the capability to add redundancy to critical ESB functions.	Release 2; Must

3.2.5.4.2.3	**ESB Administration**	
3.2.5.4.2.3.1	The system shall provide the capability to impose rule-based security control over administrative tasks.	Release 3; Must
3.2.5.4.2.3.2	The system shall provide the capability to manage services or applications dynamically.	Release 1C; Must
3.2.5.4.2.3.3	The system shall provide the capability to enable and disable services dynamically.	Release 2; Must
3.2.5.4.2.3.3.1	The system shall provide the capability to enable services dynamically.	Release 2; Must
3.2.5.4.2.3.3.2	The system shall provide the capability to disable services dynamically.	Release 2; Must
3.2.5.4.2.3.4	The system shall provide the capability to manage business processes.	Release 1C; Must
3.2.5.4.2.3.4.1	The system shall provide the capability to support business process orchestration.	Release 1C; Must
3.2.5.4.2.3.5	The system shall provide the capability to terminate, suspend and resume business processes.	Release 1C; Must

3.2.5.4.2.3.5.1	The system shall provide the capability to terminate business processes that are being orchestrated.	Release 1C; Must
3.2.5.4.2.3.5.2	The system shall provide the capability to suspend business processes that are being orchestrated.	Release 1C; Must
3.2.5.4.2.3.5.3	The system shall provide the capability to resume business processes that are suspended.	Release 1C; Must
3.2.5.4.2.3.6	The system shall provide the capability to monitor ESB processes that are being orchestrated.	Release 1C; Must
3.2.5.4.2.3.6.1	The system shall provide the capability to monitor the business processes at all available statuses: active, suspended, terminated, and completed.	Release 1C; Must
3.2.5.4.2.3.6.2	The system shall provide the capability to monitor communication latencies.	Release 1C; Must
3.2.5.4.2.3.6.3	The system shall provide the capability to send notifications in the event of problems with ESB functions.	Release 1C; Must

3.2.5.4.2.4	**ESB Interface**	
3.2.5.4.2.4.1	The system shall provide the capability to perform configuration tasks via a Graphical User Interface (GUI) tool.	Release 1C; Must
3.2.5.4.2.4.2	The system shall provide the capability to perform administrative tasks via a GUI tool.	Release 1C; Must

3.2.5.5.2	**Requirements for Data Mining**	
3.2.5.5.2.1	**Data Mining - Data Extraction**	
3.2.5.5.2.1.1	The system shall be capable of extracting data from the entire collection of BPI.	Release 2; Must
3.2.5.5.2.1.2	The system shall be capable of extracting data from the entire collection of metadata.	Release 2; Must
3.2.5.5.2.1.3	The system shall be capable of extracting data from select GPO data sources (e.g., Oracle).	Release 3; Must
3.2.5.5.2.1.3.1	The system shall be capable of extracting data from Oracle.	Release 2; Must
3.2.5.5.2.1.3.2	The system shall be capable of extracting data from additional GPO data sources in the future.	Release 3; Must
3.2.5.5.2.1.4	The system shall be capable of extracting data according to a schedule defined by users.	Release 1C; Should / Release 2; Must
3.2.5.5.2.1.5	The system shall be able to extract data according to user defined queries.	Release 2; Must
3.2.5.5.2.1.6	The system shall be able to extract random samples of data.	Release 1C; Could / Release 2; Must
3.2.5.5.2.1.7	The system shall allow users to input data to supplement system data (e.g., Web log, historical sales data).	Release 1C; Should / Release 2; Must
3.2.5.5.2.1.7.1	The system shall allow users to upload files from which data will be extracted for analysis.	Release 1C; Should / Release 2; Must
3.2.5.5.2.1.7.2	The system shall allow users to enter supplemental historical data.	Release 1C; Should / Release 2; Must

3.2.5.5.2.1.7.3	The system shall allow users to restrict access to supplemental data.	Release 1C; Should / Release 2; Must
3.2.5.5.2.1.7.4	The system shall allow users to store supplemental data for future use.	Release 1C; Should / Release 2; Must
3.2.5.5.2.1.8	The system shall be capable of extracting data from multiple formats.	Release 2; Must
3.2.5.5.2.1.8.1	The system shall be capable of extracting data from data sources in XML format.	Release 2; Must
3.2.5.5.2.1.8.2	The system shall be capable of extracting data from data sources in PDF format.	Release 2; Must
3.2.5.5.2.1.8.3	The system shall be capable of extracting data from data sources in XLS format.	Release 2; Must
3.2.5.5.2.1.8.4	The system shall be capable of extracting data from data sources in CSV format.	Release 2; Must
3.2.5.5.2.1.8.5	The system shall be support the capability of extracting data from data sources in additional formats in the future.	Release 3; Must
3.2.5.5.2.1.9	The system shall be capable of data extraction at speeds sufficient to support the creation of real-time reports.	Release 1C; Should / Release 2; Must

3.2.5.5.2.2	**Data Mining - Data Normalization**	
3.2.5.5.2.2.1	The system shall be able to normalize data based on additional administrator defined parameters in the future.	Release 2; Must
3.2.5.5.2.2.1.1	The system shall be able to identify missing values or metadata elements.	Release 2; Must
3.2.5.5.2.2.1.2	The system shall be able to identify data anomalies in BPI and metadata.	Release 2; Must
3.2.5.5.2.2.1.3	The system shall be able to identify data formats.	Release 2; Must
3.2.5.5.2.2.1.4	The system shall be able to identify format discrepancies.	Release 2; Must
3.2.5.5.2.2.1.5	The system shall be able to identify standard data elements.	Release 2; Must
3.2.5.5.2.2.1.6	The system shall be able to identify data types.	Release 2; Must
3.2.5.5.2.2.2	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).	Release 2; Must

3.2.5.5.2.3	**Data Mining - Data Analysis and Modeling**	
3.2.5.5.2.3.1	The system shall be able to perform single variable and multivariable analysis operations on extracted data.	Release 2; Must
3.2.5.5.2.3.1.0.1	The system shall be able to perform single variable analysis operations on extracted data.	Release 2; Must
3.2.5.5.2.3.1.0.2	The system shall be able to perform multivariable analysis operations on extracted data.	Release 2; Must

3.2.5.5.2.3.1.1	The system shall be able to calculate averages (mean, median, mode).	Release 2; Must
3.2.5.5.2.3.1.1.1	The system shall be able to calculate means.	Release 2; Must
3.2.5.5.2.3.1.1.2	The system shall be able to calculate medians.	Release 2; Must
3.2.5.5.2.3.1.1.3	The system shall be able to calculate modes.	Release 2; Must
3.2.5.5.2.3.1.2	The system shall be able to perform cross tabulations.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.3	The system shall be able to perform clusterization.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.4	The system shall be able to perform categorization.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.5	The system shall be able to perform association and link analyses.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.6	The system shall be able to perform regression analysis.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.7	The system shall be able to expose hierarchical or parent/child relationships.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.8	The system shall be able to expose sequential relationships and patterns.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.8.1	The system shall be able to expose sequential relationships.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.8.2	The system shall be able to expose sequential patterns.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.9	The system shall be able to expose temporal relationships and patterns.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.9.1	The system shall be able to expose temporal relationships.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.9.2	The system shall be able to expose temporal patterns.	Release 1C; Could / Release 2; Must
3.2.5.5.2.3.1.10	The system shall be able to expose inferences and rules that led to a result set.	Release 2; Could / Release 3; Must
3.2.5.5.2.3.2	The system shall be able to warn users attempting illogical operations (e.g., calculating averages out of categorical data).	Release 2; Could
3.2.5.5.2.3.2.1	The system shall be capable of showing the user the rule violation that led to the warning.	Release 2; Could
3.2.5.5.2.3.3	The system shall allow users to suspend, resume, or restart analysis	Release 1C; Should / Release 2; Must
3.2.5.5.2.3.3.1	The system shall allow users to suspend an analysis that is in progress.	Release 1C; Should / Release 2; Must
3.2.5.5.2.3.3.2	The system shall allow users to resume a suspended analysis.	Release 1C; Should / Release 2; Must
3.2.5.5.2.3.3.3	The system shall allow users to restart an analysis from the beginning.	Release 1C; Should / Release 2; Must
3.2.5.5.2.3.4	The system shall be capable of providing the user with an estimated analysis time.	Release 2; Could

3.2.5.5.2.4	**Data Mining - Report Creation and Data Presentation**	
3.2.5.5.2.4.1	The system shall be able to produce reports summarizing the analysis of BPI and metadata.	Release 2; Must
3.2.5.5.2.4.1.1	The system shall allow users to choose from the data types available in BPI and metadata and choose operations performed on that data.	Release 2; Must
3.2.5.5.2.4.1.2	The system shall be able to produce a report summarizing system usage for a user-defined time range.	Release 2; Must
3.2.5.5.2.4.1.3	The system shall be able to produce a report analyzing the usage of search terms.	Release 2; Must
3.2.5.5.2.4.2	The system shall be capable of including graphical analysis in reports, including charts, tables, and graphs.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.2.1	The system shall be capable of including charts in reports.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.2.2	The system shall be capable of including tables in reports.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.2.3	The system shall be capable of including graphs in reports.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.3	The system shall allow a set of default report templates to be accessible for each user class.	Release 2; Must
3.2.5.5.2.4.3.1	The system shall allow users to manage the default templates.	Release 2; Must
3.2.5.5.2.4.4	The system shall allow users to create custom reports and report templates based on access rights to BPI and metadata.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.4.1	The system shall allow users to create custom report templates.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.4.2	The system shall allow users to update custom report templates.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.4.3	The system shall allow users to delete custom report templates.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.5	The system shall be capable of real-time population of report templates.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.6	The system shall be capable of automatically creating reports using report templates according to a schedule defined by users.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.6.1	The system shall allow users to request notification that a scheduled report is available.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.6.2	The system shall enable GPO users to restrict view/modify access to customized report templates.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.6.2.1	The system shall enable GPO users to control which users can view a report template.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.6.2.2	The system shall enable GPO users to control which users can modify a report template.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.7	The system shall be capable of delivering reports to users.	Release 1C; Could / Release 2; Must

3.2.5.5.2.4.7.1	The system shall allow users to specify delivery method (e.g., e-mail, RSS, FTP).	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.7.1.1	The system shall support the capability to deliver reports to users using E-mail.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.7.1.2	The system shall support the capability to deliver reports to users using RSS.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.7.1.3	The system shall support the capability to deliver reports to users using FTP.	Release 1C; Could / Release 2; Must
3.2.5.5.2.4.8	The system shall be capable of supporting real-time reporting.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.9	The system shall allow users to create notifications based on real-time analysis of BPI or metadata.	Release 1C; Should / Release 2; Must
3.2.5.5.2.4.10	The system shall be able to link analysis results to data.	Release 2; Could
3.2.5.5.2.4.11	The system shall be able to expose analysis criteria and algorithms.	Release 2; Could
3.2.5.5.2.4.12	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).	Release 2; Must
3.2.5.5.2.4.12.1	The system shall be able to export reports in HTML format.	Release 2; Must
3.2.5.5.2.4.13	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.	Release 2; Must
3.2.5.5.2.4.13.1	The system shall support user interface customization and personalization based on the interactions of a user with the system.	Release 2; Must
3.2.5.5.2.4.13.2	The system shall support user interface customization by aggregating the interactions of many users with the system.	Release 2; Must

3.2.5.5.2.5	**Data Mining - Security and Administration**	
3.2.5.5.2.5.1	The system shall restrict access to BPI and metadata based on permissions and access rights, based on user profile.	Release 2; Must
3.2.5.5.2.5.1.1	The system shall restrict access to metadata based on permissions, based on user profile.	Release 2; Must
3.2.5.5.2.5.1.2	The system shall restrict access to metadata based on access rights, based on user profile.	Release 2; Must
3.2.5.5.2.5.1.3	The system shall restrict access to BPI based on permissions, based on user profile.	Release 2; Must
3.2.5.5.2.5.1.4	The system shall restrict access to BPI based on access rights, based on user profile.	Release 2; Must
3.2.5.5.2.5.2	The system shall log all user interactions with the system in metadata.	Release 2; Must
3.2.5.5.2.5.2.1	Each metadata log entry shall include at least the user identification, user class, date, time, action, and referring page, subject to GPO privacy rules.	Release 2; Must

3.2.5.5.2.5.2.1.1	Each metadata log entry shall include the user identification, subject to GPO privacy rules.	Release 2; Must
3.2.5.5.2.5.2.1.2	Each metadata log entry shall include the user class, subject to GPO privacy rules.	Release 2; Must
3.2.5.5.2.5.2.1.3	Each metadata log entry shall include the date, subject to GPO privacy rules.	Release 2; Must
3.2.5.5.2.5.2.1.4	Each metadata log entry shall include the time, subject to GPO privacy rules.	Release 2; Must
3.2.5.5.2.5.2.1.5	Each metadata log entry shall include the action, subject to GPO privacy rules.	Release 2; Must
3.2.5.5.2.5.2.1.6	Each metadata log entry shall include the referring page, subject to GPO privacy rules.	Release 2; Must
3.2.5.5.2.5.3	The system shall log all processes in metadata.	Release 2; Must
3.2.5.5.2.5.4	The system shall perform records management functions on logs.	Release 2; Must

3.2.5.5.2.6	**Data Mining - Storage**	
3.2.5.5.2.6.1	The system shall store extracted data.	Release 2; Must
3.2.5.5.2.6.1.1	Extracted data shall be held in temporary storage. Once analysis is complete, extracted data is deleted from temporary storage.	Release 2; Must
3.2.5.5.2.6.1.1.1	The system shall provide the capability to store the corpus of extracted data.	Release 2; Must
3.2.5.5.2.6.1.1.2	The system shall provide the capability to delete selected portions of the corpus of extracted data.	Release 2; Must
3.2.5.5.2.6.1.1.3	The system shall provide the capability to reload selected portions of the corpus of extracted data by re-extracting the data.	Release 2; Must
3.2.5.5.2.6.2	The system shall store metadata, supplemental data, reports, report templates, analysis criteria, and algorithms in Business Process Storage.	Release 2; Must
3.2.5.5.2.6.2.0.1	The system shall store metadata in Business Process Storage.	Release 2; Must
3.2.5.5.2.6.2.0.2	The system shall store supplemental data in Business Process Storage.	Release 2; Must
3.2.5.5.2.6.2.0.3	The system shall store reports in Business Process Storage.	Release 2; Must
3.2.5.5.2.6.2.0.4	The system shall store report templates in Business Process Storage.	Release 2; Must
3.2.5.5.2.6.2.0.5	The system shall store analysis criteria in Business Process Storage.	Release 2; Must
3.2.5.5.2.6.2.0.6	The system shall store algorithms in Business Process Storage.	Release 2; Must
3.2.5.5.2.6.2.1	The system shall have a records management process (e.g., delete files and reports at a defined time).	Release 2; Must

3.2.6.1	Requirements for Content Submission	
3.2.6.1.1	**Content Submission Core Capabilities**	
3.2.6.1.1.1	The system shall accept digital content and metadata.	Release 1B; Must
3.2.6.1.1.2	The system shall create a SIP from content and metadata.	Release 1B; Must

3.2.6.1.2	**Content Submission - System Administration**	
3.2.6.1.2.1	The system shall to be able to accept, store, and deliver encrypted files.	Release 2; Could
3.2.6.1.2.2	The system shall provide notification to the submission agency/authority that the content has been received by FDsys.	Release 1C; Must
3.2.6.1.2.2.1	The system shall notify submission agency/authority if content is not received.	Release 1C; Must
3.2.6.1.2.3	The system shall have the capability to provide notification to the submission agency/authority that the content has been released to the intended users.	Release 1B; Could / Release 1C; Must
3.2.6.1.2.4	The system shall identify files with security restrictions upon submission.	Release 1C; Must
3.2.6.1.2.4.1	Information about the files will be recorded in metadata.	Release 1B; Must
3.2.6.1.2.5	The system shall have the capability to allow users to indicate that content contains copyrighted material.	Release 1C; Must
3.2.6.1.2.5.0.1	The system shall have the capability to allow users to specify what the intended use and access rights to the content should be.	Release 1C; Must
3.2.6.1.2.5.0.2	The system shall have the capability to allow users to specify what the intended distribution of the content should be.	Release 1C; Must
3.2.6.1.2.5.0.3	The system shall have the capability to allow authorized users to modify access rights to content based on copyright information provided by Content Originators.	Release 1C; Must
3.2.6.1.2.5.0.4	The system shall have the capability to notify authorized users that copyrighted content has been submitted.	Release 1C; Must
3.2.6.1.2.5.1	Copyright information will be recorded in metadata.	Release 1C; Must
3.2.6.1.2.6	The system shall provide WIP storage for content prior to ingest.	Release 1B; Must
3.2.6.1.2.7	The system shall check content prior to ingest.	Release 1B; Must
3.2.6.1.2.7.1	Deleted.	
3.2.6.1.2.7.1.1	Deleted.	
3.2.6.1.2.7.2	Zipped files (.zip) shall be unzipped.	Release 1C; Must
3.2.6.1.2.7.3	Stuffed files (.sit) shall be unstuffed.	Release 1C; Must
3.2.6.1.2.8	The system shall accept content with specialized character sets (e.g., non-Roman, scientific notations)	Release 1B; Must

3.2.6.1.3	**Content Submission Metadata**	
3.2.6.1.3.1	The system shall accept all administrative and descriptive metadata supplied by the submission agency/authority.	Release 1B; Must
3.2.6.1.3.1.1	The system shall provide the capability to record Title or caption of content.	Release 1B; Must
3.2.6.1.3.1.2	The system shall provide the capability to record content identifiers assigned to content.	Release 1B; Must
3.2.6.1.3.1.2.1	The system shall provide the capability to record the Persistent names assigned to content.	Release 1B; Must
3.2.6.1.3.1.2.2	The system shall provide the capability to record the filenames assigned to content.	Release 1B; Must
3.2.6.1.3.1.2.3	The system shall provide the capability to record the ISBN/ISSNs assigned to content.	Release 1B; Must
3.2.6.1.3.1.2.4	The system shall provide the capability to record the Agency requisition numbers assigned to content.	Release 1B; Must
3.2.6.1.3.1.2.5	The system shall support the capability to record additional content identifiers in the future.	Release 1B; Must
3.2.6.1.3.1.3	The system shall provide the capability to record Author/Creator of the content.	Release 1B; Must
3.2.6.1.3.1.4	The system shall provide the capability to record Publisher/Authority of the content.	Release 1B; Must
3.2.6.1.3.1.5	The system shall provide the capability to record Rights Owner of the content.	Release 1B; Must
3.2.6.1.3.1.6	The system shall provide the capability to record version information of the content.	Release 1B; Must
3.2.6.1.3.1.7	The system shall provide the capability to record relationships between content packages and digital objects.	Release 1B; Must
3.2.6.1.3.1.7.1	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).	Release 1B; Must
3.2.6.1.3.1.8	The system shall provide the capability to record content description information (e.g., abstract, summary).	Release 1B; Must
3.2.6.1.3.1.9	The system shall provide the capability to record Structure Information of the content.	Release 1B; Must
3.2.6.1.3.1.10	The system shall provide the capability to record Intended Output of the content.	Release 1B; Must
3.2.6.1.3.1.11	The system shall provide the capability to record Intended Audience of the content.	Release 1B; Must
3.2.6.1.3.1.12	The system shall provide the capability to record 13 Digit ISBN Numbers to content.	Release 1B; Must
3.2.6.1.3.2	The system shall accept and capture the following elements when available and applicable.	Release 1B; Must
3.2.6.1.3.2.1	The system shall accept and capture elements relating to documents.	Release 1B; Must

3.2.6.1.3.2.1.1	The system shall accept and capture Software applications and versions used to create the digital objects.	Release 1B; Must
3.2.6.1.3.2.1.2	The system shall accept and capture Publication size.	Release 1B; Must
3.2.6.1.3.2.1.3	The system shall accept and capture the Trim size.	Release 1B; Must
3.2.6.1.3.2.1.4	The system shall accept and capture the number of pages.	Release 1B; Must
3.2.6.1.3.2.1.5	The system shall accept and capture the file format.	Release 1B; Must
3.2.6.1.3.2.1.6	The system shall accept and capture the file sizes.	Release 1B; Must
3.2.6.1.3.2.1.7	The system shall accept and capture the fonts.	Release 1B; Must
3.2.6.1.3.2.1.8	The system shall accept and capture the Furnished or embedded fonts.	Release 1B; Must
3.2.6.1.3.2.1.9	The system shall accept and capture the Font types.	Release 1B; Must
3.2.6.1.3.2.1.10	The system shall accept and capture the color mode(s).	Release 1B; Must
3.2.6.1.3.2.1.11	The system shall accept and capture the Bleed required/provided for.	Release 1B; Must
3.2.6.1.3.2.1.12	The system shall accept and capture the Construction information.	Release 1B; Must
3.2.6.1.3.2.1.13	The system shall accept and capture the Image resolutions.	Release 1B; Must
3.2.6.1.3.2.1.14	The system shall accept and capture the Language.	Release 1B; Must
3.2.6.1.3.2.1.15	The system shall accept and capture the File compression.	Release 1B; Must
3.2.6.1.3.2.1.16	The system shall support the capability to accept and capture the other document elements in the future.	Release 1B; Must
3.2.6.1.3.2.2	The system shall accept and capture elements relating to audio.	Release 1C; Must
3.2.6.1.3.2.2.1	The system shall accept and capture audio File formats.	Release 1C; Must
3.2.6.1.3.2.2.2	The system shall accept and capture audio File sizes.	Release 1C; Must
3.2.6.1.3.2.2.3	The system shall accept and capture audio playing time.	Release 1C; Must
3.2.6.1.3.2.2.4	The system shall accept and capture audio Language.	Release 1C; Must
3.2.6.1.3.2.2.5	The system shall accept and capture audio File compression.	Release 1C; Must
3.2.6.1.3.2.2.6	The system shall support the capability to accept and capture bit rate.	Release 1C; Must
3.2.6.1.3.2.2.7	The system shall support the capability to accept and capture additional audio elements in the future.	Release 1C; Must
3.2.6.1.3.2.3	The system shall accept and capture elements relating to video.	Release 1C; Must
3.2.6.1.3.2.3.1	The system shall accept and capture video File formats.	Release 1C; Must
3.2.6.1.3.2.3.2	The system shall accept and capture video File sizes.	Release 1C; Must
3.2.6.1.3.2.3.3	The system shall accept and capture Closed captioning.	Release 1C; Must

3.2.6.1.3.2.3.4	The system shall accept and capture Video runtime.	Release 1C; Must
3.2.6.1.3.2.3.5	The system shall accept and capture Video encoding scheme.	Release 1C; Must
3.2.6.1.3.2.3.6	The system shall accept and capture video Language.	Release 1C; Must
3.2.6.1.3.2.3.7	The system shall accept and capture video File compression.	Release 1C; Must
3.2.6.1.3.2.3.8	The system shall support the capability to accept and capture additional video elements in the future.	Release 1C; Must
3.2.6.1.3.2.4	The system shall provide the capability to support other formats in the future.	Release 1B; Must

3.2.6.2.2	Requirements for Deposited Content	
3.2.6.2.2.1	**Deposited Content Core Capabilities**	
3.2.6.2.2.1.1	The system shall accept digital content and metadata provided by Content Originators.	Release 1C; Must
3.2.6.2.2.1.2	The system shall have the capability to notify Content Evaluators that new content has been received by the system.	Release 1C; Must

3.2.6.2.2.2	**Deposited Content Metadata**	
3.2.6.2.2.2.1	The system shall accept “approved for release” information provided by the content originating agency.	Release 1C; Must

3.2.6.2.2.3	**Deposited Content Interfaces**	
3.2.6.2.2.3.1	Deposited content interface shall enable Congressional Content Originators and Agency Content Originators to:	Release 1C; Must
3.2.6.2.2.3.1.1	Submit digital content and metadata	Release 1C; Must
3.2.6.2.2.3.1.2	Submit content chain of custody information to the system	Release 1C; Must
3.2.6.2.2.3.1.3	Submit intended use information to the system	Release 1C; Must
3.2.6.2.2.3.1.4	Submit “approved for release” information	Release 1C; Must
3.2.6.2.2.3.1.5	Receive notification of receipt of content and content ID	Release 1C; Must
3.2.6.2.2.3.1.6	Receive notification if content is not received, explanation for why content was not received, and options for proceeding	Release 1C; Must
3.2.6.2.2.3.1.7	Receive notification of release of content	Release 1C; Must
3.2.6.2.2.3.1.8	Deleted.	
3.2.6.2.2.3.2	Deposited content interface shall enable GPO Service Providers and external Service Providers to:	Release 1C; Must
3.2.6.2.2.3.2.1	Submit digital content and metadata	Release 1C; Must
3.2.6.2.2.3.2.2	Receive notification of receipt of content and content ID	Release 1C; Must

3.2.6.2.2.3.2.3	Receive notification if content is not received, explanation for why content was not received, and options for proceeding	Release 1C; Must
3.2.6.2.2.3.2.4	Deleted.	

