UNITED STATES GOVERNMENT PRINTING OFFICE (GPO)

REQUIREMENTS DOCUMENT
(RD V2.1)

FOR THE

FUTURE DIGITAL SYSTEM (FDsys)

FINAL

April 18, 2006

Document Change/Configuration Control Sheet

Document Title: FDsys Requirements Document (RD 2.0)

Date	Filename / version #	Author	Revision Description
2/10/2006	FDsys RD v2.0 Interim	Baldwin/Villano	Interim System Requirements Document (RD 2.0), first draft
2/27/2006	FDsys RD v2.0 Interim	Fleetwood	Changed formatting from tables to text
3/22/2006	FDsys RD 2.0	Fleetwood	Final Requirements Document; began incorporating updated requirements and documentation
3/29/2006	FDsys RD 2.0	Fleetwood	Completed updating requirements and documentation; sent to PMO for review
3/30/2006	FDsys RD 2.0	PMO	PMO group review completed; sent to CTO and DCTO
3/31/2006	FDsys RD 2.0	PMO	RD 2.0 finalized and released

Document Title: FDsys Requirements Document (RD 2.1)

Date	Filename / version #	Author	Revision Description
4/18/2006	FDsys RD 2.1	PMO	Change to the following requirements resulting from RFP comments: • 1.2.7: *records* changed to *content* • 1.2.13: System response time language modified and requirement changed to <2 Seconds • 2.2.3.3: deleted • 2.2.3.9: clarification to requirement • 3.2.2.4.4.1: changed *AIP* to *SIP* • 3.3.2.3.4: subjectivity removed • 3.4.3.2.11: changed *DIP* to *system* • 4.2.1.2.2.4: functionality of digital objects better defined • 4.4.2.1.1.6: changed from a Must to a Could • 4.4.2.1.1.8: changed from a Must to a Could • 4.4.2.2.2: eliminated, redundant • 4.5.2.1.3: changed from a Must to a Should • 4.5.2.1.12: eliminated *and modifications* • 5.2.2.7.1: changed from a Release 1.A to Release 1.C • 5.2.2.8.1: changed from a Release 1.A to Release 1.C • 5.3.2.2.3.1: eliminated, redundant • 5.3.2.4.1.5.1: elevated to 5.3.2.4.1.6 and added end user to requirement • 5.3.2.7.1.2: changed COOP Plan to COOP plans. GPO sites specific elements rather than a documented PLAN • 5.3.2.7.1.6: reference to National Finance center removed • 7.2.3.3.1: clarified requirement • 8.2.3.2: created this requirement from a bullet under 8.2.3.1 • 8.3.2.1.5.2.2: added detail to requirement

Table of Contents

List of Figures

1.0 Introduction

This Requirements Document (RD V2.0) 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.

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

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

1.1 *System Purpose*

The proposed system will ingest, authenticate, provide version control, 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), whether printed or born digital. 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 *Definitions, Acronyms and Abbreviations*

Appendix A, Acronyms and Glossary contains a complete set of definitions and a list of acronyms used in FDsys documentation.

1.4 *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. 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 Access. U.S. Government Printing Office. 15 Mar. 2006 http://www.gpoaccess.gov.

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>.

1.5 *System Overview*

GPO’s Future Digital System (FDsys) will provide a comprehensive, systematic and dynamic means for preserving electronic content free from dependence on specific hardware or software. The system will automate many of the electronic content lifecycle processes and make it easier to deliver electronic content in formats suited to customers’ needs. FDsys will allow federal Content Originators to easily create and submit content that can then be preserved, authenticated, managed and delivered upon request.

1.6 *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.

For more information on system releases, please reference the document “GPO Future Digital System Releases and Capabilities”.

2.0 General System Description

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

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

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