3.2.6.3.2	**Requirements for Converted Content**	
3.2.6.3.2.1	**Converted Content Core Capabilities**	
3.2.6.3.2.1.1	The system shall have capability to accept converted content.	Release 1C; Must
3.2.6.3.2.1.1.1	Digital content may be provided in file formats for digitized tangible documents as specified in Appendix B: Operational Specification for Converted Content.	Release 1C; Must

3.2.6.3.2.2	**Converted Content Interfaces**	
3.2.6.3.2.2.1	Converted content interface shall enable GPO Service Providers and external Service Providers to:	Release 1C; Must
3.2.6.3.2.2.1.1	Submit approved content and metadata.	Release 1C; Must
3.2.6.3.2.2.1.2	Receive notification of receipt of content and content ID	Release 1C; Must
3.2.6.3.2.2.1.3	Provide notification of release of content	Release 1C; Must
3.2.6.3.2.2.1.4	Receive notification if content is not received, explanation for why content was not received, and options for proceeding	Release 1C; Must
3.2.6.3.2.2.1.5	Manage converted content	Release 1C; Must

3.2.6.4.2	**Requirements for Harvested Content**	
3.2.6.4.2.1	**Harvested Content Core Capabilities**	
3.2.6.4.2.1.1	The system shall accept digital content and metadata delivered by the harvesting function.	Release 2; Must

3.2.6.4.2.2	**Harvested Content Metadata**	
3.2.6.4.2.2.1	The system shall provide the capability to record the date and time of harvest of content.	Release 2; Must

3.2.6.4.2.3	**Harvester Requirements**	
3.2.6.4.2.3.1	The harvester shall have the capability to discover, assess, and harvest in-scope content from targeted Web sites.	Release 2; Must
3.2.6.4.2.3.2	The harvester shall have the capability to ensure that it does not harvest the same content more than once.	Release 1C; Could / Release 2; Must
3.2.6.4.2.3.3	The harvester shall have the capability to perform the discovery, assessment, and harvesting processes on target Web sites based on update schedules.	Release 1C; Could / Release 2; Must

3.2.6.4.2.3.4	The harvester shall have capability to perform simultaneous harvests.	Release 2; Must
3.2.6.4.2.3.5	The harvester shall locate and harvest all levels of Web pages within a Web site.	Release 2; Must
3.2.6.4.2.3.6	The harvester shall go outside the target domains or Web sites only when the external domain contains in-scope content.	Release 1C; Should / Release 2; Must
3.2.6.4.2.3.7	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.	Release 2; Must
3.2.6.4.2.3.8	The harvester shall stop the discovery process when a linked Web page does not contain in-scope content.	Release 1C; Should / Release 2; Must
3.2.6.4.2.3.9	The harvester shall flag content and URLs that are only partially harvested by the automated harvester for manual follow-up.	Release 2; Must
3.2.6.4.2.3.10	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.	Release 2; Must
3.2.6.4.2.3.11	The harvester shall collect in-scope discovered content and available metadata.	Release 2; Must
3.2.6.4.2.3.11.1	The harvester shall deliver all in-scope content and metadata to WIP storage.	Release 2; Must
3.2.6.4.2.3.11.2	The harvester shall have the ability to discover and collect all file types that may reside on target Web sites.	Release 2; Must
3.2.6.4.2.3.12	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).	Release 2; Must
3.2.6.4.2.3.13	The harvester shall have the ability to maintain the directory structure of Web sites that constitute entire publications.	Release 2; Must
3.2.6.4.2.3.14	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).	Release 2; Must
3.2.6.4.2.3.15	The harvester must be able to harvest hidden Web information.	Release 1C; Could / Release 2; Must
3.2.6.4.2.3.15.1	The harvester must be able to harvest content contained in query-based databases.	Release 1C; Could / Release 2; Must
3.2.6.4.2.3.15.2	The harvester must be able to harvest content contained in agency content management systems.	Release 1C; Could / Release 2; Must
3.2.6.4.2.3.15.3	The harvester must be able to harvest content contained on dynamically generated Web pages.	Release 1C; Could / Release 2; Must
3.2.6.4.2.3.15.4	The harvester must be able to harvest content contained on FTP servers.	Release 1C; Could / Release 2; Must
3.2.6.4.2.3.15.5	The harvester must be able to harvest content contained behind proxy servers.	Release 1C; Could / Release 2; Must

3.2.6.4.2.3.15.6	The harvester must be able to harvest content contained behind firewalls.	Release 1C; Could / Release 2; Must
3.2.6.4.2.3.16	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.	Release 2; Must
3.2.6.4.2.3.17	The harvester shall have the capability to time and date stamp content that has been harvested.	Release 2; Must

3.2.6.4.2.4	**Metadata Requirements for Harvester**	
3.2.6.4.2.4.1	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.	Release 2; Must
3.2.6.4.2.4.2	The harvester shall have the ability to locate and collect unique ID and title/caption information.	Release 2; Must
3.2.6.4.2.4.3	The harvester shall have the ability to locate and collect author/creator, publisher/authority, and rights owner information.	Release 2; Must
3.2.6.4.2.4.4	The harvester shall have the ability to locate and collect topical information and bibliographic descriptions.	Release 2; Must
3.2.6.4.2.4.5	The harvester shall have the ability to locate and collect version, fixity, relationship, and provenance information.	Release 2; Must
3.2.6.4.2.4.6	The harvester shall have the ability to locate and collect technical, structural, file format, packaging and representation information.	Release 2; Must
3.2.6.4.2.4.7	The harvester shall have the ability to locate and collect administrative metadata	Release 2; Must
3.2.6.4.2.4.8	The harvester shall have the capability to record the time and date of harvest.	Release 2; Must

3.2.6.4.2.5	**Harvester Rules and Instructions**	
3.2.6.4.2.5.1	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.	Release 2; Must

3.2.6.4.2.5.2	The harvester must accept and apply rules and instructions that will be used to assess whether discovered content is within scope of GPO dissemination programs.	Release 2; Must
3.2.6.4.2.5.3	The harvester must be able to create and store rule and instruction profiles for individual targeted Web sites.	Release 1C; Could / Release 2; Must

3.2.6.4.2.6	**Harvester Interface**	
3.2.6.4.2.6.1	The harvester shall provide a user interface to accommodate workflow management and scheduling of harvesting activities.	Release 2; Must
3.2.6.4.2.6.2	The user interface shall allow authorized users (GPO-specified) to schedule harvesting activities based on update schedules for targeted sites to be harvested.	Release 2; Must
3.2.6.4.2.6.2.1	Must accommodate the scheduling of harvests, including but not limited to hourly, daily, weekly, biweekly, monthly, and yearly.	Release 2; Must
3.2.6.4.2.6.3	The user interface must be able to manage rule and instruction profiles.	Release 1C; Could / Release 2; Must

3.2.6.4.2.7	**System Administration for Harvester**	
3.2.6.4.2.7.1	The harvester shall provide quality control functions to test accuracy/precision of rule application.	Release 1C; Could / Release 2; Must
3.2.6.4.2.7.2	The harvester shall be able to incorporate results of quality control functions into rule and instruction creation/refinement.	Release 1C; Could / Release 2; Must
3.2.6.4.2.7.3	The harvester shall have the capability to log and produce reports on harvesting activities.	Release 1C; Could / Release 2; Must
3.2.6.4.2.7.3.1	The harvester shall have the capability to log and report on Web sites visited by the harvester (e.g., date, time, frequency).	Release 2; Must
3.2.6.4.2.7.3.2	The harvester shall have the capability to log and report on content discovered, including location, title, description, and other relevant information.	Release 2; Must
3.2.6.4.2.7.3.3	The harvester shall have the capability to log and report on scope assessment decisions made by the harvester.	Release 2; Must
3.2.6.4.2.7.3.4	The harvester shall have the capability to log and report on target Web site structure, hierarchy, relationships, and directories.	Release 2; Must
3.2.6.4.2.7.3.5	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).	Release 2; Must
3.2.6.4.2.7.3.5.1	The harvester shall have the capability to log harvester failure or error rates (e.g. network problems, broken links, security rules, firewalls, corrupted content).	Release 2; Must

3.2.6.4.2.7.3.5.2	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).	Release 2; Must
3.2.6.4.2.7.3.6	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)	Release 1C; Could / Release 2; Must
3.2.6.4.2.7.4	The discovery and harvesting tools shall have the ability to identify GPO as the owner of the tools.	Release 2; Must
3.2.6.4.2.7.5	The harvester's method of identification shall not be intrusive to targeted Web site.	Release 2; Must
3.2.6.4.2.7.6	The harvester shall have the ability to collect integrity marks associated with content as it is being harvested.	Release 2; Must

3.2.6.5.2	Requirements for Style Tools	
3.2.6.5.2.1	**Style Tools Core Capabilities**	
3.2.6.5.2.1.1	Style tools shall accept content from authorized Content Originators, Service Providers, and Service Specialists for document creation.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.2	Style tools shall accept metadata from authorized users (e.g., title, author).	Release 2; Could / Release 3; Must
3.2.6.5.2.1.3	Style tools shall provide the capability for users to create new content for document creation.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.4	Style tools shall provide the capability for users to compose content for document creation including but not limited to text, images, and graphics.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.4.1	Style tools shall allow users to compose content based on pre-defined design rules.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.4.2	Style tools shall allow users to compose content using templates based on rules (e.g., agency style manuals).	Release 2; Could / Release 3; Must
3.2.6.5.2.1.4.3	Style tools shall have the capability to prompt users to define layout parameters from best available or system presented options.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.5	Style tools shall allow multiple users to work collaboratively on the same content, prior to publication.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.5.1	Style tools shall allow authorized users to approve/reject content changes made by collaborators.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.5.1.1	Style tools shall track approval/rejection of changes to content, prior to publication.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.5.1.2	Style tools shall allow for approval of content.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.5.1.3	Style tools shall allow for approval of content presentation.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.6	Style tools shall provide the capability to revert to a previously saved version of a working file (e.g., History palette).	Release 2; Could / Release 3; Must

3.2.6.5.2.1.7	Style tools shall provide the capability to track and undo changes to WIP content.	Release 2; Could / Release 3; Must
3.2.6.5.2.1.8	Style tools shall allow users to select output methods for viewing preliminary composition (i.e. Preparatory representation of content format or structure).	Release 2; Could / Release 3; Must
3.2.6.5.2.1.9	Style tools shall interface with Content Originator ordering.	Release 2; Could / Release 3; Must

3.2.6.5.2.2	**Style Tools - Automated Composition**	
3.2.6.5.2.2.1	Style tools shall have the capability to automatically compose content.	Release 2; Could / Release 3; Must
3.2.6.5.2.2.1.1	Style tools shall have the capability to automatically compose content and place graphical elements in locations using GPO or Agency guidelines.	Release 2; Could / Release 3; Must
3.2.6.5.2.2.1.2	Style tools shall have the capability to automatically compose content based on user preferences.	Release 2; Could / Release 3; Must
3.2.6.5.2.2.1.3	Style tools shall have the capability to automatically compose content based on content analysis.	Release 2; Could / Release 3; Must
3.2.6.5.2.2.2	Style tools shall allow users to modify automatically composed content.	Release 2; Could / Release 3; Must

3.2.6.5.2.3	**Style Tools - System Administration**	
3.2.6.5.2.3.1	The system shall accept content based on the access rights and privileges of the user submitting the content.	Release 2; Could / Release 3; Must
3.2.6.5.2.3.2	The system shall assign unique IDs to digital objects created by style tools.	Release 2; Could / Release 3; Must
3.2.6.5.2.3.3	The system shall provide storage for WIP style tools content.	Release 2; Could / Release 3; Must
3.2.6.5.2.3.3.1	The system shall allow management of WIP content based on access rights and privileges.	Release 2; Could / Release 3; Must
3.2.6.5.2.3.3.2	The system shall provide tracking of all WIP activities.	Release 2; Could / Release 3; Must
3.2.6.5.2.3.3.3	The system shall provide search and retrieval capabilities for WIP content.	Release 2; Could / Release 3; Must
3.2.6.5.2.3.4	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).	Release 2; Could / Release 3; Must
3.2.6.5.2.3.4.2.1	The system shall have the capability to provide authorized users with the ability to cancel a job.	Release 2; Should / Release 3; Must
3.2.6.5.2.3.4.2.2	The system shall have the capability to send or log notification of fulfillment to single or multiple users.	Release 2; Should / Release 3; Must
3.2.6.5.2.3.4.2.3	The system shall have the capability to provide notification of fulfillment based on the log of activities.	Release 2; Should / Release 3; Must
3.2.6.5.2.3.4.2.4	The system shall have the capability for users to specify the methods in which they receive fulfillment notification (e.g., email, alerts).	Release 2; Should / Release 3; Must
3.2.6.5.2.3.4.2.5	The system shall have the capability for users to elect not to receive notification of fulfillment.	Release 2; Should / Release 3; Must

3.2.6.5.2.3.4.2.6	The system shall allow authorized users to manage fulfillment notification.	Release 2; Should / Release 3; Must
3.2.6.5.2.3.5.1.1	The system shall have the capability to store multiple tracking numbers for each order.	Release 2; Should / Release 3; Must
3.2.6.5.2.3.5.1.2	The system shall provide a hyperlink to a fulfillment provider tracking website.	Release 2; Should / Release 3; Must
3.2.6.5.2.3.5.2.1	The system shall have the capability to receive multiple confirmations of fulfillment.	Release 2; Should / Release 3; Must

3.2.6.6.2 Requirements for Content Originator Ordering

3.2.6.6.2.1	**Content Originator Ordering Core Capabilities**	
3.2.6.6.2.1.1	The system shall provide a user interface for Content Originator ordering.	Release 1B; Must
3.2.6.6.2.1.2	The system shall have the capability to process jobs prior to content being approved for ingest.	Release 1C; Must
3.2.6.6.2.1.3	The system shall have the capability to process job orders (e.g. award jobs, send job order to Service Provider, receive order from Content Originator) prior to content being received.	Release 1C; Must
3.2.6.6.2.1.4	The system shall have the capability to track jobs using the job ID.	Release 2; Must
3.2.6.6.2.1.5	The system shall have the capability to accept and store a Content Originator supplied job tracking number in metadata.	Release 1B; Could / Release 1C; Must
3.2.6.6.2.1.5.1	The system shall have the capability to link the Content Originator supplied job tracking number to the Job ID.	Release 1B; Could / Release 1C; Must
3.2.6.6.2.1.5.2	The system shall allow users to update the Content Originator supplied job tracking number.	Release 1B; Could / Release 1C; Must
3.2.6.6.2.1.5.3	The system shall notify authorized allow users that a Content Originator supplied job tracking number has been updated.	Release 1B; Could / Release 1C; Must
3.2.6.6.2.1.5.4	The system shall allow users to search for the Content Originator supplied job tracking number.	Release 1B; Could / Release 1C; Must
3.2.6.6.2.1.6	The system shall have the capability to interface with select external agency systems in order to retrieve job orders.	Release 3; Could
3.2.6.6.2.1.7	The system shall adhere to policies set forth in GPO Publication 305.3.	Release 3; Must

3.2.6.6.2.2	**Content Originator Ordering - Job Management**	
3.2.6.6.2.2.1	The system shall provide the capability to acquire, store and edit BPI data on standard forms.	Release 1C; Must
3.2.6.6.2.2.1.1	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the Standard Form 1 (SF1).	Release 1C; Must

3.2.6.6.2.2.1.2	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 952.	Release 1C; Must
3.2.6.6.2.2.1.3	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 2511.	Release 1C; Must
3.2.6.6.2.2.1.4	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 3868.	Release 1C; Must
3.2.6.6.2.2.1.5	The system shall allow authorized users to add new BPI fields.	Release 1C; Must
3.2.6.6.2.2.1.6	The system shall provide the capability for a Content Originator to save BPI prior to submission to GPO.	Release 1C; Must
3.2.6.6.2.2.2	Deleted.	
3.2.6.6.2.2.2.1	The system shall ensure users are authorized to submit jobs.	Release 1C; Must
3.2.6.6.2.2.2.1.1	The system shall ensure users are authorized to spend funds.	Release 1C; Must
3.2.6.6.2.2.2.2	Deleted.	
3.2.6.6.2.2.2.3	The system shall support credential technologies (e.g. PKI) per the FDsys security requirements.	Release 2; Must
3.2.6.6.2.2.3	The system shall provide the capability for users to search all job specifications.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.3.1	The system shall provide the capability for users to search job specifications related to a user account or agency.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.4	The system shall have the capability to identify similar jobs and specifications (e.g., strapping jobs) that have not been awarded.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.4.1	The system shall notify Service Specialists of similar jobs and job specifications.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.5	The system shall have the capability to inform Content Evaluators that a new order has been placed by a Content Originator.	Release 3; Must
3.2.6.6.2.2.6	The system shall have the capability to support job riders.	Release 3; Must
3.2.6.6.2.2.7	The system shall provide the capability to notify authorized users that riders have been placed on their job order.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.8	The system shall provide the capability to notify users that GPO is accepting riders for a job order.	Release 3; Must
3.2.6.6.2.2.9	The system shall have the capability to determine contract types (e.g., onetime bids, SPA, term contract) based upon specification and business rules.	Release 3; Could
3.2.6.6.2.2.10	The system shall allow authorized users to specify a contract type.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.10.1	The system shall provide the capability for Content Originators to specify an existing contract (e.g., SPA, Term contract).	Release 2; Should / Release 3; Must

3.2.6.6.2.2.11	The system shall allow users to view a history of all previous jobs based on user rights.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.12	The system shall provide estimated costs for GPO products and services for jobs to users based upon user provided job specifications.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.12.1	The system shall have the capability to allow authorized users to enter an estimate for a job.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.13	The system shall provide the capability for authorized users to edit job specifications (e.g., quantity, number of colors) prior to contract award.	Release 1C; Must
3.2.6.6.2.2.14	The system shall have the capability to notify users that a job specification has been edited.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.15	The system shall provide the capability for Content Originators to specify content delivery options.	Release 1C; Must
3.2.6.6.2.2.15.1	The system shall provide the capability for Content Originators to specify hard copy Content Delivery options.	Release 1C; Must
3.2.6.6.2.2.15.2	The system shall provide the capability for Content Originators to specify electronic presentation Content Delivery options.	Release 1C; Must
3.2.6.6.2.2.15.3	The system shall provide the capability for Content Originators to specify digital media Content Delivery options.	Release 1C; Must
3.2.6.6.2.2.16	The system shall allow users to select fulfillment options for content delivery.	Release 3; Must
3.2.6.6.2.2.16.1	The system shall provide the capability to configure the tangible content delivery options.	Release 3; Must
3.2.6.6.2.2.16.2	The system shall provide the capability to enter multiple shipping and delivery destinations.	Release 1C; Must
3.2.6.6.2.2.16.2.1	The system shall allow users to attach distribution list files to a job order.	Release 1C; Must
3.2.6.6.2.2.16.2.2	The system shall be capable of extracting shipping and delivery destinations from attached distribution list files.	Release 3; Must
3.2.6.6.2.2.16.2.3	The system shall provide the capability to store shipping and delivery destinations in their user profile.	Release 3; Must
3.2.6.6.2.2.16.2.4	The system shall be able to provide distribution list information to authorized users.	Release 3; Must
3.2.6.6.2.2.16.3	The system shall provide the capability for Content Originators to select ship, fulfillment, mail, or pickup dates.	Release 3; Must
3.2.6.6.2.2.16.3.1	The system shall provide the capability for users to select zero or more ship dates for each destination in an order.	Release 3; Must
3.2.6.6.2.2.16.3.2	The system shall provide the capability for users to select zero or more delivery dates for each destination in an order.	Release 3; Must
3.2.6.6.2.2.16.3.3	The system shall provide the capability for users to select zero or more pickup dates for each destination in an order.	Release 3; Must

3.2.6.6.2.2.16.4	The system shall provide the capability for users to select shipping providers from a configurable list.	Release 3; Must
3.2.6.6.2.2.16.5	The system shall have the capability to provide estimated shipping costs based upon job specifications.	Release 3; Could
3.2.6.6.2.2.16.6	The system shall have the capability to allow Content Originators and Service Specialists to select the appropriate method for content fulfillment.	Release 3; Must
3.2.6.6.2.2.17	The system shall maintain Service Provider information.	Release 3; Must
3.2.6.6.2.2.17.1	Authorized users shall have the capability to access Service Provider information.	Release 3; Must
3.2.6.6.2.2.17.2	The system shall provide the capability for users to create Service Provider information.	Release 3; Must
3.2.6.6.2.2.17.2.1	The system shall provide the capability for authorized users to edit Service Provider information.	Release 3; Must
3.2.6.6.2.2.17.2.2	The system shall provide the capability for authorized users to delete Service Provider information.	Release 3; Must
3.2.6.6.2.2.17.2.1	Service Provider contact information shall include the company name.	Release 3; Must
3.2.6.6.2.2.17.2.1.1	Service Provider contact information shall include the physical address.	Release 3; Must
3.2.6.6.2.2.17.2.1.2	Service Provider contact information shall include the mailing address.	Release 3; Must
3.2.6.6.2.2.17.2.1.3	Service Provider contact information shall include the shipping address.	Release 3; Must
3.2.6.6.2.2.17.2.1.4	Service Provider contact information shall include the names of zero or more contact personnel.	Release 3; Must
3.2.6.6.2.2.17.2.1.5	Service Provider contact information shall include zero or more phone numbers.	Release 3; Must
3.2.6.6.2.2.17.2.1.6	Service Provider contact information shall include zero or more cell phone numbers.	Release 3; Must
3.2.6.6.2.2.17.2.1.7	Service Provider contact information shall include zero or more e-mail address.	Release 3; Must
3.2.6.6.2.2.17.2.1.8	Service Provider contact information shall include zero or more fax numbers.	Release 3; Must
3.2.6.6.2.2.17.2.1.9	Service Provider contact information shall include the state code.	Release 3; Must
3.2.6.6.2.2.17.2.1.10	Service Provider contact information shall include the contractor code.	Release 3; Must
3.2.6.6.2.2.17.2.2	Deleted.	
3.2.6.6.2.2.17.3	Deleted.	
3.2.6.6.2.2.17.3.1	The system shall allow authorized users to manage a list of equipment categories.	Release 2; Could / Release 3; Must
3.2.6.6.2.2.17.3.1.1	Service Providers shall be able to specify the equipment categories they meet from a predefined list.	Release 2; Could / Release 3; Must
3.2.6.6.2.2.17.3.1.2	Service Providers shall be able to manage their equipment categories from a predefined list.	Release 2; Could / Release 3; Must

3.2.6.6.2.2.17.3.1.3	The system shall provide a text field for Service Providers to specify specific equipment they utilize.	Release 2; Could / Release 3; Must
3.2.6.6.2.2.17.4	Service Providers shall be able to specify products and services that they are capable of providing from a configurable list.	Release 3; Must
3.2.6.6.2.2.17.4.1	The system shall allow authorized users to manage a configurable list of products and services.	Release 3; Must
3.2.6.6.2.2.17.4.2	The system shall allow Service Providers to input customized capabilities not included on the configurable list in a note field.	Release 3; Must
3.2.6.6.2.2.17.5	Deleted.	
3.2.6.6.2.2.17.6	The system shall maintain Service Provider performance information comprised of quality history, quality level, compliance history, and notices.	Release 3; Must
3.2.6.6.2.2.17.6.1	The system shall allow authorized users to manage Service Provider performance information.	Release 3; Must
3.2.6.6.2.2.17.6.2	Quality levels shall be assigned by authorized GPO personnel in accordance with GPO Publication 310.1.	Release 3; Must
3.2.6.6.2.2.17.6.3	Service Provider information shall include quality history data.	Release 3; Must
3.2.6.6.2.2.17.6.3.1	Quality history data shall include the number of jobs completed at given quality levels.	Release 3; Must
3.2.6.6.2.2.17.6.3.2	Quality history data shall include the number of jobs inspected at given quality level	Release 3; Must
3.2.6.6.2.2.17.6.3.3	Quality history data shall include the number of jobs rejected at given quality levels	Release 3; Must
3.2.6.6.2.2.17.6.4	Service Provider information shall include compliance history data.	Release 3; Must
3.2.6.6.2.2.17.6.4.1	Compliance history shall include the number of jobs completed.	Release 3; Must
3.2.6.6.2.2.17.6.4.2	Compliance history shall include the number of jobs completed late	Release 3; Must
3.2.6.6.2.2.17.6.4.3	Compliance history shall include the percentage of job completed late.	Release 3; Must
3.2.6.6.2.2.17.6.5	Service Provider information shall include notices.	Release 3; Must
3.2.6.6.2.2.17.6.5.1	Notices received shall include the number of cure notices.	Release 3; Must
3.2.6.6.2.2.17.6.5.2	Notices received shall include the number of show-cause notices.	Release 3; Must
3.2.6.6.2.2.17.6.5.3	Notices received shall include the number of shipped short letters.	Release 3; Must
3.2.6.6.2.2.17.6.5.4	Notices received shall include the number of do not condone letters.	Release 3; Must
3.2.6.6.2.2.17.6.5.5	Notices received shall include the number of terminations for default (program).	Release 3; Must
3.2.6.6.2.2.17.6.5.6	Notices received shall include the number of terminations for default (orders).	Release 3; Must
3.2.6.6.2.2.17.6.5.7	Notices received shall include the number of erroneous information letters.	Release 3; Must

3.2.6.6.2.2.17.6.5.8	Notices received shall include the number of non-responsible quality history letters.	Release 3; Must
3.2.6.6.2.2.17.6.5.9	Notices received shall include the number of non-responsible performance letters.	Release 3; Must
3.2.6.6.2.2.17.6.5.10	Notices received shall include the number of non-responsible other letters.	Release 3; Must
3.2.6.6.2.2.17.6.5.11	Notices received shall include the number of exception clause letters	Release 3; Must
3.2.6.6.2.2.17.6.6	Service Provider information shall include note text field.	Release 3; Must
3.2.6.6.2.2.18	The system shall provide the capability to search Service Provider information.	Release 3; Must
3.2.6.6.2.2.19	The system shall generate a list of Service Providers in response to a user search request.	Release 3; Must
3.2.6.6.2.2.19.1	Deleted.	
3.2.6.6.2.2.20	The system shall allow authorized users to generate solicitations.	Release 3; Must
3.2.6.6.2.2.20.1	The system shall distribute solicitations.	Release 3; Must
3.2.6.6.2.2.21	The system shall accept bids from Service Providers for jobs.	Release 3; Must
3.2.6.6.2.2.21.0.1	The system shall allow authorized users to submit bid information.	Release 3; Must
3.2.6.6.2.2.21.1	The system shall accept bids with zero to many line items.	Release 3; Must
3.2.6.6.2.2.21.2	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).	Release 3; Must
3.2.6.6.2.2.21.3	The system shall electronically stamp bids with the time it was received.	Release 3; Must
3.2.6.6.2.2.21.3.1	The system shall electronically stamp bids with the date it was received.	Release 3; Must
3.2.6.6.2.2.21.3.2	The system shall electronically stamp bids with user profile information.	Release 3; Must
3.2.6.6.2.2.21.3.3	The system shall allow authorized users to enter electronic stamp information when tangible bids are received.	Release 3; Must
3.2.6.6.2.2.21.4	The system shall allow authorized users to electronically post bid results.	Release 3; Must
3.2.6.6.2.2.22	The system shall allow Service Specialists and Content Originators to award jobs to Service Providers.	Release 3; Must
3.2.6.6.2.2.22.1	Deleted.	
3.2.6.6.2.2.23	The system shall allow authorized users to request contract modifications.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.24	The system shall allow authorized users to approve contract modifications.	Release 2; Should / Release 3; Must
3.2.6.6.2.2.24.1	The system shall allow authorized users to manage contract modifications.	Release 2; Should / Release 3; Must

3.2.6.6.2.2.25	Deleted.	
3.2.6.6.2.2.26	The system shall provide the capability for users to request re-orders.	Release 3; Must

3.2.6.6.2.3	**Content Originator Ordering - Job Tracking**	
3.2.6.6.2.3.1	The system shall have the capability to log activities and communications between users	Release 3; Must
3.2.6.6.2.3.1.0.1	Activities and communications include that the job was made available to Service Provider.	Release 3; Must
3.2.6.6.2.3.1.0.2	Activities and communications include that the job was received by Service Provider.	Release 3; Must
3.2.6.6.2.3.1.0.3	Activities and communications include that the proofs were sent to Content Originator	Release 3; Must
3.2.6.6.2.3.1.0.4	Activities and communications include that the proofs were received by Content Originator	Release 3; Must
3.2.6.6.2.3.1.0.5	Activities and communications include that the proofs were approved.	Release 3; Must
3.2.6.6.2.3.1.0.6	Activities and communications include that the proofs were approved with author's alterations.	Release 3; Must
3.2.6.6.2.3.1.0.7	Activities and communications include that the proofs were approved with Service Provider's errors.	Release 3; Must
3.2.6.6.2.3.1.0.8	Activities and communications include that new proofs were requested due to author's alterations.	Release 3; Must
3.2.6.6.2.3.1.0.9	Activities and communications include that new proofs were requested due to Service Provider's errors	Release 3; Must
3.2.6.6.2.3.1.0.10	Activities and communications include that proofs were sent to Service Provider.	Release 3; Must
3.2.6.6.2.3.1.0.11	Activities and communications include that proofs were received by Service Provider.	Release 3; Must
3.2.6.6.2.3.1.0.12	Activities and communications include that changes were made by Content Originator.	Release 3; Must
3.2.6.6.2.3.1.0.13	Activities and communications include that changes were made by Service Provider.	Release 3; Must
3.2.6.6.2.3.10..14	Activities and communications include that the job is complete.	Release 3; Must
3.2.6.6.2.3.1.0.15	Activities and communications include that the job is delivered to each individual destination.	Release 3; Must
3.2.6.6.2.3.1.0.16	Activities and communications include job shipped to all destinations.	Release 3; Must
3.2.6.6.2.3.1.0.17	Activities and communications include job delivered to all destinations.	Release 3; Must
3.2.6.6.2.3.1.0.18	Activities and communications include job delivery receipts are available.	Release 3; Must
3.2.6.6.2.3.1.0.19	Activities and communications include type of communication (e.g., telephone, meeting, e-mail).	Release 3; Must
3.2.6.6.2.3.1.0.20	Activities and communications include Job ID referenced,	Release 3; Must

3.2.6.6.2.3.1.0.21	Activities and communications include approved for publication.	Release 3; Must
3.2.6.6.2.3.1.1	The system shall provide a means to add notes to each job.	Release 3; Must
3.2.6.6.2.3.2	The system shall provide the capability to automatically request job status information from users.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.2.1	Deleted.	
3.2.6.6.2.3.2.2	The system shall have the capability for authorized users to request automated notifications of job activities.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.3	The system shall allow Service Specialists to generate notifications to Service Providers and Content Originators.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.3.1	The system shall allow Service Specialists to distribute notification to Service Providers and Content Originators.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.3.2	Notifications include show cause notices.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.3.3	Notifications include cure notices.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.3.4	Notifications include GPO Form 907.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.4	The system shall have the capability to provide shipping notification to authorized users.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.4.0.1	The system shall have the capability to provide delivery notification to authorized users.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.4.1	Notification of delivery shall include tracking numbers from the Service Provider.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.4.1.1	Notification of delivery shall include signed delivery receipts.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.4.1.2	The system shall have the capability to upload digitized signed delivery receipts.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.4.1.3	Notification of delivery shall include confirmation of delivery from agency recipients.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.4.2	The system shall have the capability to provide users with options in response to undelivered content (e.g., resubmit content, cancel fulfillment).	Release 2; Should / Release 3; Must
3.2.6.6.2.3.5	Deleted.	
3.2.6.6.2.3.5.1	The system shall have the capability to receive and store product delivery tracking numbers (e.g., Fed-Ex Tracking Number) from Service Providers.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.5.2	The system shall have the capability to receive confirmation of delivery from the agency or end user.	Release 2; Should / Release 3; Must
3.2.6.6.2.3.6	The system shall have the capability to support Job Definition Format (JDF).	Release 3; Could

3.2.7.2	**Requirements for Access Content Processing**	
3.2.7.2.1	**Access Core Capabilities**	

3.2.7.2.1.1	The system shall provide open and interoperable access to content.	Release 1B; Must
3.2.7.2.1.2	The system must provide open and interoperable access to metadata.	Release 1B; Must
3.2.7.2.1.3	The system shall provide access to content at the minimum level of granularity that is specified in the FDsys unique ID requirements.	Release 1B; Must
3.2.7.2.1.4	The system shall provide the capability for users to use persistent names to access content.	Release 1C; Must
3.2.7.2.1.5	The system shall provide the capability for users to access content that has been published in non-English languages and non-Roman character sets.	Release 3; Must
3.2.7.2.1.6	The system shall provide the capability for users to access information about content relationships.	Release 1B; Must
3.2.7.2.1.6.1	The system shall provide the capability for users to access information about relationships between content packages.	Release 1B; Must
3.2.7.2.1.6.2	The system shall provide the capability for users to access information about relationships between digital objects.	Release 1B; Must
3.2.7.2.1.6.3	The system shall provide the capability for users to access information about relationships between digital objects and content packages.	Release 1B; Must
3.2.7.2.1.6.4	The system shall enforce the continuity of content in context.	Release 1B; Must
3.2.7.2.1.6.5	The system shall provide the capability to access content based on relationships between versions of a Congressional bill.	Release 1C; Must
3.2.7.2.1.6.6	The system shall provide the capability to access content based on relationships between publications that are used in the Federal legislative process.	Release 1C; Must
3.2.7.2.1.6.7	The system shall provide the capability to access content based on relationships between publications that are used in the Federal regulatory process.	Release 1C; Must
3.2.7.2.1.6.8	The system shall provide the capability to access content based on relationships between Supreme Court publications that are part of the opinion process.	Release 1C; Must
3.2.7.2.1.7	The system shall provide the capability to use GPO's ILS to access metadata repositories not resident within the system.	Release 2; Must
3.2.7.2.1.8	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including the following:	Release 2; Must
3.2.7.2.1.8.1	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.	Release 2; Must

3.2.7.2.1.8.2	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.	Release 2; Must
3.2.7.2.1.8.3	CyberCemetery (University of North Texas): Provide permanent online access to electronic publications of selected federal Government agencies which have ceased operation.	Release 2; Must
3.2.7.2.1.8.4	FRASER (Federal Reserve Bank of St. Louis): Provides for public access to content in the Federal Reserve Archival System for Economic Research (FRASER) service.	Release 2; Must
3.2.7.2.1.8.5	National Library of Medicine: Provides permanent public access to Medline, Medical Subject Headings, and NLM LocatorPlus.	Release 2; Must
3.2.7.2.1.8.6	National Renewable Energy Laboratory: Provides permanent public access to NREL's laboratory and outreach publications.	Release 2; Must

3.2.7.2.2	**Access to Content Packages**	
3.2.7.2.2.1	The system must provide the capability for GPO to manage access to content packages according to GPO business rules.	Release 2; Must
3.2.7.2.2.2	The system shall accept access rules for content packages.	Release 1C; Must
3.2.7.2.2.3	The system shall provide the capability to limit access to content with re-dissemination restrictions as specified by authorized users.	Release 1C; Must
3.2.7.2.2.4	The system shall provide the capability to limit access to content with limited distribution as specified by authorized users.	Release 1C; Must
3.2.7.2.2.5	The system shall provide the capability to limit access to Sensitive But Unclassified (SBU) content as specified by authorized users.	Release 1C; Must
3.2.7.2.2.6	The system shall provide the capability to limit access to copyrighted content as specified by authorized users.	Release 1C; Must
3.2.7.2.2.7	The system shall provide the capability to limit access to content that is out of scope for GPO's dissemination programs.	Release 1C; Must
3.2.7.2.2.8	The system shall provide the capability to limit access to content that has not been approved by authorized users for public release.	Release 1C; Must
3.2.7.2.2.9	The system shall provide the capability to limit access to embargoed content until the appropriate release date and time as specified by authorized users.	Release 1C; Must
3.2.7.2.2.10	The system must provide the capability to limit access to content based on criteria specified by the Content Originator.	Release 1C; Must

3.2.7.2.2.10.1	The system shall provide the capability to limit access to content based on criteria specified by authorized users.	Release 1C; Must
3.2.7.2.2.11	The system must provide access to content currently available on GPO Access.	Release 1C; Must
3.2.7.2.2.11.1	The system shall provide the capability for users to access select publications enumerated in 7.4.2.2.4.b at a level of granularity that is less than a publication.	Release 1C; Must
3.2.7.2.2.11.2	The system shall provide the capability to create persistent links to renditions of publications listed in 4.7.2.2.4.b (list of GPO Access applications).	Release 1C; Must
3.2.7.2.2.11.2.1	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.	Release 1C; Must
3.2.7.2.2.11.2.2	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.	Release 1C; Must
3.2.7.2.2.11.2.3	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.	Release 1C; Must
3.2.7.2.2.11.2.4	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.	Release 1C; Must
3.2.7.2.2.11.2.5	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.	Release 1C; Must
3.2.7.2.2.11.2.6	The system shall provide the capability to create predictable links to renditions of publications listed in 4.7.2.2.4.b (list of GPO Access applications).	Release 1C; Must
3.2.7.2.2.11.2.7	The system shall provide the capability for internal linking of publications listed in 4.7.2.2.4.b (list of GPO Access applications) at all available levels of granularity.	Release 1C; Must
3.2.7.2.2.11.2.8	The system shall provide the capability to link Congressional bill citations in digital objects to appropriate versions of Congressional bill renditions.	Release 1C; Must
3.2.7.2.2.11.2.9	The system shall provide the capability to link public law citations in digital objects to appropriate versions of public law renditions.	Release 1C; Must
3.2.7.2.2.11.2.10	The system shall provide the capability to link United States Code citations in digital objects to appropriate versions of United States Code renditions.	Release 1C; Must
3.2.7.2.2.11.2.11	The system shall provide the capability to link Statutes at Large citations in digital objects to appropriate versions of Statutes at Large renditions.	Release 1C; Must

3.2.7.2.2.11.2.12	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.	Release 1C; Must
3.2.7.2.2.11.2.13	The system shall provide the capability to link Congressional Record citations in digital objects to appropriate versions of Congressional Record renditions.	Release 1C; Must
3.2.7.2.2.11.2.14	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.	Release 1C; Must
3.2.7.2.2.11.2.15	The system shall provide the capability to link Federal Register citations in digital objects to appropriate versions of Federal Register renditions.	Release 1C; Must
3.2.7.2.2.11.2.16	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.	Release 1C; Must
3.2.7.2.2.11.2.17	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.	Release 1C; Must
3.2.7.2.2.11.2.18	The system shall provide the capability to link Bound Congressional Record citations in digital objects to appropriate versions of Bound Congressional Record renditions.	Release 1C; Must
3.2.7.2.2.11.2.19	The system shall provide the capability to link Congressional Hearing citations in digital objects to appropriate versions of Congressional Hearing renditions.	Release 1C; Must
3.2.7.2.2.11.2.20	The system shall provide the capability to link Congressional Report citations in digital objects to appropriate versions of Congressional Report renditions.	Release 1C; Must
3.2.7.2.2.11.2.21	The system shall provide the capability to link Congressional Document citations in digital objects to appropriate versions of Congressional Document renditions.	Release 1C; Must
3.2.7.2.2.11.2.22	The system shall provide the capability to link Congressional Calendar citations in digital objects to appropriate versions of Congressional Calendar renditions.	Release 1C; Must
3.2.7.2.2.11.2.23	The system shall provide the capability to link Congressional Committee Print citations in digital objects to appropriate versions of Congressional Committee Print renditions.	Release 1C; Must
3.2.7.2.2.11.2.24	The system shall provide the capability to manage links as managed objects.	Release 1C; Must
3.2.7.2.2.12	The system shall provide the capability to notify users of limitations on access to content.	Release 1C; Must

3.2.7.2.2.13	The system shall provide the capability to provide customized access to content packages.	Release 1C; Should / Release 2; Must
3.2.7.2.2.14	The system shall provide the capability to provide personalized access to content packages.	Release 1C; Could / Release 2; Must
3.2.7.2.2.15	The system shall provide the capability for users to access in scope final published versions of ACPs.	Release 1B; Could / Release 1C; Must
3.2.7.2.2.16	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.	Release 1C; Must

3.2.7.2.3	**Access to the System**	
3.2.7.2.3.1	The system shall have the capability to provide access to system functions by user class.	Release 1C; Must
3.2.7.2.3.2	The system shall provide access to public End Users that does not require them to log-in or register with the system.	Release 1B; Must
3.2.7.2.3.2.1	The system shall provide access to public End Users that does not require them to log-in to the system.	Release 1B; Must
3.2.7.2.3.2.2	The system shall provide access to public End Users that does not require them to register with the system.	Release 1B; Must
3.2.7.2.3.3	The system shall provide the capability for authorized users to access WIP storage.	Release 1B; Must
3.2.7.2.3.3.1	The system shall have the capability to allow authorized users to authorize access to content in WIP.	Release 1B; Must
3.2.7.2.3.3.2	The system shall provide "check in and check out" capabilities for content in WIP.	Release 1B; Could / Release 1C; Must
3.2.7.2.3.3.2.1	The system shall provide check out of work in progress content	Release 1B; Could / Release 1C; Must
3.2.7.2.3.3.2.1.1	The system shall not allow other users to modify content when one user has checked it out	Release 1B; Could / Release 1C; Must
3.2.7.2.3.3.2.1.2	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	Release 1B; Could / Release 1C; Must
3.2.7.2.3.3.2.1.3	The system shall allow authorized users to release locks on content	Release 1B; Could / Release 1C; Must
3.2.7.2.3.3.2.2	The system shall link all versions of work in progress content	Release 1B; Could / Release 1C; Must
3.2.7.2.3.3.2.3	The system shall allow users to check in content.	Release 1B; Could / Release 1C; Must
3.2.7.2.3.4	Deleted.	
3.2.7.2.3.5	Deleted.	

3.2.7.2.4	**Access - User Registration**	
3.2.7.2.4.1	The system shall provide the capability for users to register with the system.	Release 1B; Must

3.2.7.2.4.2	The system shall provide the capability to establish a user account for each registered user.	Release 1B; Must
3.2.7.2.4.3	The system shall provide the capability to create user records for registered users.	Release 1B; Must
3.2.7.2.4.4	The system shall have capability to store and manage an unlimited number of user records.	Release 1B; Must
3.2.7.2.4.4.1	The system shall have the capability to store an unlimited number of user records.	Release 1B; Must
3.2.7.2.4.4.2	The system shall have the capability to manage an unlimited number of user records.	Release 1B; Must
3.2.7.2.4.5	The system shall provide the capability for authorized users to access user records.	Release 1B; Must
3.2.7.2.4.6	The system shall provide the capability for authorized users to set required fields in user records.	Release 1C; Must
3.2.7.2.4.7	The system shall provide the capability to record information submitted by users during registration with system.	Release 1B; Must
3.2.7.2.4.8	The system shall provide the capability for GPO to customize what information is collected during user registration.	Release 2; Must
3.2.7.2.4.8.1	The system shall have the capability to collect name from the user during registration (e.g., honorific title, first name, last name, job title).	Release 1C; Must
3.2.7.2.4.8.2	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).	Release 1C; Must
3.2.7.2.4.8.3	Deleted.	
3.2.7.2.4.8.4	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).	Release 2; Must
3.2.7.2.4.8.4.1	Users may be members of multiple user classes simultaneously.	Release 1B; Must
3.2.7.2.4.8.4.2	The system shall associate registered users with at least one user class.	Release 1C; Must
3.2.7.2.4.8.5	The system shall provide the capability to collect role-based information from the user during registration.	Release 1C; Must
3.2.7.2.4.8.6	The system shall provide the capability to collect proof of identity information from the user during registration.	Release 2; Must
3.2.7.2.4.8.7	The system shall provide the capability to collect authority to publish information from the user during registration.	Release 2; Must
3.2.7.2.4.9	The system shall provide the capability to perform records management functions on user records.	Release 1C; Must

3.2.7.2.5	**Access - User Preferences**	
3.2.7.2.5.1	The system shall provide the capability for authorized users to manage the following user preferences:	Release 1C; Should / Release 2; Must
3.2.7.2.5.1.1	Preferred contact methods	Release 2; Must
3.2.7.2.5.1.2	Delivery options	Release 2; Must
3.2.7.2.5.1.3	User interfaces	Release 2; Must
3.2.7.2.5.1.4	Alert services	Release 2; Must
3.2.7.2.5.1.5	Help features	Release 2; Must
3.2.7.2.5.1.6	Frequently accessed tools	Release 2; Must
3.2.7.2.5.1.7	Search preferences	Release 2; Must
3.2.7.2.5.1.8	The system shall provide the capability for authorized users to manage future user preferences.	Release 2; Must
3.2.7.2.5.2	The system shall provide the capability for authorized users to manage other users' preferences.	Release 1C; Should / Release 2; Must
3.2.7.2.5.3	The system shall provide the capability for GPO to establish and manage default user preferences.	Release 1C; Should / Release 2; Must
3.2.7.2.5.4	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.	Release 1C; Could / Release 2; Must
3.2.7.2.5.5	Deleted.	
3.2.7.2.5.6	Deleted.	

3.2.7.2.6	**Access Processing**	
3.2.7.2.6.1	The system shall provide the capability to process and manage ACPs.	Release 1C; Must
3.2.7.2.6.1.1	The system shall provide the capability to process and manage digital objects that are used for access.	Release 2; Must
3.2.7.2.6.1.2	The system shall provide the capability to manage metadata that are used for access.	Release 2; Must
3.2.7.2.6.2	The system shall provide the capability to create access derivatives.	Release 2; Must
3.2.7.2.6.3	Deleted.	
3.2.7.2.6.4	Deleted.	
3.2.7.2.6.5	The system shall provide the capability for access processing to request that an ACP be modified or created from an AIP.	Release 1C; Must
3.2.7.2.6.6	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.	Release 2; Must
3.2.7.2.6.6.1	The system shall provide content to delivery processing for the purpose of fulfilling an End User request.	Release 2; Must

3.2.7.2.6.6.2	The system shall provide metadata to delivery processing for the purpose of fulfilling an End User request.	Release 2; Must
3.2.7.2.6.6.3	The system shall provide business process information to delivery processing for the purpose of fulfilling an End User request.	Release 2; Must
3.2.7.2.6.6.4	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.	Release 2; Must
3.2.7.2.6.6.5	The system shall provide content to delivery processing for the purpose of fulfilling an Content Originator order.	Release 2; Must
3.2.7.2.6.6.6	The system shall provide metadata to delivery processing for the purpose of fulfilling an Content Originator order.	Release 2; Must
3.2.7.2.6.6.7	The system shall provide business process information to delivery processing for the purpose of fulfilling a Content Originator order.	Release 2; Must
3.2.7.2.6.6.8	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.	Release 2; Must
3.2.7.2.6.7	The system shall provide the capability to perform records management functions on ACPs.	Release 2; Must
3.2.7.2.6.7.1	Records management functions shall comply with GPO and Federal records management policies.	Release 2; Must
3.2.7.2.6.7.2	Records management functions shall be performed according to records management schedules for content and metadata within the system.	Release 2; Must
3.2.7.2.6.8	The system shall provide the capability to identify and manage relationships between digital objects, between content packages, and between digital objects and content packages.	Release 2; Must
3.2.7.2.6.8.1	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.	Release 2; Must
3.2.7.2.6.8.2	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.	Release 2; Must

3.2.7.3.2	**Requirements for Accessibility**	
3.2.7.3.2.1	**Accessibility Core Capabilities**	
3.2.7.3.2.1.1	The system must provide the capability to assess content for compliance with Section 508 technical standards.	Release 2; Must

3.2.7.3.2.1.1.1	The system shall provide the capability to assess all content for compliance with Section 508 technical standards.	Release 2; Must
3.2.7.3.2.1.1.2	The system shall provide the capability to assess content available in release 1c for compliance with Section 508 technical standards.	Release 1C; Must
3.2.7.3.2.1.2	The system shall provide the capability to create content that is compliant with Section 508 technical standards.	Release 2; Must
3.2.7.3.2.1.3	The system shall provide the capability to validate content for compliance with Section 508 technical standards.	Release 2; Must
3.2.7.3.2.1.4	The system shall accept accessibility requirements and implementation guidance from Content Originators.	Release 2; Must
3.2.7.3.2.1.5	The system shall provide Section 508 compliant access to the system.	Release 1C; Must
3.2.7.3.2.1.6	In order to achieve compliance with Section 508 technical standards, established best practices shall be followed.	Release 2; Could
3.2.7.3.2.1.7	The system shall create content that contains well formed code which conforms to World Wide Web Consortium (W3C) Guidelines.	Release 2; Must

3.2.7.3.2.2	**Accessibility - Section 508 Technical Standards**	
3.2.7.3.2.2.1	FDsys software applications and operating systems shall be Section 508 compliant according to 36 CFR Part 1194.21.	Release 2; Should
3.2.7.3.2.2.1.1	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.	Release 2; Should
3.2.7.3.2.2.1.2	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.	Release 2; Should
3.2.7.3.2.2.1.3	An on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes.	Release 2; Should
3.2.7.3.2.2.1.3.1	The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.	Release 2; Should

3.2.7.3.2.2.1.4	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.	Release 2; Should
3.2.7.3.2.2.1.5	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.	Release 2; Should
3.2.7.3.2.2.1.6	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.	Release 2; Should
3.2.7.3.2.2.1.7	Applications shall not override user selected contrast and color selections and other individual display attributes.	Release 2; Should
3.2.7.3.2.2.1.8	When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	Release 2; Should
3.2.7.3.2.2.1.9	Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Release 2; Should
3.2.7.3.2.2.1.10	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.	Release 2; Should
3.2.7.3.2.2.1.11	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.	Release 2; Should
3.2.7.3.2.2.1.12	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.	Release 2; Should
3.2.7.3.2.2.2	FDsys Web-based intranet and internet information and applications shall be Section 508 compliant according to 36 CFR Part 1194.22.	Release 2; Should
3.2.7.3.2.2.2.1	A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	Release 2; Should
3.2.7.3.2.2.2.2	Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Release 2; Should
3.2.7.3.2.2.2.3	Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	Release 2; Should
3.2.7.3.2.2.2.4	Documents shall be organized so they are readable without requiring an associated style sheet.	Release 2; Should

3.2.7.3.2.2.2.5	Redundant text links shall be provided for each active region of a server-side image map.	Release 2; Should
3.2.7.3.2.2.2.6	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.	Release 2; Should
3.2.7.3.2.2.2.7	Row and column headers shall be identified for data tables.	Release 2; Should
3.2.7.3.2.2.2.8	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.	Release 2; Should
3.2.7.3.2.2.2.9	Frames shall be titled with text that facilitates frame identification and navigation.	Release 2; Should
3.2.7.3.2.2.2.10	Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Release 2; Should
3.2.7.3.2.2.2.11	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	Release 2; Should
3.2.7.3.2.2.2.12	When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.	Release 2; Should
3.2.7.3.2.2.2.13	When a web page requires another application be present on the client system to interpret page content the page must provide a link to the required tool that complies with §1194.21(a) through (l).	Release 2; Should
3.2.7.3.2.2.2.13.1	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 must provide a link to a plug-in or applet that complies with §1194.21(a).	Release 2; Should
3.2.7.3.2.2.2.13.2	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 must provide a link to a plug-in or applet that complies with §1194.21(b).	Release 2; Should
3.2.7.3.2.2.2.13.3	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 must provide a link to a plug-in or applet that complies with §1194.21(c).	Release 2; Should
3.2.7.3.2.2.2.13.4	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 must provide a link to a plug-in or applet that complies with §1194.21(d).	Release 2; Should
3.2.7.3.2.2.2.13.5	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 must provide a link to a plug-in or applet that complies with §1194.21(e).	Release 2; Should

3.2.7.3.2.2.2.13.6	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 must provide a link to a plug-in or applet that complies with §1194.21(f).	Release 2; Should
3.2.7.3.2.2.2.13.7	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 must provide a link to a plug-in or applet that complies with §1194.21(g).	Release 2; Should
3.2.7.3.2.2.2.13.8	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 must provide a link to a plug-in or applet that complies with §1194.21(h).	Release 2; Should
3.2.7.3.2.2.2.13.9	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 must provide a link to a plug-in or applet that complies with §1194.21(i).	Release 2; Should
3.2.7.3.2.2.2.14	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.	Release 2; Should
3.2.7.3.2.2.2.15	A method shall be provided that permits users to skip repetitive navigation links.	Release 2; Should
3.2.7.3.2.2.2.16	When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	Release 2; Should
3.2.7.3.2.2.3	FDsys telecommunications products shall be Section 508 compliant according to 36 CFR Part 1194.23.	Release 2; Should
3.2.7.3.2.2.3.1	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.	Release 2; Should
3.2.7.3.2.2.3.2	Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer nonproprietary standard TTY signal protocols.	Release 2; Should
3.2.7.3.2.2.3.3	Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.	Release 2; Should
3.2.7.3.2.2.3.4	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.	Release 2; Should

3.2.7.3.2.2.3.5	Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.	Release 2; Should
3.2.7.3.2.2.3.6	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.	Release 2; Should
3.2.7.3.2.2.3.7	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.	Release 2; Should
3.2.7.3.2.2.3.8	Where a telecommunications product delivers output by an audio transducer which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.	Release 2; Should
3.2.7.3.2.2.3.9	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.	Release 2; Should
3.2.7.3.2.2.3.10	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.	Release 2; Should
3.2.7.3.2.2.3.10.1	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.	Release 2; Should
3.2.7.3.2.2.3.10.1.1	Technologies which use encoding, signal compression or format transformation shall not remove information needed for access or shall restore it upon delivery.	Release 2; Should
3.2.7.3.2.2.3.11	Products which have mechanically operated controls or keys, shall comply with the following:	Release 2; Should
3.2.7.3.2.2.3.11.1	Controls and keys shall be tactilely discernible without activating the controls or keys.	Release 2; Should
3.2.7.3.2.2.3.11.2	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.	Release 2; Should

3.2.7.3.2.2.3.11.3	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.	Release 2; Should
3.2.7.3.2.2.3.11.4	The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.	Release 2; Should
3.2.7.3.2.2.4	FDsys video and multimedia products shall be Section 508 compliant according to 36 CFR Part 1194.24	Release 2; Should
3.2.7.3.2.2.4.1	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.	Release 2; Should
3.2.7.3.2.2.4.1.1	All analog television displays 13 inches and larger shall be equipped with caption decoder circuitry which displays closed captioning.	Release 2; Should
3.2.7.3.2.2.4.1.2	All computer equipment that includes analog television receiver or display circuitry shall be equipped with caption decoder circuitry which displays closed captioning.	Release 2; Should
3.2.7.3.2.2.4.1.3	Widescreen digital television (DTV) displays measuring at least 7.8 inches vertically shall display closed captions.	Release 2; Should
3.2.7.3.2.2.4.1.4	DTV sets with conventional displays measuring at least 13 inches vertically shall display closed captions.	Release 2; Should
3.2.7.3.2.2.4.1.5	Standalone DTV tuners shall display closed captions.	Release 2; Should
3.2.7.3.2.2.4.1.6	Computer equipment that includes DTV receiver or display circuitry shall display closed captions.	Release 2; Should
3.2.7.3.2.2.4.2	Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.	Release 2; Should
3.2.7.3.2.2.4.3	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.	Release 2; Should

3.2.7.3.2.2.4.4	All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.	Release 2; Should
3.2.7.3.2.2.4.5	Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.	Release 2; Should
3.2.7.3.2.2.5	FDsys self contained, closed products shall be Section 508 compliant according to 36 CFR Part 1194.25	Release 2; Should
3.2.7.3.2.2.5.1	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.	Release 2; Should
3.2.7.3.2.2.5.2	When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	Release 2; Should
3.2.7.3.2.2.5.3	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).	Release 2; Should
3.2.7.3.2.2.5.3.1	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (1).	Release 2; Should
3.2.7.3.2.2.5.3.2	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (2).	Release 2; Should
3.2.7.3.2.2.5.3.3	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (3).	Release 2; Should
3.2.7.3.2.2.5.3.4	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (4).	Release 2; Should
3.2.7.3.2.2.5.4	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.	Release 2; Should
3.2.7.3.2.2.5.5	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 must provide the ability to interrupt, pause, and restart the audio at anytime.	Release 2; Should

3.2.7.3.2.2.5.6	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.	Release 2; Should
3.2.7.3.2.2.5.7	Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Release 2; Should
3.2.7.3.2.2.5.8	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.	Release 2; Should
3.2.7.3.2.2.5.9	Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Release 2; Should
3.2.7.3.2.2.5.10	Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following:	Release 2; Should
3.2.7.3.2.2.5.10.1	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.	Release 2; Should
3.2.7.3.2.2.5.10.2	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.	Release 2; Should
3.2.7.3.2.2.5.10.3	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.	Release 2; Should
3.2.7.3.2.2.5.10.4	Operable controls shall not be more than 24 inches behind the reference plane	Release 2; Should
3.2.7.3.2.2.6	FDsys desktop and portable computer products shall be Section 508 compliant according to 36 CFR Part 1194.26.	Release 2; Should
3.2.7.3.2.2.6.1	All mechanically operated controls and keys shall comply with §1194.23 (k) (1) through (4).	Release 2; Should
3.2.7.3.2.2.6.1.1	All mechanically operated controls and keys shall comply with §1194.23 (k) (1).	Release 2; Should
3.2.7.3.2.2.6.1.2	All mechanically operated controls and keys shall comply with §1194.23 (k) (2).	Release 2; Should
3.2.7.3.2.2.6.1.3	All mechanically operated controls and keys shall comply with §1194.23 (k) (3).	Release 2; Should
3.2.7.3.2.2.6.1.4	All mechanically operated controls and keys shall comply with §1194.23 (k) (4).	Release 2; Should

3.2.7.3.2.2.6.2	If a product touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	Release 2; Should
3.2.7.3.2.2.6.2.1	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1).	Release 2; Should
3.2.7.3.2.2.6.2.2	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (2).	Release 2; Should
3.2.7.3.2.2.6.2.3	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (3).	Release 2; Should
3.2.7.3.2.2.6.2.4	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (4).	Release 2; Should
3.2.7.3.2.2.6.3	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.	Release 2; Should
3.2.7.3.2.2.6.4	Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards.	Release 2; Should

3.2.7.4.2	**Requirements for Search**	
3.2.7.4.2.1	**Search Core Capabilities**	
3.2.7.4.2.1.1	The system shall provide the capability to search for and retrieve content from the system.	Release 1B; Must
3.2.7.4.2.1.2	The system shall provide the capability to search for and retrieve metadata from the system.	Release 1B; Must
3.2.7.4.2.1.3	The system shall provide the capability to search across multiple internal content and metadata repositories simultaneously and separately.	Release 1C; Must
3.2.7.4.2.1.4	The system shall provide the capability to search content that is currently available on the GPO Access public Web site.	Release 1C; Must
3.2.7.4.2.1.5	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 7.2.1.8 and its sub requirements.	Release 3; Must
3.2.7.4.2.1.6	The system shall provide the capability to search and retrieve unstructured content (e.g., text).	Release 1C; Must
3.2.7.4.2.1.7	The system shall provide the capability to match character strings (e.g., search exact phrases).	Release 1B; Must
3.2.7.4.2.1.8	The system shall provide the capability to search and retrieve semi-structured content (e.g., inline markup).	Release 1C; Must
3.2.7.4.2.1.9	The system shall provide the capability to search and retrieve structured content (e.g., fielded).	Release 1B; Must

3.2.7.4.2.1.10	The system shall provide the capability to search for content by means of querying metadata.	Release 1B; Must
3.2.7.4.2.1.11	The system shall provide the capability for users to search collections based on user class, user role, and access rights.	Release 1C; Must
3.2.7.4.2.1.12	The system shall provide the capability to return content packages in any form simultaneously or separately.	Release 1C; Must
3.2.7.4.2.1.12.1	The system shall provide the capability to search for digital objects.	Release 1C; Must
3.2.7.4.2.1.12.1.1	The system shall provide the capability to search for only work in progress content.	Release 1C; Must
3.2.7.4.2.1.12.1.2	The system shall provide the capability to search for work in progress content simultaneously with other content.	Release 1C; Must
3.2.7.4.2.1.12.1.3	The system shall provide the capability to search for only SIPs.	Release 1C; Must
3.2.7.4.2.1.12.1.4	The system shall provide the capability to search for SIPs simultaneously with other content.	Release 1C; Must
3.2.7.4.2.1.12.1.5	The system shall provide the capability to search for only AIPs.	Release 1C; Must
3.2.7.4.2.1.12.1.6	The system shall provide the capability to search for AIPs simultaneously with other content.	Release 1C; Must
3.2.7.4.2.1.12.1.7	The system shall provide the capability to search for only ACPs.	Release 1C; Must
3.2.7.4.2.1.12.1.8	The system shall provide the capability to search for ACPs simultaneously with other content.	Release 1C; Must

3.2.7.4.2.2	**Search - Query**	
3.2.7.4.2.2.1	The system shall provide the capability for users to select content collections to search.	Release 1B; Must
3.2.7.4.2.2.2	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).	Release 1B; Should / Release 2; Must
3.2.7.4.2.2.3	The system shall provide the capability for users to select search complexity levels (e.g., simple search, advanced/fielded search).	Release 1B; Must
3.2.7.4.2.2.3.1	The system shall allow a simple search, which allows the user to input a search term to search across one or multiple content collections.	Release 1B; Must
3.2.7.4.2.2.3.2	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.	Release 1C; Must
3.2.7.4.2.2.4	The system shall allow searching on any number of collections of content.	Release 1C; Must
3.2.7.4.2.2.4.1	The system shall allow users to search any collection based on the metadata associated with that collection.	Release 1C; Must

3.2.7.4.2.2.4.2	The system shall allow users to search collections currently available on GPO Access including the following:	Release 1C; Must
3.2.7.4.2.2.4.2.1	Public and Private Laws	Release 1C; Must
3.2.7.4.2.2.4.2.2	Congressional Reports	Release 1C; Must
3.2.7.4.2.2.4.2.3	Congressional Documents	Release 1C; Must
3.2.7.4.2.2.4.2.4	Congressional Bills	Release 1C; Must
3.2.7.4.2.2.4.2.5	Federal Register	Release 1C; Must
3.2.7.4.2.2.4.2.6	History of Bills	Release 1C; Must
3.2.7.4.2.2.4.2.7	Congressional Record	Release 1C; Must
3.2.7.4.2.2.4.2.8	Congressional Record Index	Release 1C; Must
3.2.7.4.2.2.4.2.9	United States Code	Release 1C; Must
3.2.7.4.2.2.4.2.10	Code of Federal Regulations	Release 1C; Must
3.2.7.4.2.2.4.2.11	List of Sections Affected (LSA)	Release 1C; Must
3.2.7.4.2.2.4.2.12	Congressional Hearings (including House and Senate Appropriations Hearings)	Release 1C; Must
3.2.7.4.2.2.4.2.13	Congressional Committee Prints	Release 1C; Must
3.2.7.4.2.2.4.2.14	Congressional Calendars (including House, Senate, and Committee)	Release 1C; Must
3.2.7.4.2.2.4.2.15	Weekly Compilation of Presidential Documents	Release 1C; Must
3.2.7.4.2.2.4.2.16	Budget of the United States Government	Release 1C; Must
3.2.7.4.2.2.4.2.17	Congressional Record (Bound)	Release 1C; Must
3.2.7.4.2.2.4.2.18	House Journal	Release 1C; Must
3.2.7.4.2.2.4.2.19	Semiannual regulatory Agenda (Unified Agenda)	Release 1C; Must
3.2.7.4.2.2.4.2.20	U.S. Constitution Analysis and Interpretation	Release 1C; Must
3.2.7.4.2.2.4.2.21	Economic Indicators	Release 1C; Must
3.2.7.4.2.2.4.2.22	Economic Report of the President	Release 1C; Must
3.2.7.4.2.2.4.2.23	Congressional Directory	Release 1C; Must
3.2.7.4.2.2.4.2.24	U.S. Government Manual	Release 1C; Must
3.2.7.4.2.2.4.2.25	Public Papers of the President of the United States	Release 1C; Must
3.2.7.4.2.2.4.2.26	House Ways and Means Committee Prints (Green Book)	Release 1C; Must
3.2.7.4.2.2.4.2.27	GAO Comptroller General Decisions	Release 1C; Must
3.2.7.4.2.2.4.2.28	GAO Reports	Release 1C; Must
3.2.7.4.2.2.4.2.29	House Practice	Release 1C; Must
3.2.7.4.2.2.4.2.30	Senate Manual	Release 1C; Must
3.2.7.4.2.2.4.2.31	House Rules and Manual	Release 1C; Must
3.2.7.4.2.2.4.2.32	Privacy Act Issuances	Release 1C; Must
3.2.7.4.2.2.4.2.33	Department of Interior Inspector General Reports	Release 1C; Must
3.2.7.4.2.2.4.2.34	U.S. Government Printing Office Style Manual	Release 1C; Must
3.2.7.4.2.2.4.2.35	Cannon's Precedents of the U.S. House of Representatives	Release 1C; Must
3.2.7.4.2.2.4.2.36	Hinds' Precedents of the House of Representatives	Release 1C; Must

3.2.7.4.2.2.4.2.37	Independent Counsel's Referral to Congress	Release 1C; Must
3.2.7.4.2.2.4.2.38	Government Information Locator Service Records (GILS)	Release 1C; Must
3.2.7.4.2.2.4.2.39	Supreme Court Decisions 1937-75	Release 1C; Must
3.2.7.4.2.2.4.2.40	Davis-Bacon Wage Determinations	Release 1C; Must
3.2.7.4.2.2.4.2.41	Commerce Business Daily	Release 1C; Must
3.2.7.4.2.2.4.2.42	Congressional Publications	Release 1C; Must
3.2.7.4.2.2.4.2.43	Statutes at Large	Release 1C; Must
3.2.7.4.2.2.5	Deleted.	
3.2.7.4.2.2.6	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).	Release 1C; Must
3.2.7.4.2.2.6.1	The system shall allow authorized users to manage concept relationships.	Release 1C; Must
3.2.7.4.2.2.6.1.1	The system shall allow authorized users to add concept relationships.	Release 1C; Must
3.2.7.4.2.2.6.1.2	The system shall allow authorized users to delete concept relationships.	Release 1C; Must
3.2.7.4.2.2.6.1.3	The system shall allow authorized users to modify concept relationships.	Release 1C; Must
3.2.7.4.2.2.6.1.4	The system shall suggest new concept relationships based on ingested content.	Release 1C; Must
3.2.7.4.2.2.6.1.4.1	The system shall automatically create new concept relationships based on an authorized users acceptance of suggested new concept relationships	Release 1C; Must
3.2.7.4.2.2.6.1.5	The system shall use new concepts without requiring previously indexed content is reindexed.	Release 1C; Must
3.2.7.4.2.2.6.2	Deleted.	
3.2.7.4.2.2.6.3	Deleted.	
3.2.7.4.2.2.7	The system shall support standard Boolean search language.	Release 1C; Must
3.2.7.4.2.2.7.1	The system shall support full Boolean operators, including AND, OR, NOT, BEFORE, NEAR, and ADJACENT.	Release 1B; Must
3.2.7.4.2.2.7.2	The system shall support implied Boolean operators, including “+” and “-“.	Release 1C; Must
3.2.7.4.2.2.7.3	The system shall support the nesting of Boolean operators via parentheses.	Release 1C; Must
3.2.7.4.2.2.7.4	No user shall be required to enter case sensitive operators.	Release 1B; Must
3.2.7.4.2.2.8	The system shall allow users to perform a natural language search.	Release 1C; Must
3.2.7.4.2.2.9	The system shall support a customizable list of stop words.	Release 1C; Must
3.2.7.4.2.2.9.1	The system shall support a customizable list of idioms.	Release 1C; Must
3.2.7.4.2.2.10	The system shall allow for stemming of search terms.	Release 1C; Must
3.2.7.4.2.2.10.1	The system shall allow for left side stemming.	Release 1C; Should

3.2.7.4.2.2.10.2	The system shall allow for right side stemming.	Release 1C; Must
3.2.7.4.2.2.11	The system shall allow users to use wildcard characters to replace characters within words.	Release 1B; Must
3.2.7.4.2.2.12	The system shall support proximity searching.	Release 1C; Must
3.2.7.4.2.2.13	The system shall support synonyms searching.	Release 1C; Must
3.2.7.4.2.2.14	The system shall provide the capability for contextual searching.	Release 1C; Could
3.2.7.4.2.2.15	The system shall conform to ISO 239.50.	Release 1C; Must
3.2.7.4.2.2.16	Deleted.	
3.2.7.4.2.2.17	The system shall have a documented interface (e.g., API) to allow search by non-GPO systems.	Release 1C; Must
3.2.7.4.2.2.18	Deleted.	
3.2.7.4.2.2.19	The system shall allow users to select specified search functionality.	Release 1B; Must
3.2.7.4.2.2.20	The system shall support queries of variable lengths.	Release 1B; Must
3.2.7.4.2.2.21	The system shall have the ability to limit search query length.	Release 1C; Must
3.2.7.4.2.2.22	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).	Release 1C; Must

3.2.7.4.2.3	**Search - Refine**	
3.2.7.4.2.3.1	The system shall provide the capability for users to modify previous search queries to enable execution of subsequent searches.	Release 1C; Must
3.2.7.4.2.3.1.1	The system shall provide the capability to direct subsequent queries against different content collections.	Release 2; Must
3.2.7.4.2.3.1.2	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.	Release 2; Must
3.2.7.4.2.3.2	The system shall provide the capability to display a list of terms that are conceptually related to the original search term.	Release 2; Must
3.2.7.4.2.3.2.1	The system shall provide users with the ability to directly execute a search from conceptually related terms.	Release 1C; Must
3.2.7.4.2.3.3	The system shall be able to recognize alternate spellings of terms.	Release 1C; Must
3.2.7.4.2.3.3.1	The system shall suggest corrected spellings of terms.	Release 2; Must

3.2.7.4.2.4	**Search - Results**	
3.2.7.4.2.4.0.1	The system shall have the capability to take users to the exact occurrence of the search term or its conceptual equivalent in a result.	Release 1C; Must

3.2.7.4.2.4.0.2	The system shall allow a user to navigate the levels of granularity applied to a result from within that result.	Release 1C; Must
3.2.7.4.2.4.0.3	The system shall provide the capability for users to bookmark individual search results.	Release 1C; Must
3.2.7.4.2.4.1	The system shall provide search results to users.	Release 1B; Must
3.2.7.4.2.4.2	The system must provide the capability for field collapsing (i.e. show one search result and have it link to multiple formats, versions, etc.)	Release 1B; Should / Release 2; Must
3.2.7.4.2.4.3	The system shall provide the capability to sort results lists on displayable attributes in the result set.	Release 1C; Must
3.2.7.4.2.4.4	The system shall provide the capability to categorize results.	Release 1C; Must
3.2.7.4.2.4.5	The system shall provide the capability to cluster results.	Release 1C; Should
3.2.7.4.2.4.6	The system shall provide the capability to analyze results.	Release 2; Could
3.2.7.4.2.4.7	The system shall provide the capability to display results graphically.	Release 2; Could
3.2.7.4.2.4.8	The system shall provide the capability to apply one or multiple taxonomies.	Release 1C; Must
3.2.7.4.2.4.9	The system shall provide the capability for users to limit the number of results displayed.	Release 1C; Must
3.2.7.4.2.4.10	The system shall provide the capability to display the total number of results in the result set returned by the search.	Release 2; Must
3.2.7.4.2.4.10.1	The system shall allow the user to select the number of results in a result set from available options.	Release 2; Must
3.2.7.4.2.4.10.2	The system shall allow a result set equal to the size of all records in all indexes.	Release 2; Must
3.2.7.4.2.4.11	The system shall allow authorized users to select which metadata attributes are viewable for each collection.	Release 1B; Must
3.2.7.4.2.4.11.1	Deleted.	
3.2.7.4.2.4.11.2	Deleted.	
3.2.7.4.2.4.12	The system shall provide the capability to highlight query terms.	Release 1C; Could
3.2.7.4.2.4.12.1	The system shall provide the capability to highlight query terms in the document.	Release 1C; Could
3.2.7.4.2.4.12.2	The system shall provide the capability to highlight query terms in the document abstract or document summary that appears results list.	Release 1C; Could
3.2.7.4.2.4.13	The system shall provide feedback to the user in the event of an error.	Release 1B; Must
3.2.7.4.2.4.14	The system shall provide the capability to display inline image thumbnails of content in a results list.	Release 2; Must
3.2.7.4.2.4.15	The system shall allow users to save search results individually or as a batch (e.g., without selecting each result individually) for export.	Release 1B; Should / Release 1C; Must

3.2.7.4.2.4.16	The system shall provide the capability to return search results at the lowest level of granularity supported by the content package.	Release 1C; Must
3.2.7.4.2.4.17	The system shall provide the capability for authorized users to modify relevancy ranking factors.	Release 1B; Should / Release 1C; Must

3.2.7.4.2.5	**Saved Searches**	
3.2.7.4.2.5.1	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.	Release 1C; Should / Release 2; Must
3.2.7.4.2.5.1.1	The system shall allow users with an established user account and profile to enter or store and recall queries.	Release 2; Must
3.2.7.4.2.5.1.2	The system shall allow users with an established user account and profile to enter or store and recall preferences.	Release 2; Must
3.2.7.4.2.5.1.3	The system shall allow users with an established user account and profile to enter or store and recall results sets as a whole.	Release 2; Must
3.2.7.4.2.5.1.4	The system shall allow users with an established user account and profile to enter or store and recall portions of results sets.	Release 2; Must
3.2.7.4.2.5.2	The system shall provide the capability to automatically execute saved searches on a schedule defined by the user.	Release 1C; Should / Release 2; Must
3.2.7.4.2.5.3	The system shall provide the capability to notify users when automatically executed searches return results that were not included in the original search.	Release 1C; Should / Release 2; Must

3.2.7.4.2.6	**Search Interface**	
3.2.7.4.2.6.1	The system shall provide a search interface that allows users to submit queries to the system and receive results.	Release 1B; Must
3.2.7.4.2.6.2	Deleted.	
3.2.7.4.2.6.3	The system shall provide the capability to have customizable search interfaces based on user preferences.	Release 1B; Should / Release 1C; Must
3.2.7.4.2.6.4	The system shall provide the capability to have navigational elements to allow users to navigate through results.	Release 1B; Must
3.2.7.4.2.6.5	Deleted.	

3.2.7.4.2.7	**Search Administration**	
3.2.7.4.2.7.1	The system shall provide the capability to manage an unlimited number of collections.	Release 1B; Must
3.2.7.4.2.7.2	The system must provide a Web-based administrator graphical user interface (GUI).	Release 1B; Must
3.2.7.4.2.7.3	Deleted.	

3.2.7.4.2.7.4	The system shall provide for the control of search run times, including the ability to preempt runtimes by an administrator-defined limit.	Release 2; Must
3.2.7.4.2.7.5	The system shall provide the capability to support user search while other system functions are being performed (e.g., re-indexing databases, updating content).	Release 1B; Must
3.2.7.4.2.7.6	The system shall provide the capability to log search activities.	Release 1B; Must

3.2.7.5.2	**Requirements for Request**	
3.2.7.5.2.1	**Request Core Capabilities**	
3.2.7.5.2.1.1	The system shall provide the capability for users to request delivery of content.	Release 1B; Must
3.2.7.5.2.1.2	The system shall provide the capability for users to request delivery of metadata.	Release 1C; Must
3.2.7.5.2.1.3	Deleted.	

3.2.7.5.2.2	**No Fee Requests**	
3.2.7.5.2.2.1	The system shall provide the capability for End Users to request no-fee content delivery.	Release 1B; Must
3.2.7.5.2.2.1.1	The system shall not restrict or otherwise diminish access to items that are currently available through GPO Access.	Release 1C; Must
3.2.7.5.2.2.1.2	The system shall provide the capability for users to print and download information currently available through GPO Access.	Release 1C; Must
3.2.7.5.2.2.1.2.1	The system shall maintain printing functionality currently available within GPO Access content collections.	Release 1C; Must
3.2.7.5.2.2.1.2.2	The system shall maintain downloading functionality currently available within GPO Access content collections.	Release 1C; Must
3.2.7.5.2.2.2	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.	Release 2; Must

3.2.7.5.2.2.3	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.	Release 2; Must
3.2.7.5.2.2.4	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.	Release 2; Must
3.2.7.5.2.2.5	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 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.	Release 2; Must
3.2.7.5.2.2.6	The system shall provide the capability to process no-fee requests for delivery of content with access restrictions.	Release 2; Must
3.2.7.5.2.2.7	The system shall support the delivery of serials and periodicals.	Release 2; Must
3.2.7.5.2.2.8	The system shall provide the capability for users to cancel full or partial requests prior to fulfillment.	Release 1C; Must
3.2.7.5.2.2.9	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…").	Release 1C; Could / Release 2; Must
3.2.7.5.2.2.9.1	The system shall provide the capability for users to opt-out of personalized offers.	Release 1C; Could / Release 2; Must
3.2.7.5.2.2.10	The system must provide the capability to provide authorized users with a detailed transaction summary	Release 1C; Should / Release 2; Must

3.2.7.5.2.2.11	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.	Release 1C; Should / Release 2; Must
3.2.7.5.2.2.12	The system shall provide the capability to generate reports for no-fee transactions.	Release 1C; Must

3.2.7.5.2.3	**Fee-based Requests**	
3.2.7.5.2.3.1	The system shall provide the capability for users to request fee-based content delivery.	Release 2; Must
3.2.7.5.2.3.2	The system shall have the capability to interface with external “Authorized Representatives” as designated by GPO’s Publication and Information Sales business unit for processing of fee-based delivery requests.	Release 2; Must
3.2.7.5.2.3.3	The system shall provide the capability to interface with GPO’s financial and inventory systems for processing of fee-based requests.	Release 2; Must
3.2.7.5.2.3.5	The system shall have the capability to retrieve price information from external systems.	Release 2; Must
3.2.7.5.2.3.6	The system shall have the capability to adjust price information for fee-based content delivery.	Release 2; Must
3.2.7.5.2.3.6.1	Pricing structures shall comply with GPO’s legislative mandates under Title 44 of the United States Code and GPO’s Sales Program policies.	Release 2; Must
3.2.7.5.2.3.6.2	The system shall provide the capability for authorized users to manually adjust the price.	Release 2; Must
3.2.7.5.2.3.6.3	The system shall provide the capability to dynamically adjust the price.	Release 2; Must
3.2.7.5.2.3.6.4	The system shall provide the capability to apply price schedules.	Release 2; Must
3.2.7.5.2.3.7	The system shall adhere to industry best practices for performance of a Web-accessible e-commerce system.	Release 2; Must
3.2.7.5.2.3.8	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.	Release 2; Must

3.2.7.5.2.3.9	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.	Release 2; Must
3.2.7.5.2.3.10	The system shall provide the capability to process fee-based requests for the delivery of content with access restrictions.	Release 2; Must
3.2.7.5.2.3.11	The system shall support the collection of information (order taking) and pass this information to external systems for processing.	Release 2; Must
3.2.7.5.2.3.11.1	The system shall support the collection of payment information via the following methods:	Release 2; Must
3.2.7.5.2.3.11.1.1	Check/electronic transfer	Release 2; Must
3.2.7.5.2.3.11.1.2	Major credit cards including Visa, MasterCard, Discover/NOVUS, and American Express	Release 2; Must
3.2.7.5.2.3.11.1.3	Debit cards	Release 2; Must
3.2.7.5.2.3.11.1.4	Purchase orders	Release 2; Must
3.2.7.5.2.3.11.1.5	Requests for invoicing	Release 2; Must
3.2.7.5.2.3.11.1.6	Deposit accounts	Release 2; Must
3.2.7.5.2.3.11.1.7	Government Account	Release 2; Must
3.2.7.5.2.3.11.1.8	Cash	Release 2; Must
3.2.7.5.2.3.11.1.9	Gift card	Release 2; Must
3.2.7.5.2.3.11.2	The system shall securely pass information to external systems for processing.	Release 2; Must
3.2.7.5.2.3.11.3	The system shall comply with the Federal Trade Commission's Mail or Telephone Order Merchandise Rule.	Release 2; Must
3.2.7.5.2.3.11.4	The system shall comply with the Fair Credit Billing Act.	Release 2; Must
3.2.7.5.2.3.11.5	The system shall comply with the Fair Credit Reporting Act.	Release 2; Must
3.2.7.5.2.3.11.9	The system shall comply with the Children's Online Privacy Protection Act (COPPA).	Release 2; Must
3.2.7.5.2.3.11.10	The system shall comply with the FTC's rules for implementing the Children's Online Privacy Protection Act (COPPA).	Release 2; Must
3.2.7.5.2.3.12	The system shall provide the capability to automatically verify and validate payment information submitted by users prior to delivery fulfillment.	Release 2; Must
3.2.7.5.2.3.12.1	The system shall provide the capability to validate payment information in real-time via external GPO systems.	Release 2; Must
3.2.7.5.2.3.12.2	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	Release 2; Must

3.2.7.5.2.3.13	The system shall provide the capability for users to delegate requests to other users (e.g. users "hand-off" orders to other authorized officials to submit payment).	Release 1C; Should / Release 2; Must
3.2.7.5.2.3.14	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.	Release 1C; Should / Release 2; Must
3.2.7.5.2.3.14.1	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.	Release 2; Must
3.2.7.5.2.3.15	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.)	Release 2; Must
3.2.7.5.2.3.15.1	The system shall provide the capability to manage, secure, and maintain End User information associated with subscriptions.	Release 2; Must
3.2.7.5.2.3.15.2	The system shall provide the capability to notify End Users when their subscriptions are about to end (e.g., renewal notices).	Release 1C; Could / Release 2; Must
3.2.7.5.2.3.16	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…").	Release 1C; Could / Release 2; Must
3.2.7.5.2.3.16.1	The system shall provide the capability for users to opt-out of personalized offers.	Release 1C; Could / Release 2; Must
3.2.7.5.2.3.17	The system shall provide the capability for users to cancel full or partial requests prior to fulfillment.	Release 2; Must
3.2.7.5.2.3.18	The system shall provide the capability to provide authorized users with a detailed transaction summary.	Release 2; Must
3.2.7.5.2.3.19	The system shall provide the capability for authorized users to configure transaction summaries.	Release 1C; Should / Release 2; Must
3.2.7.5.2.3.20	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.	Release 2; Must
3.2.7.5.2.3.20.1	The system shall securely maintain electronic copies of orders, shipments, and financial records for at least seven years.	Release 2; Must
3.2.7.5.2.3.21	The system shall provide the capability to generate reports for fee-based transactions (e.g., order histories, sales transactions, inventory data).	Release 2; Must

3.2.7.5.2.4	**Request - Delivery Options**	
3.2.7.5.2.4.1	The system must have the capability to determine what options are available for delivery of particular content or metadata.	Release 1C; Must

3.2.7.5.2.4.2	The system shall provide the capability for users to request delivery of content or metadata from available options as defined by GPO business units.	Release 2; Must
3.2.7.5.2.4.3	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).	Release 1C; Must
3.2.7.5.2.4.4	The system shall provide the capability for users to select file type from available options (e.g., DOC, MP3, PDF).	Release 1C; Must
3.2.7.5.2.4.5	The system shall provide the capability for users to select resolution (e.g., images, video) from available options.	Release 1C; Could / Release 2; Must
3.2.7.5.2.4.6	The system shall provide the capability for users to select color space from available options (e.g. RGB, CMYK).	Release 1C; Could / Release 2; Must
3.2.7.5.2.4.7	The system shall provide the capability for users to select compression and size from available options.	Release 1C; Could / Release 2; Must
3.2.7.5.2.4.8	The system shall provide the capability for users to select transfer rate from available options.	Release 1C; Could / Release 2; Must
3.2.7.5.2.4.9	The system shall provide the capability for users to select platform from available options.	Release 2; Must
3.2.7.5.2.4.10	The system shall provide the capability for users to select the version of content from available options.	Release 1B; Must
3.2.7.5.2.4.11	The system shall provide the capability for users to select delivery of related content from available options.	Release 1C; Could / Release 2; Must
3.2.7.5.2.4.12	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).	Release 1C; Must
3.2.7.5.2.4.13	The system shall provide the capability for users to select quantity of items requested for delivery (e.g., one, five, batch).	Release 1C; Must
3.2.7.5.2.4.14	The system shall provide the capability for users to select output type from available options (e.g., hard copy, electronic presentation, digital media).	Release 1C; Must
3.2.7.5.2.4.15	The system shall provide the capability for users to select data storage device from available options (e.g., CD, DVD, server).	Release 1C; Must
3.2.7.5.2.4.16	The system shall provide the capability for users to select level of granularity from available options (e.g., title, part, section, paragraph, graphic, page).	Release 1B; Must
3.2.7.5.2.4.17	The system shall provide the capability for users to select electronic delivery method from available options (e.g., FTP, RSS, email, download, broadcast).	Release 1C; Must
3.2.7.5.2.4.18	The system shall provide the capability for users to schedule delivery from the system.	Release 1C; Must

3.2.7.5.2.4.19	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).	Release 2; Must
3.2.7.5.2.4.20	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.	Release 2; Must
3.2.7.5.2.4.21	The system shall provide the capability for users to submit multiple address options for delivery or shipment of tangible content.	Release 2; Must
3.2.7.5.2.4.22	The system must provide the capability to preview requested content.	Release 2; Should / Release 3; Must
3.2.7.5.2.4.22.1	The system shall provide the capability to view the access copy of content where available.	Release 1C; Must
3.2.7.5.2.4.22.2	The system shall provide the capability for authorized users to preview publications that have been created from custom composition and content formatting.	Release 3; Must
3.2.7.5.2.4.23	The system shall have the capability to support custom composition and content formatting from available options (e.g., 2 columns, cover stock, font).	Release 2; Should / Release 3; Must

3.2.7.5.2.5	**Request - User Accounts**	

3.2.7.5.2.6	**Order Numbers and Request Status**	
3.2.7.5.2.6.1	The system shall provide the capability to assign an order number for requests.	Release 2; Must
3.2.7.5.2.6.2	The system shall not repeat an order number.	Release 2; Must
3.2.7.5.2.6.3	The system shall record order numbers in metadata.	Release 2; Must
3.2.7.5.2.6.4	The system shall have the capability to provide order numbers to users.	Release 2; Must
3.2.7.5.2.6.5	The system shall provide the capability for users to track the status of their requests.	Release 2; Must

3.2.7.6.2	**Requirements for Cataloging and Reference Tools**	
3.2.7.6.2.1	**Cataloging and Reference Tools - Metadata Management**	
3.2.7.6.2.1.1	Deleted.	
3.2.7.6.2.1.2	The system shall support creation of metadata according to specified cataloging rules.	Release 1B; Must
3.2.7.6.2.1.3	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).	Release 1C; Must
3.2.7.6.2.1.4	The system shall support the creation of ONIX metadata	Release 2; Must

3.2.7.6.2.1.4.1	The system shall support the creation of ONIX metadata from existing metadata.	Release 2; Must
3.2.7.6.2.1.4.2	FDsys shall notify users that content is available for selection for the sales program.	Release 2; Must
3.2.7.6.2.1.5	The system shall support the creation of library standard bibliographic records (e.g., MARC).	Release 1B; Must
3.2.7.6.2.1.6	The system shall support the extraction of metadata from content.	Release 2; Must
3.2.7.6.2.1.7	Deleted.	
3.2.7.6.2.1.8	The system shall provide for the creation of new metadata records based on existing metadata records.	Release 1B; Must
3.2.7.6.2.1.9	The system shall provide the capability to acquire and integrate metadata from external sources.	Release 2; Must
3.2.7.6.2.1.10	The system shall relate descriptive metadata with the content described.	Release 1B; Must
3.2.7.6.2.1.11	The system shall provide capability for authorized users to manage metadata.	Release 1B; Must
3.2.7.6.2.1.11.1	The system shall provide capability for authorized users to add metadata.	Release 1B; Must
3.2.7.6.2.1.11.2	The system shall provide capability for authorized users to modify metadata.	Release 1B; Must
3.2.7.6.2.1.11.3	The system shall provide capability for authorized users to delete metadata.	Release 1B; Must
3.2.7.6.2.1.12	System shall record the change history of cataloging metadata.	Release 2; Must
3.2.7.6.2.1.13	The system shall have the ability to provide access to metadata throughout the lifecycle of the content.	Release 1B; Must
3.2.7.6.2.1.14	The system shall provide the capability to add metadata specifically for GPO sales purposes (e.g., book jacket art, reviews, summaries).	Release 2; Could
3.2.7.6.2.1.15	The system shall have the capability to record and manage relationships among the issues or volumes of serially-issued publications.	Release 1B; Must

3.2.7.6.2.2	**Cataloging and Reference Tools - Metadata Delivery**	
3.2.7.6.2.2.1	The system shall provide the capability to export metadata as individual records or in batch based on user-defined parameters.	Release 1C; Must
3.2.7.6.2.2.2	The system will provide for display and output of brief citations.	Release 1B; Must
3.2.7.6.2.2.3	The system will provide for display and output of basic bibliographic citations.	Release 1C; Must
3.2.7.6.2.2.4	The system will provide for display and output of full records.	Release 1B; Must
3.2.7.6.2.2.5	The system will provide for display and output of MARC records.	Release 1B; Must

3.2.7.6.2.2.6	The system will provide for the delivery of output in a variety user-specified methods or formats, including electronic mail or Web pages.	Release 2; Must
3.2.7.6.2.2.6.1	The system will be capable of delivering metadata to users in electronic mail messages.	Release 2; Must
3.2.7.6.2.2.6.2	The system will be capable of delivering metadata to users in Web pages.	Release 2; Must
3.2.7.6.2.2.6.3	The system shall support the capability to deliver metadata to users in additional formats in the future.	Release 2; Must
3.2.7.6.2.2.7	The system shall output metadata in formats specified by the user, including MARC, ONIX, ASCII text, or comma delimited text.	Release 2; Must
3.2.7.6.2.2.7.1	The system shall output metadata in MARC format when requested by the user.	Release 2; Must
3.2.7.6.2.2.7.2	The system shall output metadata in ONIX format when requested by the user.	Release 2; Must
3.2.7.6.2.2.7.3	The system shall output metadata in ASCII text format when requested by the user.	Release 2; Must
3.2.7.6.2.2.7.4	The system shall output metadata in comma-delimited format when requested by the user.	Release 2; Must
3.2.7.6.2.2.7.5	The system shall support the capability to output metadata in additional formats in the future.	Release 2; Must

3.2.7.6.2.3	**Reference Tools**	
3.2.7.6.2.3.1	The system shall have the ability to generate lists based on any metadata field.	Release 2; Must
3.2.7.6.2.3.2	The system shall have the capability to generate lists based on search query (e.g., that match a library's item selection profile).	Release 2; Must
3.2.7.6.2.3.3	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).	Release 2; Must
3.2.7.6.2.3.4	The system should have the capability to generate lists that point to metadata (e.g., lists of publications available for selection by depository libraries).	Release 2; Must
3.2.7.6.2.3.5	The system should have the capability to generate lists that point to related resources or other reference tools (e.g., Browse Topics).	Release 2; Should
3.2.7.6.2.3.6	The system shall have the capability to link to external content and metadata.	Release 2; Must
3.2.7.6.2.3.7	The system shall be interoperable with third party reference tools (e.g., search catalogs of other libraries).	Release 3; Should
3.2.7.6.2.3.8	The system shall have the capability to dynamically generate reference tools.	Release 3; Could
3.2.7.6.2.3.9	The system will allow GPO to manage reference tools.	Release 2; Must
3.2.7.6.2.3.9.1	The system will allow GPO to add reference tools.	Release 2; Must

3.2.7.6.2.3.9.2	The system will allow GPO to update reference tools with capability of saving previous versions	Release 2; Must
3.2.7.6.2.3.9.3	The system will allow GPO to delete reference tools, with capability of saving previous versions.	Release 2; Must
3.2.7.6.2.3.10	The system shall be able to generate lists based on user preferences.	Release 1C; Should / Release 2; Must
3.2.7.6.2.3.11	The system shall provide the capability for users to customize reference tools.	Release 1C; Should / Release 2; Must
3.2.7.6.2.3.12	The system shall support interactive processes so users can create reference tools.	Release 2; Should

3.2.7.6.2.4	**Cataloging and Reference Tools - Interoperability and Standards**	
3.2.7.6.2.4.1	The system shall interface with, and allow full functionality of, the GPO Integrated Library System.	Release 2; Must
3.2.7.6.2.4.2	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.	Release 2; Must
3.2.7.6.2.4.2.1	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.	Release 2; Must
3.2.7.6.2.4.2.2	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.	Release 2; Must

3.2.7.6.2.4.2.3	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.	Release 2; Must
3.2.7.6.2.4.2.4	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.	Release 2; Must
3.2.7.6.2.4.2.5	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 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.	Release 2; Must
3.2.7.6.2.4.2.6	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.	Release 2; Must

3.2.7.6.2.4.2.7	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.	Release 2; Must
3.2.7.6.2.4.2.8	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.	Release 2; Must
3.2.7.6.2.4.2.9	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.	Release 2; Must
3.2.7.6.2.4.2.10	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.	Release 2; Must

3.2.7.6.2.4.3	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Anglo-American Cataloging Rules, 2nd and 3d edition (AACR2 and RDA), Library of Congress Classification, Library of Congress Cataloging Rules, AACR2 Rev., LC Rule Interpretations, Cooperative Online Serials (CONSER), CONSER Access Level Record Guidelines, Cataloging Guidelines, Superintendent of Documents Classification Manual, Library of Congress Subject Headings, NASA Subject Headings, MESH Subject Headings, all MARC Formats, and other GPO specified standards and best practices.	Release 1C; Must
3.2.7.6.2.4.3.1	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Anglo-American Cataloging Rules, 2nd and 3d edition (AACR2 and RDA).	Release 1C; Must
3.2.7.6.2.4.3.2	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Library of Congress Classification.	Release 1C; Must
3.2.7.6.2.4.3.3	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Library of Congress Cataloging Rules.	Release 1C; Must
3.2.7.6.2.4.3.4	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the AACR2 Rev.	Release 1C; Must
3.2.7.6.2.4.3.5	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the LC Rule Interpretations.	Release 1C; Must
3.2.7.6.2.4.3.6	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Cooperative Online Serials (CONSER).	Release 1C; Must
3.2.7.6.2.4.3.7	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the CONSER Access Level Record Guidelines.	Release 1C; Must
3.2.7.6.2.4.3.8	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Cataloging Guidelines.	Release 1C; Must
3.2.7.6.2.4.3.9	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Superintendent of Documents Classification Manual.	Release 1C; Must
3.2.7.6.2.4.3.10	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Library of Congress Subject Headings.	Release 1C; Must
3.2.7.6.2.4.3.11	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the NASA Subject Headings.	Release 1C; Must

3.2.7.6.2.4.3.12	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the MESH Subject Headings.	Release 1C; Must
3.2.7.6.2.4.3.13	The system shall support the use of the following and support all subsequent modifications, updates and revisions to all MARC Formats.	Release 1C; Must
3.2.7.6.2.4.3.14	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.	Release 1C; Must
3.2.7.6.2.4.4	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.	Release 2; Must
3.2.7.6.2.4.5	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 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.	Release 2; Must

3.2.7.7.2	**Requirements for User Interface**	
3.2.7.7.2.1	**User Interface Core Capabilities**	
3.2.7.7.2.1.1	The system shall provide a default Graphical User Interface (GUI) for each functional element as required in accordance with the system release schedule.	Release 1B; Must
3.2.7.7.2.1.2	The system must provide a default workbench for each user class as required in accordance with the system release schedule.	Release 1B; Must
3.2.7.7.2.1.2.1	Deleted.	
3.2.7.7.2.1.2.2	The system shall provide the capability for GPO to create workbenches for subsets of user classes.	Release 2; Must
3.2.7.7.2.1.2.3	The system shall provide the capability for GPO to manage the toolsets that are available on default workbenches.	Release 1C; Must

3.2.7.7.2.1.2.4	The system shall provide a default public End User workbench that allows users to access the system without registering.	Release 1B; Must
3.2.7.7.2.1.2.4.1	The system shall allow all user to perform the actions allowed to unregistered users.	Release 1B; Must
3.2.7.7.2.1.2.5	Public End User GUIs shall be section 508 compliant.	Release 1C; Must
3.2.7.7.2.1.2.5.1	Content Originator GUIs shall be section 508 compliant.	Release 1C; Must
3.2.7.7.2.1.2.6	The system shall provide a default Service Specialist workbench that provides the capability for Service Specialists to handle exception processing.	Release 1B; Must
3.2.7.7.2.1.2.7	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.	Release 1B; Must
3.2.7.7.2.1.3	The system shall provide the capability to maintain a consistent look and feel throughout workbenches and GUIs to the extent possible.	Release 1C; Must
3.2.7.7.2.1.3.1	GUIs shall conform to GPO design guidelines.	Release 1C; Should
3.2.7.7.2.1.4	The system shall support web-based GUIs.	Release 1B; Must
3.2.7.7.2.1.5	The system shall support non web-based GUIs, as necessary.	Release 1B; Should
3.2.7.7.2.1.6	Deleted.	
3.2.7.7.2.1.7	The system shall provide for non-English language extensibility such that GUIs could contain non-English language text.	Release 1C; Could / Release 2; Must
3.2.7.7.2.1.8	The system shall provide GUIs that accept input of information by users.	Release 1B; Must
3.2.7.7.2.1.9	The system shall provide GUIs that accept submission of content by users.	Release 1B; Must
3.2.7.7.2.1.10	The system shall provide GUIs that allow users to input and submit registration information and login to the system.	Release 1B; Must
3.2.7.7.2.1.11	The system shall only display GUI functionality appropriate to the user and the actions the user is taking.	Release 1B; Must
3.2.7.7.2.1.11.1	The system shall have the capability to assign access to system functionality based on a user role.	Release 1B; Must
3.2.7.7.2.1.11.2	The system shall have the capability to assign access to system functionality based on user security settings.	Release 1B; Must
3.2.7.7.2.1.12	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.	Release 1B; Must
3.2.7.7.2.1.13	The system must provide GUIs that can be displayed on Macintosh, Unix, and Windows environments.	Release 1B; Must
3.2.7.7.2.1.13.1	The system shall provide Release 1B GUIs that are displayable in Firefox 1.5.x.	Release 1B; Must

3.2.7.7.2.1.13.2	The system shall provide Release 1B GUIs that are displayable in IE 6.x.	Release 1B; Must
3.2.7.7.2.1.14	The system shall provide GUIs that are capable of providing feedback, alerts, or notices to users.	Release 1B; Must
3.2.7.7.2.1.15	The system shall provide GUIs that are capable of providing context specific help and user support.	Release 1B; Must

3.2.7.7.2.2	**User Interface Standards and Best Practices**	
3.2.7.7.2.2.1	The system shall comply with best practices and guidelines regarding usability for graphical user interface design.	Release 1B; Should
3.2.7.7.2.2.1.1	GUIs shall be developed in accordance with the Research Based Web Design & Usability Guidelines, 2006 edition.	Release 1B; Should
3.2.7.7.2.2.1.2	Web GUIs shall be developed in accordance with the Web Style Guide, 2nd edition.	Release 1B; Should
3.2.7.7.2.2.2	Where the system uses the following technologies for interoperability it will use the stated standards as follows:	Release 1B; Must
3.2.7.7.2.2.2.1	The system shall conform to Extensible Markup Language (XML).	Release 1B; Must
3.2.7.7.2.2.2.2	The system shall conform to Extensible Style sheet Language (XSL).	Release 1B; Must
3.2.7.7.2.2.2.3	The system shall conform to Document Type Definition (DTD) and schema.	Release 1B; Must
3.2.7.7.2.2.2.3.1	The system shall conform to Document Type Definition (DTD).	Release 1B; Must
3.2.7.7.2.2.2.3.2	The system shall conform to schema.	Release 1B; Must
3.2.7.7.2.2.2.4	The system shall conform to XSL Transformations (XSLT).	Release 1B; Must
3.2.7.7.2.2.2.5	The system shall conform to XML Path Language (XPath).	Release 1B; Must
3.2.7.7.2.2.2.6	The system shall conform to Extensible HyperText Markup Language (XHTML).	Release 1B; Must
3.2.7.7.2.2.2.7	The system shall conform to Cascading Style Sheets (CSS).	Release 1B; Must
3.2.7.7.2.2.2.8	The system shall conform to DHTML.	Release 1B; Must
3.2.7.7.2.2.2.9	The system shall conform to WML.	Release 2; Must

3.2.7.7.2.3	**User Interface Customization and Personalization**	
3.2.7.7.2.3.1	The system shall provide the capability for authorized users who have registered with the system to customize GUIs.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.1.1	The system shall provide the capability to add tools.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.1.2	The system shall provide the capability to remove tools.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.1.3	The system shall provide the capability to hide tools.	Release 1C; Should / Release 2; Must

3.2.7.7.2.3.1.4	The system shall provide the capability to modify the placement of tools.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.1.5	The system shall provide the capability to modify the size of tools.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.1.6	The system shall provide the capability to select text size from available options.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.1.7	The system shall provide the capability to select color scheme from available options.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.2	The system shall provide the capability to provide personalized GUIs and workbenches to users that have registered with the system.	Release 1C; Could / Release 2; Must
3.2.7.7.2.3.3	The system shall provide the capability to provide personalized GUIs and workbenches that are created from user histories as analyzed through data mining.	Release 1C; Could / Release 2; Must
3.2.7.7.2.3.4	The system shall provide the capability for users to revert to their original default GUIs and workbenches.	Release 1C; Should / Release 2; Must
3.2.7.7.2.3.5	The system shall provide the capability to maintain interface configurations across user sessions.	Release 1C; Should / Release 2; Must

3.2.7.7.2.4	**User Interface Default Workbenches**	
3.2.7.7.2.4.1	The system must provide the capability to configure workbenches according to criticality and release schedules specified in individual requirements.	Release 2; Must
3.2.7.7.2.4.2	The system must provide a workbench for Content Originators (e.g., Congressional Content Originators, Agency Content Originators) that has the capability to include but is not limited to the following tools. a) The style tools GUI shall enable users to • Submit content to pre-ingest WIP. • Input metadata. • Develop, edit, and compose content. • View preliminary compositions. • Work collaboratively with other users. b) Deposited content GUI shall enable users to • Submit content to pre-ingest WIP. • Input metadata. c) Content Originator ordering GUI shall enable users to • View job estimates and costs. • Input BPI including content delivery and job specifications. • Request proofs. • Approve or reject content for publication. • Ride requests for delivery. • Track jobs status. d) Search GUI shall enable users to • Search and retrieve content and metadata stored in ACS and WIP. e) User support GUI shall enable users to • Submit inquires and receive responses. • Search knowledge base. f) Data mining GUI shall enable users to • Create, schedule, and view reports.	Release 2; Must

3.2.7.7.2.4.3	The system must provide a workbench for GPO Content Evaluators that has the capability to include but is not limited to the following tools. a) Content processing GUI shall enable users to • View content, metadata, and BPI. • Input metadata and BPI. • View and input decisions related to deposited, harvested, and converted content (e.g., scope determination, preservation plan). • Ride requests for delivery. • Assign persistent names and name spaces. • Modify rules for version triggers. b) Data mining GUI shall enable users to • Create, schedule, and view reports.	Release 1B; Must
3.2.7.7.2.4.4	The system must provide a default interface for GPO Service Specialists that includes but is not limited to the following tools. a) Style tools GUI shall enable users to • Submit content to pre-ingest WIP. • Input metadata. • Develop, edit, and compose content. • View preliminary composition. • Work collaboratively with other users. b) Search shall enable users to • Search and retrieve content and metadata stored in ACS and WIP. c) Content Originator ordering GUI shall enable users to • View job estimates and costs. • Input and augment BPI including job specifications. • Request proofs. • Track jobs status. d) Deposited content GUI shall enable users to • Submit content to pre-ingest WIP. • Input metadata. e) Content processing GUI shall enable users to • Input metadata and BPI. • Manage content packages. • Manage content processes. • Manage relationships between content packages, between digital objects, and between digital object and content packages. • Assign persistent names and name spaces. f) Preservation GUI shall enable users to • Manage preservation processes including assessments. g) Version control GUI shall enable users to • Input, view, and manage version information. h) Cataloging GUI shall enable users to • Input, view, create, and manage metadata including library standard and book industry bibliographic records. • View, manage, and export metadata. • Access cataloging resources and references. • Interact with bibliographic utilities. i) Reference tools GUI shall enable users to • Create, manage, and access reference tools. j) User support GUI shall enable users to • Communicate with users. • Manage user support tools. • Search and manage knowledgebase. k) Request GUI shall enable users to • Input, select, and manage delivery options. • Schedule delivery. l) Data mining GUI shall enable users to • Input supplemental data. • Input parameters for data normalization. • Extract data for analysis. • Create, schedule, and view reports.	Release 1B; Must

3.2.7.7.2.4.5	The system must provide a workbench for Service Providers (e.g., GPO Service Providers and External Service Providers) that has the capability to include but is not limited to the following tools. a) Style tools GUI shall enable users to • Submit content to pre-ingest WIP. • Input metadata. • Develop, edit, and compose content. • View preliminary composition. • Work collaboratively with other users. b) Deposited content GUI shall enable users to • Submit content to pre-ingest WIP. • Input metadata and BPI. c) Harvested content GUI shall enable users to • Manage harvesting processes. • Submit content to pre-ingest WIP. • Input metadata and BPI. d) Converted content GUI shall enable users to • Manage converted content. • Submit content to pre-ingest WIP. • Input metadata and BPI. e) Content Originator ordering GUI shall enable users to • Input and view BPI. • View jobs status. f) Search shall enable users to • Search and retrieve content and metadata stored in ACS and WIP. g) Request GUI shall enable users to • Select content delivery options. • Schedule content delivery. h) Content delivery GUI shall enable users to • Pull content packages from the system. i) Data mining GUI shall enable users to • Create, schedule, and view reports. j) User support GUI shall enable users to • Submit inquires and receive responses. • Search knowledge base.	Release 1B; Must

3.2.7.7.2.4.6	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 has the capability to include but is not limited to the following tools. a) Search GUI shall enable users to • Submit queries against content and metadata including bibliographic records. • View, sort, and categorize results. b) Request GUI shall enable users to • Input and select delivery options. • Perform custom composition and content formatting from available options. • Schedule delivery. • Submit payment for delivery. • Track request status. c) Access GUI shall enable users to • View relationships between content packages, between digital objects, and between content packages and digital objects. d) Cataloging GUI shall enable users to • View and export metadata. e) Reference tools GUI shall enable users to • Access reference tools. f) User support GUI shall enable users to • Search knowledge base. • Subscribe and unsubscribe to alert services. • Access training materials. • Submit inquires and receive responses. g) Content delivery GUI shall enable users to • Pull content packages from the system. • View content rendered for electronic presentation. h) Data mining GUI shall enable users to • Create, schedule, and view reports.	Release 1B; Must
3.2.7.7.2.4.7	The system must provide a workbench for GPO Business Managers that has the capability to include but is not limited to the following tools. A) Data Mining GUI shall enable users to • Create, schedule, and view reports.	Release 1C; Could / Release 2; Must
3.2.7.7.2.4.8	The system shall provide a default interface for authorized users that includes but is not limited to the following tools. Clarification: This is a high level requirement that will be met by lower level requirements.	Release 1B; Must
3.2.7.7.2.4.8.1	The system shall provide a default security GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Perform security administration. • Interact with the identity management system including managing user roles and user accounts in a role based security system. • View and manage system, application, audit, and security logs. • Monitor system security policy settings and policy enforcement. • Administer access rules.	Release 1B; Must

3.2.7.7.2.4.8.2	The system shall provide a default content processing GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Manage content packages. • Manage content processes. • Transfer content from the system. • Perform records management functions.	Release 1B; Must
3.2.7.7.2.4.8.3	The system shall provide a default authentication GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Manage authentication processes including content certification and integrity marks. • Monitor content integrity and receive notification of changes to content.	Release 1B; Must
3.2.7.7.2.4.8.4	The system shall provide a default search GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Manage and configure search tools.	Release 1B; Must
3.2.7.7.2.4.8.5	The system shall provide a default storage shall GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Manage storage. • Monitor storage.	Release 1B; Must
3.2.7.7.2.4.8.6	The system shall provide a default workflow GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Manage workflows, activities, and work lists. • Monitor all workflows. • Send notifications.	Release 1B; Must
3.2.7.7.2.4.8.7	The system shall provide a default ESB GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Configure all ESB processes. • Manage business processes. • Perform administrative tasks. • Monitor all processes.	Release 1B; Must
3.2.7.7.2.4.8.8	The system shall provide a default data mining GUI for authorized Systems Administrators / Operations Managers users that shall enable users them to, at a minimum: • Manage default report templates. • Input supplemental data. • Input parameters for data normalization. • Extract data for analysis. • Create, schedule, and view reports.	Release 1B; Must

3.2.7.8.2	Requirements for User Support	
3.2.7.8.2.1	**User Support Core Capabilities**	
3.2.7.8.2.1.1	The system shall provide multiple methods of contact for user assistance.	Release 2; Must
3.2.7.8.2.1.1.1	The system shall provide multiple methods for users to contact authorized users for user assistance.	Release 2; Must
3.2.7.8.2.1.1.1.1	The system shall provide web form for users to contact authorized users for user assistance.	Release 1C; Should / Release 2; Must
3.2.7.8.2.1.1.1.2	The system shall provide phone service for users to contact authorized users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.1.3	The system shall provide e-mail for users to contact authorized users for user assistance.	Release 2; Must
3.2.7.8.2.1.1.1.4	The system shall provide mail for users to contact authorized users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.1.5	The system shall provide real-time text chat for users to contact GPO Service Specialists for user assistance.	Release 2; Could
3.2.7.8.2.1.1.1.6	The system shall provide Facsimile for users to contact authorized users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.1.7	The system shall provide desktop facsimile for users to contact authorized users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.2	The system shall provide multiple methods for authorized users to contact users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.2.1	The system shall provide phone services for authorized users to contact users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.2.2	The system shall provide e-mail for GPO Service Specialists to contact users for user assistance.	Release 2; Must
3.2.7.8.2.1.1.2.3	The system shall provide real-time text chat for authorized users to contact users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.2.4	The system shall provide facsimile for authorized users to contact users for user assistance.	Release 2; Could
3.2.7.8.2.1.1.2.5	The system shall provide desktop facsimile for GPO Service Specialists to contact users for user assistance.	Release 2; Could
3.2.7.8.2.1.2	The system shall provide users with the ability to opt-out of user support features.	Release 2; Could
3.2.7.8.2.1.2.1	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.	Release 2; Could
3.2.7.8.2.1.2.2	The system shall provide users with the ability to enable or disable context specific that consists of clickable help icons or text on the user interface.	Release 2; Could

3.2.7.8.2.1.2.2.1	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.	Release 2; Could
3.2.7.8.2.1.2.2.2	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.	Release 2; Could
3.2.7.8.2.1.2.2.3	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.	Release 2; Could
3.2.7.8.2.1.2.2.4	The system shall have the capability to process e-mail marketing campaigns	Release 2; Could

3.2.7.8.2.2	**User Support - Context Specific Help**	
3.2.7.8.2.2.1	The system shall provide context-specific help on user interfaces.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.1	Content of context specific help shall be related to what is being viewed on the screen and shall be dynamically generated.	Release 2; Could / Release 3; Must
3.2.7.8.2.2.1.2	Deleted.	
3.2.7.8.2.2.1.3	Context specific help shall consist of help menus.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.3.1	Help menus shall contain user support information related to what is on the current user interface.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.3.2	Help menus shall provide access to all available user support information for the entire system.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.3.3	Authorized uses shall have the ability to manage information (text, images, audio, video, multimedia) in the help menu.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.3.4	All users shall have the ability to search the help menu.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.3.5	The system shall return search results to the user.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.3.6	All users shall have the ability to navigate the help menu using an index.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.4	Context specific help shall consist of customizable descriptive text displayed when a user points the mouse over an item on the user interface.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.4.1	Authorized users shall have the ability to manage customizable descriptive text.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.5	Context specific help shall consist of clickable help icons or text on the user interface.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.5.1	All users shall have the ability to click on help icons or text.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.2.1.5.2	Upon clicking on help icons or text, the system shall display text, images, audio, video or multimedia components.	Release 1B; Could / Release 1C; Must

3.2.7.8.2.2.1.5.3	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.	Release 1C; Could / Release 2; Must
3.2.7.8.2.2.1.5.4	Authorized users shall have the ability to place help icons or text where needed on the user interface.	Release 1C; Could / Release 2; Must
3.2.7.8.2.2.1.5.5	All users shall have the ability to view information displayed by clickable help icons.	Release 1B; Could / Release 1C; Must

3.2.7.8.2.3	**User Support - Helpdesk**	
3.2.7.8.2.3.1	The system shall have the capability to support a helpdesk to route, track, prioritize, and resolve user inquiries to authorized users.	Release 2; Must
3.2.7.8.2.3.2	Information collected and maintained by the helpdesk shall comply with GPO and Federal privacy policies.	Release 1C; Must
3.2.7.8.2.3.2.1	Information collected and maintained by the helpdesk shall comply with “Records maintained on individuals” Title 5 U.S. Code Sec. 552a, 2000 edition."	Release 2; Must
3.2.7.8.2.3.2.2	Information collected and maintained by the helpdesk shall comply with H.R. 2458, E-Government Act of 2002.	Release 2; Must
3.2.7.8.2.3.3	The system shall have the capability to receive inquiries from registered and non-registered users.	Release 2; Must
3.2.7.8.2.3.3.1	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.	Release 2; Must
3.2.7.8.2.3.4	Users shall have the capability to select from lists of categories when submitting inquiries.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.4.1	Users shall have the capability to select from subgroups of categories when submitting inquiries.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.4.2	Authorized users shall have the capability to manage categories and subcategories.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.5	A user shall have the capability to attach files when submitting inquiries.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.6	The system shall have the capability to notify users that their inquiry has been received.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.7	The system shall have the capability to time and date stamp all inquiries and responses.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.8	The system shall have the capability to notify a user that they have been assigned an inquiry.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.9	The system shall have the capability to route, track, and prioritize inquiries and responses received.	Release 2; Must
3.2.7.8.2.3.9.1	The helpdesk shall have the capability to support multiple departments and additional future departments, when needed.	Release 2; Must
3.2.7.8.2.3.9.2	The helpdesk and knowledge base shall have the capability to synchronize with data entered into the system while not connected to the internet.	Release 2; Must

3.2.7.8.2.3.9.3	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)	Release 2; Must
3.2.7.8.2.3.9.4	Other systems/functional elements shall have the capability to access information stored in the helpdesk.	Release 2; Must
3.2.7.8.2.3.9.5	The helpdesk shall have the capability to access information stored in other systems/functional elements.	Release 2; Must
3.2.7.8.2.3.9.6	The system shall allow users to specify job numbers (e.g., CO Ordering numbers, Request Ordering numbers) and other identifiers (e.g., voucher numbers, ISBN numbers) in inquiry fields.	Release 2; Must
3.2.7.8.2.3.9.7	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)	Release 2; Must
3.2.7.8.2.3.9.8	The system shall assign unique identifiers based on the type of template used. (e.g., to track complaints, modification requests)	Release 2; Must
3.2.7.8.2.3.9.9	The system shall allow authorized GPO users to manage templates for submission of inquiries.	Release 2; Must
3.2.7.8.2.3.9.10	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)	Release 2; Must
3.2.7.8.2.3.9.11	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)	Release 2; Must
3.2.7.8.2.3.10	The system shall allow authorized users to manually create a new inquiry in order to accommodate inquiries that do not enter the system electronically.	Release 2; Must
3.2.7.8.2.3.11	The system shall provide the capability to queue inquiries.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.12	The system shall support priority processing.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.13	The system shall allow authorized users to manage the status categories for inquires.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.14	The system shall provide the capability for authorized users to restrict access to inquiry tracking.	Release 2; Must
3.2.7.8.2.3.15	The system shall provide automated routing of inquiries to the departments/individuals according to workflow guidelines, including the following.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.15.1	Automated inquiry routing shall be based on selections made by the user when an inquiry is made.	Release 1C; Could / Release 2; Must

3.2.7.8.2.3.15.2	Automated inquiry routing shall be based on keywords in the inquiry sent by the user.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.15.3	Automated inquiry routing shall be based on the user class of the inquirer.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.15.4	Deleted.	
3.2.7.8.2.3.16	Authorized users shall have the capability to route inquiries to other authorized users.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.16.1	Authorized users shall have the ability to route an inquiry to a selected individual.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.16.2	Authorized users shall have the ability to route an inquiry to a selected department.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.16.3	Authorized users shall have the ability to route inquiries to users who do not have access to the system using e-mail.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.17	The system shall allow the user to determine the departments or individuals they wish to request answers from.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.17.1	The system shall allow the user to determine the departments they wish to request answers from.	Release 2; Must
3.2.7.8.2.3.17.2	The system shall allow the user individuals they wish to request answers from.	Release 2; Must
3.2.7.8.2.3.18	The system shall provide the capability to request user feedback regarding quality of response given.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.19	The system shall provide users with access to history of their inquiries and responses.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.20	The system shall store inquiries and responses.	Release 2; Must
3.2.7.8.2.3.21	The system shall have the capability to allow authorized users to amend inquiries and responses.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.22	The system shall have the capability for users to search inquiries and responses.	Release 2; Must
3.2.7.8.2.3.23	The system shall allow authorized users to search for inquiries by any field.	Release 2; Must
3.2.7.8.2.3.24	The system shall support the capability to monitor the quality of responses given by helpdesk staff.	Release 1C; Could; / Release 2; Must
3.2.7.8.2.3.25	The system shall have the capability to provide users with access to inquiries from other users related to their queries.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.25.1	The system shall allow for search of inquiries from other users.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.25.2	The system shall provide the capability to assign user access rights to individual questions and answers.	Release 1C; Could / Release 2; Must
3.2.7.8.2.3.26	The system shall provide the capability to record users responding to inquiries.	Release 2; Must
3.2.7.8.2.3.27	The system shall provide the capability to log information exchanges.	Release 2; Must
3.2.7.8.2.3.27.1	Information exchange logs shall store metadata relating to what is being discussed.	Release 2; Must
3.2.7.8.2.3.28	The system shall provide the capability to spell-check inquiries and responses before submission.	Release 1B; Could / Release 2; Must

3.2.7.8.2.4	**User Support - Knowledge Base**	
3.2.7.8.2.4.1	The system shall allow authorized users to add information to a knowledge base.	Release 2; Must
3.2.7.8.2.4.2	The system shall provide the ability for an authorized user to add electronic files to the knowledge base as attachments.	Release 2; Must
3.2.7.8.2.4.3	The system shall provide the capability to create customized templates for knowledge base entries.	Release 2; Could
3.2.7.8.2.4.3.1	The system shall provide the capability for authorized users to choose from a list of templates when creating knowledge base entries.	Release 2; Could
3.2.7.8.2.4.4	The system shall have the capability to time and date stamp all knowledge base entries.	Release 2; Must
3.2.7.8.2.4.5	The system shall provide the ability for authorized users to manage information in the knowledge base.	Release 2; Must
3.2.7.8.2.4.6	The system shall provide the capability to add inquiries and answers from the helpdesk to the knowledge base.	Release 2; Must
3.2.7.8.2.4.6.1	The system shall allow authorized users to edit and approve inquiries and responses for addition to the knowledge base.	Release 2; Must
3.2.7.8.2.4.6.2	The system shall have the capability for GPO users to recommend helpdesk inquiries and responses for the knowledge base.	Release 2; Must
3.2.7.8.2.4.7	The system shall provide the ability for authorized users to create categories and subcategories for information stored in the knowledge base.	Release 2; Must
3.2.7.8.2.4.8	The system shall provide the capability to store standard responses for use by specific user groups or subgroups.	Release 1C; Could / Release 2; Must
3.2.7.8.2.4.9	The system shall allow for information stored in the knowledge base to have role-based access restrictions.	Release 2; Must
3.2.7.8.2.4.9.1	The system shall allow for access restrictions to be applied to complete categories.	Release 2; Must
3.2.7.8.2.4.9.2	The system shall allow for access restrictions to be applied to individual knowledge base entries.	Release 2; Must
3.2.7.8.2.4.9.2.1	The system shall allow users to assign key words to knowledge base entries.	Release 2; Must
3.2.7.8.2.4.9.2.2	The system shall allow for fields (e.g., subject, title) with an unlimited number of characters.	Release 2; Must
3.2.7.8.2.4.9.2.3	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)	Release 2; Must
3.2.7.8.2.4.9.2.4	The system shall have the capability for intelligent searching of knowledge base. (e.g., when searching, system asks, “did you mean xxx”?)	Release 2; Must
3.2.7.8.2.4.9.2.5	The system shall have the capability to search by title.	Release 2; Must

3.2.7.8.2.4.9.2.6	The system shall have the capability to search by unique identifiers.	Release 2; Must
3.2.7.8.2.4.9.2.7	The system shall provide the capability to store standard responses for knowledge base entries for use by specific user groups or subgroups.	Release 2; Must
3.2.7.8.2.4.10	The system shall provide the capability for all users to search the knowledge base.	Release 2; Must
3.2.7.8.2.4.10.1	The system shall provide the capability for all users to perform a full-text search the knowledge base.	Release 2; Must
3.2.7.8.2.4.10.2	The system shall provide the capability for all users to search the knowledge base by phrase.	Release 2; Must
3.2.7.8.2.4.10.3	The system shall provide the capability for all users to search the knowledge base by identification number.	Release 2; Must
3.2.7.8.2.4.11	The system shall provide the capability to sort results of knowledge base searches.	Release 2; Must
3.2.7.8.2.4.11.1	The system shall provide the capability to sort search results by category.	Release 2; Must
3.2.7.8.2.4.11.2	The system shall provide the capability to sort search results by subject.	Release 2; Must
3.2.7.8.2.4.11.3	The system shall provide the capability to sort search results by a default sort.	Release 2; Must
3.2.7.8.2.4.12	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.	Release 1B; Could / Release 2; Must
3.2.7.8.2.4.13	The system shall provide the capability to perform records management functions on knowledge base data.	Release 2; Must
3.2.7.8.2.4.14	The system shall provide the capability to spell-check knowledge base entries before submission.	Release 2; Could

3.2.7.8.2.5	**User Support - Alerts**	
3.2.7.8.2.5.1	The system shall have the capability to provide alert services.	Release 1B; Must
3.2.7.8.2.5.1.1	The system shall allow all users to subscribe and unsubscribe to alert services	Release 1B; Could / Release 1C; Must
3.2.7.8.2.5.1.2	Alert services shall be provided via the following channels.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.5.1.2.1	E-mail messages	Release 1C; Must
3.2.7.8.2.5.1.2.2	RSS Feeds conforming to the RSS 2.0 Specification.	Release 1C; Must
3.2.7.8.2.5.1.2.3	Messages while logged into FDsys	Release 1C; Must
3.2.7.8.2.5.1.3	The system shall allow users to chose the method an alert is delivered in from a list of available options.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.5.1.4	The system shall provide alerts based on user profiles and history.	Release 1C; Could / Release 2; Must
3.2.7.8.2.5.1.5	The system shall have the capability to automatically send alerts based on system events.	Release 1B; Could / Release 1C; Must

3.2.7.8.2.5.1.6	The system shall have the capability to automatically send alerts based on business events (e.g., new version of publication available, new services available).	Release 1B; Could / Release 1C; Must
3.2.7.8.2.5.1.7	The system shall have the capability to automatically send notifications to users based on job processing events.	Release 1C; Must
3.2.7.8.2.5.1.8	Authorized users shall be able to create new alert categories where new alerts are manually generated.	Release 1B; Could / Release 1C; Must
3.2.7.8.2.5.1.9	The system shall have the capability to populate the knowledge base with alerts.	Release 1C; Could / Release 2; Must
3.2.7.8.2.5.1.10	The system shall provide the capability for users to add alerts to the knowledge base.	Release 1C; Could / Release 2; Must

3.2.7.8.2.6	**User Support - Training and Events**	
3.2.7.8.2.6.1	The system shall provide users access to training materials and training history.	Release 2; Could
3.2.7.8.2.6.1.1	The system shall provide access to training materials available as digital video.	Release 2; Could
3.2.7.8.2.6.1.2	The system shall provide access to training materials available as digital documents.	Release 2; Could
3.2.7.8.2.6.1.3	The system shall provide access to training materials available as digital audio.	Release 2; Could
3.2.7.8.2.6.1.4	The system shall provide access to training materials available as digital multimedia.	Release 2; Could
3.2.7.8.2.6.1.5	The system shall provide access to training materials available in other formats.	Release 2; Could
3.2.7.8.2.6.2	The system shall allow authorized users to manage training materials and training history.	Release 2; Could
3.2.7.8.2.6.3	The system shall have the capability for authorized users to restrict access to training material and training history.	Release 2; Could
3.2.7.8.2.6.3.1	Access restrictions to training materials shall be based on user class.	Release 2; Could
3.2.7.8.2.6.3.2	Access restrictions to training materials shall be based on individual users.	Release 2; Could
3.2.7.8.2.6.4	The system shall allow users to enroll in training and events.	Release 2; Could
3.2.7.8.2.6.5	The system shall allow authorized users to manage training and events.	Release 2; Could
3.2.7.8.2.6.6	The system shall provide interactive training.	Release 2; Could
3.2.7.8.2.6.6.1	The system shall provide interactive self-paced training.	Release 2; Could
3.2.7.8.2.6.6.2	The system shall provide interactive instructor-led training.	Release 2; Could
3.2.7.8.2.6.7	The system shall provide users verification of enrollment in training and events.	Release 2; Could
3.2.7.8.2.6.8	The system shall provide the capability for users to measure their progress and performance.	Release 2; Could

3.2.7.8.2.6.9	The system shall provide the capability for users to provide feedback on training.	Release 2; Could
3.2.7.8.2.6.10	The system shall provide online tutorials.	Release 2; Could

3.2.7.8.2.7	**Contact Management**	
3.2.7.8.2.7.1	The system shall enable GPO users to view and manage contact data while not connected to the internet or internal server.	Release 2; Must
3.2.7.8.2.7.2	The system shall have the capability to synchronize data managed offline with the contact database when reconnected.	Release 2; Must
3.2.7.8.2.7.3	The system shall enable GPO users to track contact data (e.g., name, company, address, phone, e-mail, last meeting date, and status).	Release 2; Must
3.2.7.8.2.7.4	The system shall enable GPO users to create customizable fields for contact data (e.g., billing address code, GPO Express Customer).	Release 2; Must
3.2.7.8.2.7.5	The system shall enable GPO users to manage notes, history, sales, and attached files to each contact record.	Release 2; Must
3.2.7.8.2.7.6	The system shall allow each contact to have an owner associated with the contact record.	Release 2; Must
3.2.7.8.2.7.7	The system shall enable GPO users to manage groups of related contact records (e.g., all contacts at a single agency).	Release 2; Must
3.2.7.8.2.7.8	The system shall enable GPO users to hierarchically group contact records.	Release 2; Must
3.2.7.8.2.7.9	The system shall enable GPO users to track sales opportunities.	Release 2; Must
3.2.7.8.2.7.10	The system shall enable GPO users to generate sales opportunities reports.	Release 2; Must
3.2.7.8.2.7.11	The system shall have the capability to integrate with GPO's e-mail client (e.g., Microsoft Outlook).	Release 2; Must
3.2.7.8.2.7.12	The system shall have the capability to integrate with handheld devices used by GPO employees (e.g., Blackberry devices).	Release 2; Must
3.2.7.8.2.7.13	The system shall have a calendar which synchronizes with GPO's e-mail client calendar.	Release 2; Must
3.2.7.8.2.7.14	The system shall enable GPO users to schedule calls, meetings and tasks associated with each contact record.	Release 2; Must
3.2.7.8.2.7.15	The system shall enable users to prioritize tasks.	Release 2; Must
3.2.7.8.2.7.16	The system shall enable GPO users to generate mail merges using information stored in contact records.	Release 2; Must
3.2.7.8.2.7.17	The system shall enable GPO users to search records with any field.	Release 2; Must
3.2.7.8.2.7.18	The system shall enable GPO users to search for empty fields or non-empty fields.	Release 2; Must
3.2.7.8.2.7.19	The system shall enable GPO users to generate reports.	Release 2; Must

3.2.7.8.2.7.20	The system shall enable GPO users to create customized report templates/layouts.	Release 2; Must
3.2.7.8.2.7.21	The system shall allow users to record and store meeting minutes with internal and external contacts.	Release 2; Could
3.2.7.8.2.7.22	The system shall allow users to associate multiple internal and external contacts with the meeting minutes.	Release 2; Could
3.2.7.8.2.7.23	The system shall allow users to associate meeting minutes with a list of hierarchical categories.	Release 2; Could
3.2.7.8.2.7.24	The system shall allow users to record the date, time, location and subject of the meeting.	Release 2; Could
3.2.7.8.2.7.25	The system shall allow users to record the content of the meeting using an unlimited number of characters.	Release 2; Could
3.2.7.8.2.7.26	The system shall allow users to create reports with details of all meeting minutes.	Release 2; Could
3.2.7.8.2.7.27	The system shall allow users to filter the data for the report by contact, department, and category.	Release 2; Could
3.2.7.8.2.7.28	The system shall allow users to create reports including the following elements:	Release 2; Could
3.2.7.8.2.7.29	Meeting subject	Release 2; Could
3.2.7.8.2.7.30	List of all contacts associated with the meeting	Release 2; Could
3.2.7.8.2.7.31	Date, time and location of meeting	Release 2; Could
3.2.7.8.2.7.32	Full meeting minutes	Release 2; Could
3.2.7.8.2.7.33	List of all categories associated with the meeting	Release 2; Could

3.2.8.2	**Requirements for Content Delivery and Processing**	
3.2.3.2.8.2.1	**Content Delivery Core Capabilities**	
3.2.8.2.1.1	The system shall have the capability to retrieve ACPs from Access Content Storage based on user request.	Release 1C; Must
3.2.8.2.1.2	The system shall have the capability to create DIPs from ACPs in delivery processing based upon a user request.	Release 1C; Must
3.2.8.2.1.3	The system shall have the capability to create pre-ingest bundles in delivery processing.	Release 1C; Must
3.2.8.2.1.4	The system shall have the capability to deliver DIPs and pre-ingest bundles based on user requests.	Release 1C; Must
3.2.8.2.1.4.1	The system shall have the capability to deliver DIPs based on user requests.	Release 1C; Must
3.2.8.2.1.4.2	The system shall have the capability to deliver pre-ingest bundles based on user requests.	Release 1C; Must
3.2.8.2.1.6	Users shall have the ability to pull DIPs and pre-ingest bundles from the system.	Release 1C; Must
3.2.8.2.1.6.1	The system shall provide the capability for a user to request the download of a DIP from the system.	Release 1C; Must
3.2.8.2.1.6.2	The system shall provide the capability for a user to perform an FTP get on a DIP from the system.	Release 1C; Must

3.2.8.2.1.6.3	The system shall support the capability for a user to pull a DIP from the system using additional methods in the future.	Release 3; Must
3.2.8.2.1.6.4	The system shall provide the capability for a user to request the download of a PIB from the system.	Release 1C; Must
3.2.8.2.1.6.5	The system shall provide the capability for a user to perform an FTP get on a PIB from the system.	Release 1C; Must
3.2.8.2.1.6.6	The system shall support the capability for a user to pull a PIB from the system using additional methods in the future.	Release 3; Must
3.2.8.2.1.7	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.	Release 1C; Must
3.2.8.2.1.7.1	The system shall have the capability to restrict Service Providers' access to DIPs for jobs that they have not been awarded.	Release 1C; Must
3.2.8.2.1.7.2	The system shall have the capability to restrict Service Providers' access to pre-ingest bundles for jobs that they have not been awarded.	Release 1C; Must
3.2.8.2.1.8	The system shall have the capability to determine if delivery is possible.	Release 1C; Must
3.2.8.2.1.8.1	The system shall have the capability to determine if delivery is possible based upon business rules.	Release 1C; Must
3.2.8.2.1.8.2	The system shall have the capability to determine if delivery is possible based upon limitations of delivery mechanisms.	Release 1C; Must
3.2.8.2.1.8.3	The system shall have the capability to determine if delivery is possible based upon limitations of content formats.	Release 1C; Must
3.2.8.2.1.8.4	The system shall have the capability to inform users that delivery is not possible.	Release 1C; Must
3.2.8.2.1.8.5	The system shall have the capability to inform users why delivery is not possible.	Release 1C; Must
3.2.8.2.1.9	The system shall have the capability to provide users with estimated transfer time for delivery.	Release 1C; Could
3.2.8.2.1.10	The system shall have the capability to provide notification of fulfillment to users.	Release 1B; Must
3.2.8.2.1.10.1	The system shall have the capability to provide notification based on user preferences.	Release 1B; Should / Release 1C; Must
3.2.8.2.1.10.2	The system shall have the capability to provide notification based on information gathered at time of request.	Release 1B; Must

3.2.8.2.2	**Content Delivery Processing**	
3.2.8.2.2.1	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.	Release 1B; Must
3.2.8.2.2.1.1	The system shall have the capability to package DIPs containing digital objects.	Release 1B; Must

3.2.8.2.2.1.2	The system shall have the capability to package DIPs containing metadata.	Release 1B; Must
3.2.8.2.2.1.3	The system shall have the capability to package DIPs containing BPI.	Release 1B; Must
3.2.8.2.2.2	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.	Release 1C; Must
3.2.8.2.2.2.1	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.	Release 1C; Must
3.2.8.2.2.2.2	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.	Release 1C; Must
3.2.8.2.2.2.3	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.	Release 1C; Must
3.2.8.2.2.3	The system shall have capability to transform digital objects to different formats.	Release 1C; Must
3.2.8.2.2.4	The system shall have the capability to make adjustments to digital objects for delivery based on digital object format.	Release 1B; Could / Release 2; Must
3.2.8.2.2.4.1	The system shall have the capability to adjust the resolution of digital objects.	Release 1B; Could / Release 2; Must
3.2.8.2.2.4.2	The system shall have the capability to resize digital objects.	Release 1B; Could / Release 2; Must
3.2.8.2.2.4.3	The system shall have the capability to adjust the compression of digital objects.	Release 1B; Could / Release 2; Must
3.2.8.2.2.4.4	The system shall have the capability to adjust the color space of digital objects. (e.g., CMYK to RGB)	Release 1B; Could / Release 2; Must
3.2.8.2.2.4.5	The system shall have the capability to adjust the image quality settings of digital objects. (e.g., transparency, dithering, anti-aliasing)	Release 1B; Could / Release 2; Must
3.2.8.2.2.4.6	The system shall have the capability to rasterize digital objects.	Release 1B; Could / Release 2; Must
3.2.8.2.2.5	The system shall have the capability to process DIPs based on user request.	Release 1C; Must
3.2.8.2.2.6	The system shall have the capability to repurpose content from multiple packages into a single DIP.	Release 2; Must

3.2.8.2.3	**Content Delivery Mechanisms**	
3.2.8.2.3.1	The system shall have the capability to push DIPs and PIBs to users using various delivery mechanisms.	Release 1C; Must
3.2.8.2.3.1.1	The system shall have the capability to push DIPs to users using an RSS feeds conforming to the RSS 2.0 Specification.	Release 1C; Must

3.2.8.2.3.1.2	The system shall have the capability to push DIPs to users using E-mail.	Release 1C; Must
3.2.8.2.3.1.3	The system shall have the capability to push DIPs to users using File Transfer Protocol.	Release 1C; Must
3.2.8.2.3.1.4	The system shall have the capability to push DIPs to users using Secure File Transfer Protocol.	Release 3; Must
3.2.8.2.3.1.5	The system shall support the capability to push DIPs to users using additional methods in the future.	Release 3; Must
3.2.8.2.3.1.6	The system shall have the capability to push PIBs to users using RSS feeds conforming to the RSS 2.0 Specification.	Release 1C; Must
3.2.8.2.3.1.7	The system shall have the capability to push PIBs to users using E-mail.	Release 1C; Must
3.2.8.2.3.1.8	The system shall have the capability to push PIBs to users using File Transfer Protocol.	Release 1C; Must
3.2.8.2.3.1.9	The system shall have the capability to push PIBs to users using Secure File Transfer Protocol.	Release 3; Must
3.2.8.2.3.1.10	The system shall support the capability to push PIBs to users using additional methods in the future.	Release 3; Must
3.2.8.2.3.1.11	The maximum size DIP delivered by HTTP download shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.12	The maximum size PIB delivered by HTTP download shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.13	The maximum size DIP delivered by RSS feed shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.14	The maximum size PIB delivered by RSS feed shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.15	The maximum size DIP delivered by e-mail shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.16	The maximum size PIB delivered by e-mail shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.17	The maximum size DIP delivered by FTP shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.18	The maximum size PIB delivered by FTP shall be configurable by an authorized user.	Release 1C; Must
3.2.8.2.3.1.19	The maximum size DIP delivered by a future electronic channel shall be configurable by an authorized user.	Release 3; Must
3.2.8.2.3.1.20	The maximum size PIB delivered by a future electronic channel shall be configurable by an authorized user.	Release 3; Must
3.2.8.2.3.1.21	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.	Release 3; Must
3.2.8.2.3.1.22	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.	Release 3; Must

3.2.8.2.3.1.23	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.	Release 3; Must
3.2.8.2.3.1.24	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.	Release 3; Must
3.2.8.2.3.2	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.	Release 1B; Must

3.2.8.3.2	**Requirements for Hard Copy Output**	
3.2.8.3.2.1	**Hard Copy Output Core Capabilities**	
3.2.8.3.2.1.1	The system shall have the capability to deliver DIPs and pre-ingest bundles to users from which hard copy output can be created.	Release 1B; Must
3.2.8.3.2.1.1.1	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).	Release 1B; Must
3.2.8.3.2.1.1.1.1	The system shall have the capability to provide DIPs that support the production of hard copy on any required hard copy output technology.	Release 1B; Must
3.2.8.3.2.1.1.1.2	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.	Release 1B; Must
3.2.8.3.2.1.2	The system shall have the capability to deliver DIPs and pre-ingest bundles that support static text and images.	Release 1B; Must
3.2.8.3.2.1.2.1	The system shall have the capability to deliver DIPs that support static text and images.	Release 3; Could
3.2.8.3.2.1.2.2	The system shall have the capability to deliver pre-ingest bundles that support static text and images.	Release 3; Could
3.2.8.3.2.1.3	The system shall have the capability to support hard copy output for variable data printing processes.	Release 3; Could
3.2.8.3.2.1.4	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.	Release 2; Could
3.2.8.3.2.1.4.1	The system shall allow users to manually add the Imprint line.	Release 2; Could
3.2.8.3.2.1.4.2	The system shall automatically add the Imprint Line.	Release 2; Could
3.2.8.3.2.1.4.3	The system shall allow users to manually adjust the location of the Imprint line.	Release 2; Could

3.2.8.3.2.1.5	DIPs and pre-ingest bundles for hard copy output shall be delivered in file formats that conform to industry best practices.	Release 1B; Must
3.2.8.3.2.1.5.1	The system shall have the capability to deliver files in their native application file format.	Release 1B; Must
3.2.8.3.2.1.5.1.1	The system shall have the capability to convert native files to PDF.	Release 1C; Must
3.2.8.3.2.1.5.2	The system shall have the capability to deliver optimized (print, press) PDFs.	Release 1B; Must
3.2.8.3.2.1.5.2.1	Optimized PDFs shall have fonts and images embedded.	Release 1B; Must
3.2.8.3.2.1.5.2.2	Image resolution of PDFs shall conform to industry best practices as defined in GPO's press optimized PDF settings.	Release 1B; Must
3.2.8.3.2.1.5.3	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files.	Release 1B; Must
3.2.8.3.2.1.5.3.1	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe InDesign.	Release 1B; Must
3.2.8.3.2.1.5.3.2	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in QuarkXPress.	Release 1B; Must
3.2.8.3.2.1.5.3.3	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe Framemaker.	Release 1B; Must
3.2.8.3.2.1.5.3.4	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe Pagemaker.	Release 1B; Must
3.2.8.3.2.1.5.3.5	The system shall support the capability to deliver page layout files containing images, fonts, and linked text files in additional formats in the future.	Release 3; Must
3.2.8.3.2.1.5.4	The system shall have the capability to deliver vector graphics.	Release 1B; Must
3.2.8.3.2.1.5.5	The system shall have the capability to deliver raster images.	Release 1B; Must
3.2.8.3.2.1.5.6	The system shall have the capability to deliver Microsoft Office Suite application files.	Release 1B; Must
3.2.8.3.2.1.5.6.1	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Word.	Release 1B; Must
3.2.8.3.2.1.5.6.2	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft PowerPoint.	Release 1B; Must
3.2.8.3.2.1.5.6.3	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Excel.	Release 1B; Must
3.2.8.3.2.1.5.6.4	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Visio.	Release 1B; Must
3.2.8.3.2.1.5.7	The system shall have the capability to deliver XML.	Release 1B; Must

3.2.8.3.2.1.5.7.1	The system shall support cascading style sheets.	Release 1B; Must
3.2.8.3.2.1.5.7.2	The system shall support document type definition/schema.	Release 1B; Must
3.2.8.3.2.1.5.8	The system shall have the capability to deliver text files.	Release 1B; Must
3.2.8.3.2.1.5.8.1	The system shall have the capability to deliver text files in Rich Text (RTF) format.	Release 1B; Must
3.2.8.3.2.1.5.8.2	The system shall have the capability to deliver text files in ASCII text format.	Release 1B; Must
3.2.8.3.2.1.5.8.3	The system shall have the capability to deliver text files in Unicode format.	Release 1B; Must
3.2.8.3.2.1.5.8.4	The system shall have the capability to deliver text files in Universal Multi-Octet Coded Character Set - ISO/IEC 10646 format.	Release 1B; Must
3.2.8.3.2.1.5.8.5	The system shall support the capability to deliver text files in additional file formats in the future.	Release 3; Must
3.2.8.3.2.1.5.9	The system shall have the capability to deliver OASIS Open Document Format for Office Applications (OpenDocument) v1.0.	Release 1B; Must
3.2.8.3.2.1.5.10	The system shall have the capability to deliver postscript files.	Release 1B; Must
3.2.8.3.2.1.6	The system shall have the capability to generate DIPs and pre-ingest bundles that contain Job Definition Format (JDF) data.	Release 3; Could

3.2.8.4.2	**Requirements for Electronic Presentation**	
3.2.8.4.2.1	**Electronic Presentation Core Capabilities**	
3.2.8.4.2.1.1	The system shall have the capability to create DIPs for electronic presentation that comply with the FDsys accessibility requirements.	Release 1C; Must
3.2.8.4.2.1.1.1	The system shall have the capability to manually check digital objects for compliance with FDsys accessibility requirements.	Release 1C; Must
3.2.8.4.2.1.1.2	The system shall have the capability to automatically check digital objects for compliance with FDsys accessibility requirements.	Release 2; Must
3.2.8.4.2.1.1.3	The system shall have the capability to manually transform digital objects so that they are compliant with FDsys accessibility requirements.	Release 1C; Must
3.2.8.4.2.1.1.4	The system shall have the capability to automatically transform digital objects so that they are compliant with FDsys accessibility requirements.	Release 2; Must
3.2.8.4.2.1.2	The system shall have the capability to render content for presentation on end user devices.	Release 2; Must
3.2.8.4.2.1.3	The system shall have the capability to render content for presentation on multiple computer platforms, including but not limited to Windows, Macintosh, and Unix.	Release 2; Must

3.2.8.4.2.1.3.1	The system shall have the capability to render content for presentation on a Windows platform.	Release 1C; Must
3.2.8.4.2.1.3.2	The system shall have the capability to render content for presentation on Macintosh platform.	Release 1C; Must
3.2.8.4.2.1.3.3	The system shall have the capability to render content for presentation on a Unix platform.	Release 2; Must
3.2.8.4.2.1.4	The system shall have the capability to render content for presentation on non-desktop devices.	Release 2; Should / Release 3; Must
3.2.8.4.2.1.4.1	The system shall have the capability to render content for presentation on Digital Assistants (PDAs).	Release 2; Should / Release 3; Must
3.2.8.4.2.1.4.2	The system shall have the capability to render content for presentation on Digital Audio Players.	Release 2; Should / Release 3; Must
3.2.8.4.2.1.4.3	The system shall have the capability to render content for presentation on Electronic Books (E-Books).	Release 2; Should / Release 3; Must
3.2.8.4.2.1.4.4	The system shall have the capability to render content for presentation on Cell Phones.	Release 2; Should / Release 3; Must
3.2.8.4.2.1.5	The system shall have the capability to determine and deliver the file format needed for non-desktop electronic devices.	Release 2; Could
3.2.8.4.2.1.6	The system shall provide the capability to deliver DIPs that support static and dynamic text in multiple formats.	Release 2; Must
3.2.8.4.2.1.6.1	The system shall have the capability to deliver electronic content in XML conforming to Extensible Markup Language (XML) 1.1.	Release 1B; Must
3.2.8.4.2.1.6.2	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 conforming to the HTML 4.0.1 Specification.	Release 1B; Must
3.2.8.4.2.1.6.3	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 conforming to the XHTML™ 1.0 The Extensible Hypertext Markup Language (Second Edition) specification.	Release 1B; Must
3.2.8.4.2.1.6.4	The system shall have the capability to deliver electronic content in ASCII text conforming to ANSI INCITS 4-1986 (R2002).	Release 1B; Must
3.2.8.4.2.1.6.4.1	The system shall have the capability to convert images to descriptive ASCII text.	Release 2; Must
3.2.8.4.2.1.6.4.1.1	The system shall have the capability to replace images with descriptive text when available while converting digital objects to ASCII.	Release 1C; Must
3.2.8.4.2.1.6.5	The system shall have the capability to deliver electronic content in Unicode text conforming to the Unicode Standard, Version 4.0.	Release 1B; Must
3.2.8.4.2.1.6.5.1	The system shall have the capability to convert images to descriptive Unicode text.	Release 2; Must

3.2.8.4.2.1.6.5.1.1	The system shall have the capability to replace images with descriptive text when available while converting digital objects to ASCII.	Release 1C; Must
3.2.8.4.2.1.6.6	The system shall have the capability to deliver electronic content in Open Document Format conforming to OpenDocument Format for Office Applications (OpenDocument) v1.0.	Release 1B; Must
3.2.8.4.2.1.6.7	The system shall have the capability to deliver content in MS Office formats.	Release 1B; Must
3.2.8.4.2.1.6.7.1	The system shall have the capability to deliver electronic content in Microsoft Excel (.xls) format.	Release 1B; Must
3.2.8.4.2.1.6.7.2	The system shall have the capability to deliver electronic content in Microsoft Word Document File Format (.doc).	Release 1B; Must
3.2.8.4.2.1.6.7.3	The system shall have the capability to deliver electronic content in Microsoft PowerPoint File Format (.ppt).	Release 1B; Must
3.2.8.4.2.1.6.7.4	The system shall have the capability to deliver electronic content in Microsoft Publisher File Format (.pub).	Release 1B; Must
3.2.8.4.2.1.6.8	The system shall have the capability to deliver electronic content in PDF conforming to PDF Reference, Fifth Edition, Version 1.6.	Release 1B; Must
3.2.8.4.2.1.6.9	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.	Release 2; Could
3.2.8.4.2.1.7	The system shall provide the capability to deliver DIPs that support static and dynamic images in multiple formats.	Release 1B; Must
3.2.8.4.2.1.7.1	The system shall have the capability to deliver electronic content in JPEG conforming to ISO/IETC 10918-1: 1994 Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines.	Release 1B; Must
3.2.8.4.2.1.7.2	The system shall have the capability to deliver electronic content in JPEG 2000 conforming to ISO/IEC 15444-6:2003 Information technology -- JPEG 2000 image coding system -- Part 6: Compound image file format.	Release 1B; Must
3.2.8.4.2.1.7.3	The system shall have the capability to deliver electronic content in TIFF conforming to TIFF – Revision 6.0.	Release 1B; Must
3.2.8.4.2.1.7.4	The system shall have the capability to deliver electronic content in GIF conforming to Graphics Interchange Format: Version 89a.	Release 1B; Must
3.2.8.4.2.1.7.5	The system shall have the capability to deliver electronic content in SVG conforming to Scalable Vector Graphic (SVG) 1.1 Specification.	Release 1B; Must

3.2.8.4.2.1.7.6	The system shall have the capability to deliver electronic content in EPS conforming to Encapsulated PostScript File Format Specification Version 3.0.	Release 1B; Must
3.2.8.4.2.1.8	The system shall provide the capability to deliver DIPs that support audio information in multiple formats, including, but not limited to:	Release 1B; Must
3.2.8.4.2.1.8.1	The system shall have the capability to deliver audio content in MPEG 1 – Audio Layer 3 (MP3) conforming to ISO/IEC 11172-3:1993 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s -- Part 3: Audio	Release 1C; Must
3.2.8.4.2.1.8.2	The system shall have the capability to deliver audio content in FLAC (Free Lossless Audio Codec) conforming to Free Lossless Audio Codec specifications.	Release 1C; Could
3.2.8.4.2.1.8.3	The system shall have the capability to deliver audio content in Ogg Vorbis conforming to the Vorbis I Specification.	Release 1C; Could
3.2.8.4.2.1.8.4	The system shall have the capability to deliver audio content in CDDA (Compact Disc Digital Audio) conforming to Audio Recording – Compact disc digital audio system. (IEC 60908 Ed. 2.0).	Release 1C; Must
3.2.8.4.2.1.9	The system shall provide the capability to deliver DIPs that support audiovisual content (e.g., video, multimedia) in MPEG format.	Release 1B; Should / Release 1C; Must
3.2.8.4.2.1.10	The system shall have the capability to deliver electronic content that maintains desired user functionality.	Release 1B; Must
3.2.8.4.2.1.10.1	The system shall deliver electronic content that maintains hyperlinks to the extent possible.	Release 1B; Must
3.2.8.4.2.1.10.2	The system shall deliver electronic content that maintains interactive content functionality.	Release 1B; Must

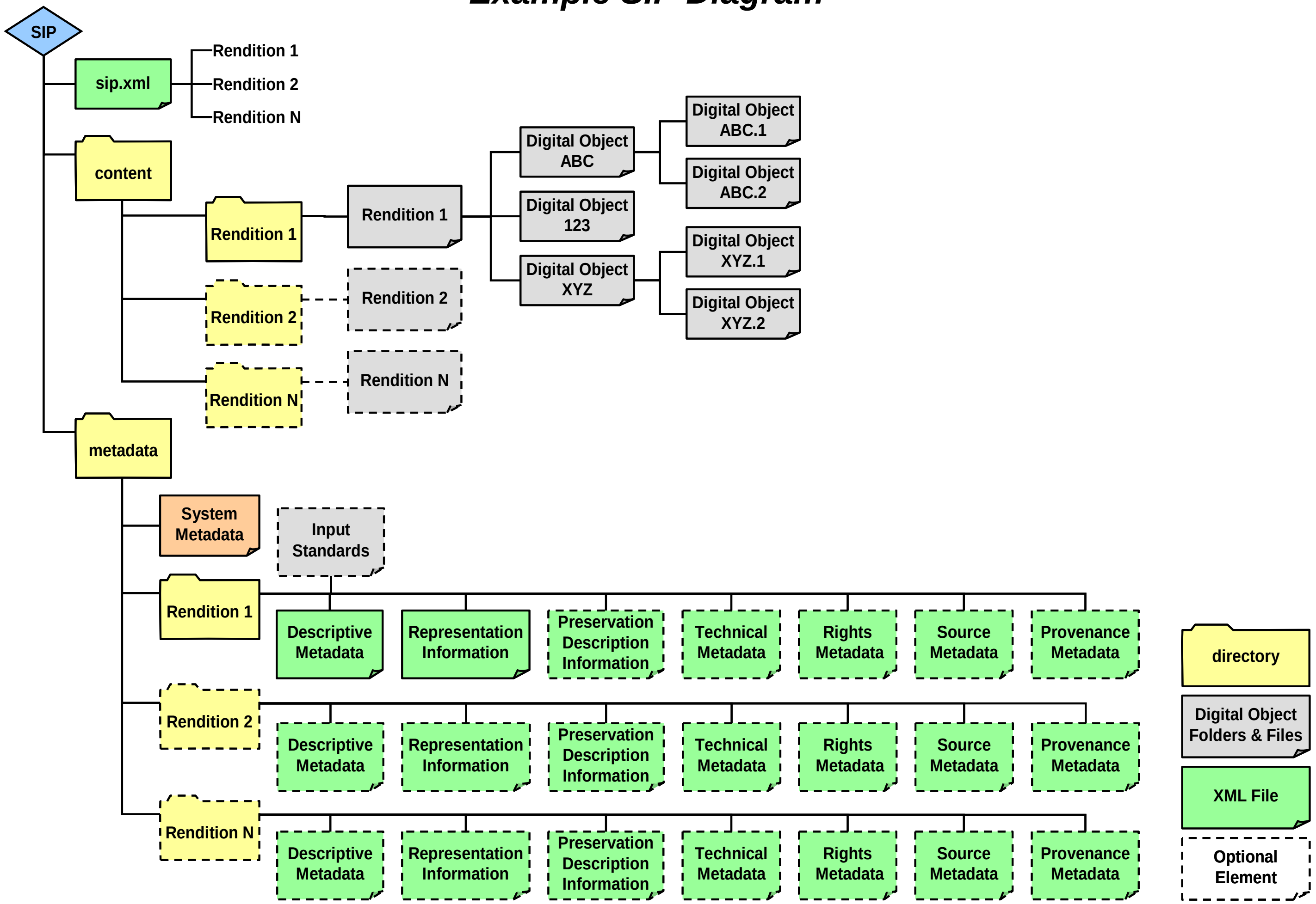
3.2.8.5.2	**Requirements for Digital Media**	
3.2.8.5.2.1	**Digital Media Core Capabilities**	
3.2.8.5.2.1.1	The system shall have the capability to deliver pre-ingest bundles and DIPs for digital media containing electronic content for electronic presentation, hard copy output or data storage.	Release 1B; Must
3.2.8.5.2.1.2	The system shall have the capability to deliver pre-ingest bundles and DIPs that support the creation of removable digital media.	Release 1B; Must
3.2.8.5.2.1.2.1	The system shall have the capability to deliver pre-ingest bundles and DIPs that support the creation of removable optical digital media.	Release 1B; Must
3.2.8.5.2.1.2.1.1	Compact Discs (CD)	Release 1B; Must
3.2.8.5.2.1.2.1.2	Digital Versatile Discs (DVD)	Release 1B; Must
3.2.8.5.2.1.2.1.3	Blu-ray Discs (BD)	Release 2; Could

3.2.8.5.2.1.2.2	The system shall have the capability to deliver pre-ingest bundles and DIPs that support the creation of removable magnetic digital media.	Release 1B; Must
3.2.8.5.2.1.2.2.1	The system shall have the capability to deliver pre-ingest bundles that support the creation of magnetic tapes.	Release 1B; Must
3.2.8.5.2.1.2.2.2	The system shall have the capability to deliver pre-ingest bundles that support the creation of removable magnetic hard disks.	Release 1B; Must
3.2.8.5.2.1.2.2.3	The system shall have the capability to deliver pre-ingest bundles that support the creation of magnetic floppy disks.	Release 1B; Must
3.2.8.5.2.1.2.2.4	The system shall have the capability to deliver DIPs that support the creation of magnetic tapes.	Release 1B; Must
3.2.8.5.2.1.2.2.5	The system shall have the capability to deliver DIPs that support the creation of removable magnetic hard disks.	Release 1B; Must
3.2.8.5.2.1.2.2.6	The system shall have the capability to deliver DIPs that support the creation of magnetic floppy disks.	Release 1B; Must
3.2.8.5.2.1.2.3	The system shall have the capability to deliver pre-ingest bundles and DIPs that support the creation of removable semiconductor digital media.	Release 1B; Must
3.2.8.5.2.1.2.3.1	The system shall have the capability to deliver pre-ingest bundles for storage on Universal Serial Bus (USB) flash drives.	Release 1B; Must
3.2.8.5.2.1.2.3.2	The system shall have the capability to deliver pre-ingest bundles for storage on flash memory cards.	Release 1B; Must
3.2.8.5.2.1.2.3.3	The system shall have the capability to deliver DIPs for storage on Universal Serial Bus (USB) flash drives.	Release 1B; Must
3.2.8.5.2.1.2.3.4	The system shall have the capability to deliver DIPs for storage on flash memory cards.	Release 1B; Must
3.2.8.5.2.1.2.4	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.	Release 1B; Could / Release 2; Should
3.2.8.5.2.1.2.4.1	The system shall have the capability to generate ISO image files.	Release 1B; Could / Release 1C; Should
3.2.8.5.2.1.2.4.2	The system shall have the capability to generate VCD image files.	Release 1B; Could / Release 2; Should
3.2.8.5.2.1.2.4.3	The system shall have the capability to generate UDF image files.	Release 1B; Could / Release 2; Should
3.2.8.5.2.1.2.5	The system shall have the capability to generate autorun files for use on removable digital media.	Release 1C; Could / Release 2; Should
3.2.8.5.2.1.2.5.1	Users shall have the capability to specify the file that will open when the removable digital media is inserted into a computer.	Release 1C; Could / Release 2; Should
3.2.8.5.2.1.3	The system shall have the capability to deliver DIPs and pre-ingest bundles to digital media.	Release 1C; Could / Release 2; Should
3.2.8.5.2.1.3.1	The system shall have the capability to deliver DIPs and pre-ingest bundles to GPO storage devices. (e.g., GPO servers).	Release 1C; Must

3.2.8.5.2.1.3.1.1	The system shall have the capability to deliver DIPs to GPO storage devices.	Release 1C; Must
3.2.8.5.2.1.3.1.2	The system shall have the capability to deliver PIBs to GPO storage devices.	Release 1C; Must
3.2.8.5.2.1.3.2	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)	Release 1B; Should / Release 1C; Must
3.2.8.5.2.1.3.2.1	The system shall have the capability to deliver DIPs to non-GPO storage devices.	Release 1B; Should / Release 1C; Must
3.2.8.5.2.1.3.2.2	The system shall have the capability to deliver PIBs to non-GPO storage devices.	Release 1B; Should / Release 1C; Must
3.2.8.5.2.1.3.3	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	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.1	The system shall have the capability to deliver DIPs to Digital Assistants (PDAs).	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.2	The system shall have the capability to deliver DIPs to Digital Audio Players.	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.3	The system shall have the capability to deliver DIPs to Electronic Books (E-Books).	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.4	The system shall have the capability to deliver DIPs to Cell Phones.	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.5	The system shall have the capability to deliver PIBs to Digital Assistants (PDAs).	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.6	The system shall have the capability to deliver PIBs to Digital Audio Players.	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.7	The system shall have the capability to deliver PIBs to Electronic Books (E-Books).	Release 2; Should / Release 3; Must
3.2.8.5.2.1.3.3.8	The system shall have the capability to deliver PIBs to Cell Phones.	Release 2; Should / Release 3; Must

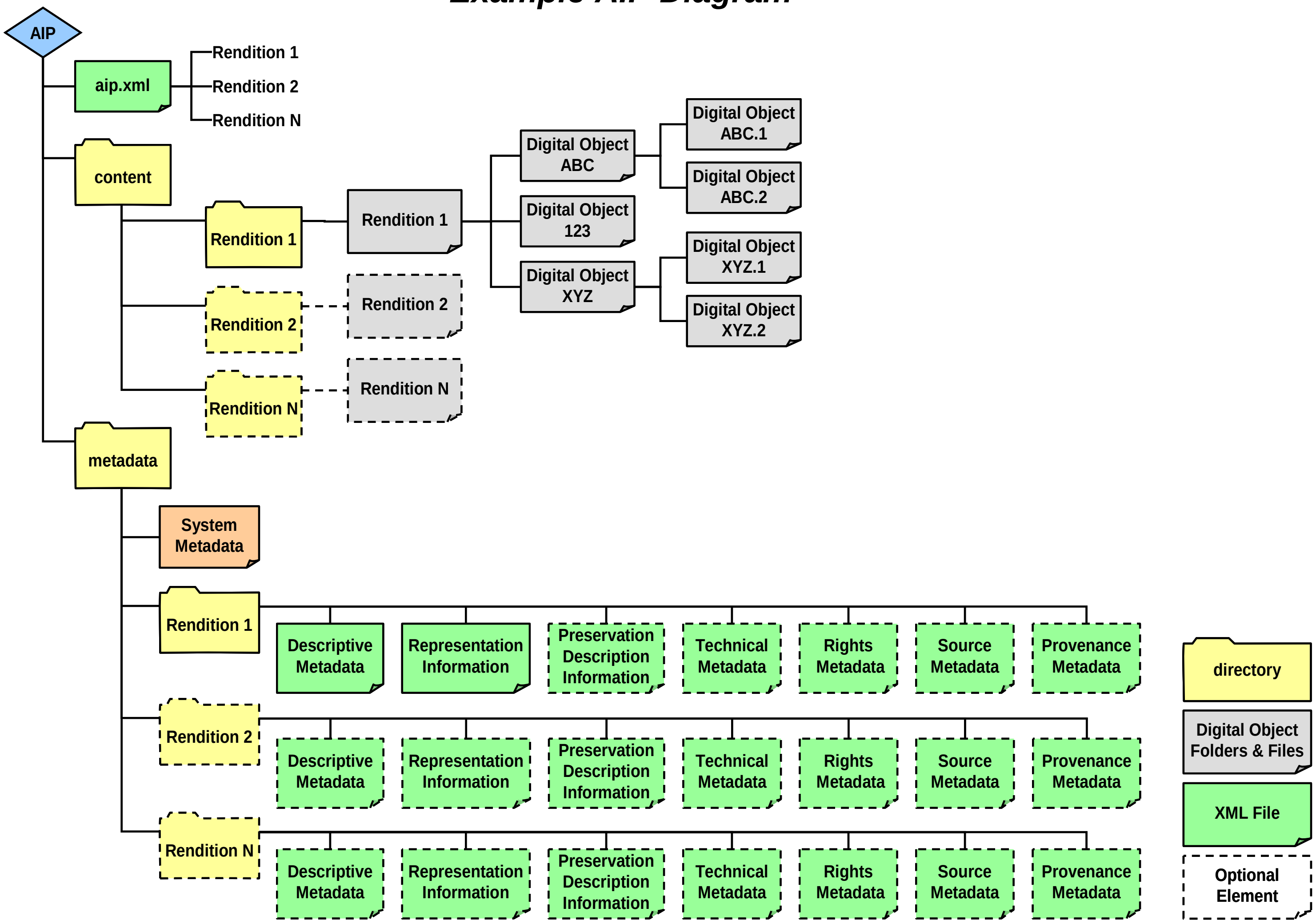
Appendix A – Example Package Diagrams

Example SIP Diagram

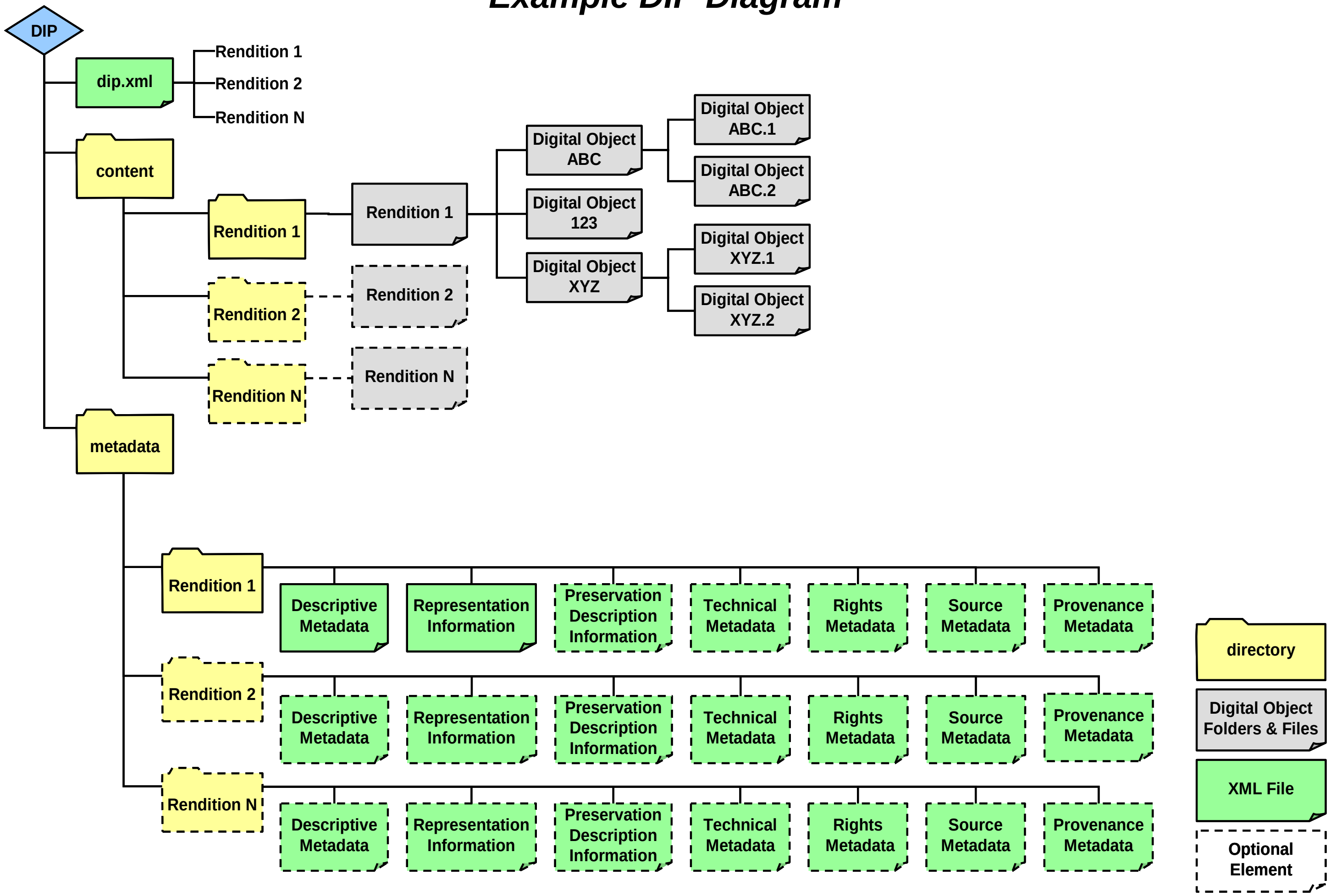


FINAL

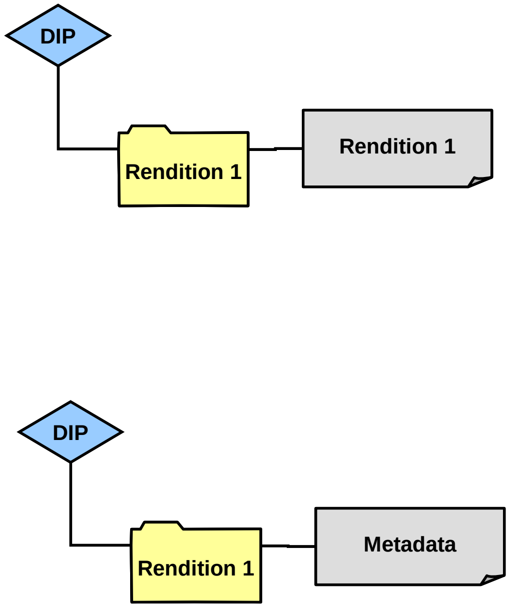
Example AIP Diagram



Example DIP Diagram



Example End User DIPs



Appendix B – 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. An Audit Checklist for the Certification of Trusted Digital Repositories, Draft For Public Comment. College Park, MD: 2005. Research Libraries Group. 29 Mar. 2006 <http://www.rlg.org/en/pdfs/rlgnara-repositorieschecklist.pdf>.

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 C – 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

ACRONYM	DEFINITION
DPI	Dots Per Inch
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

ACRONYM	DEFINITION
MOCAT	Monthly Catalog of Government Publications
MODS	Metadata Object Descriptive Schema
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

ACRONYM	DEFINITION
SHA	Secure Hash Algorithm
SIP	Submission Information Package
SMP	Storage Management Processor
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: A test for the system prior to final release. Beta testing is the last stage of testing, and normally can involves real-world, external exposure or operation of 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.

Internal User Testing: A test for the system prior to final release and prior to Beta testing. This testing involves real-world, internal exposure or operation of the system.

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.

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.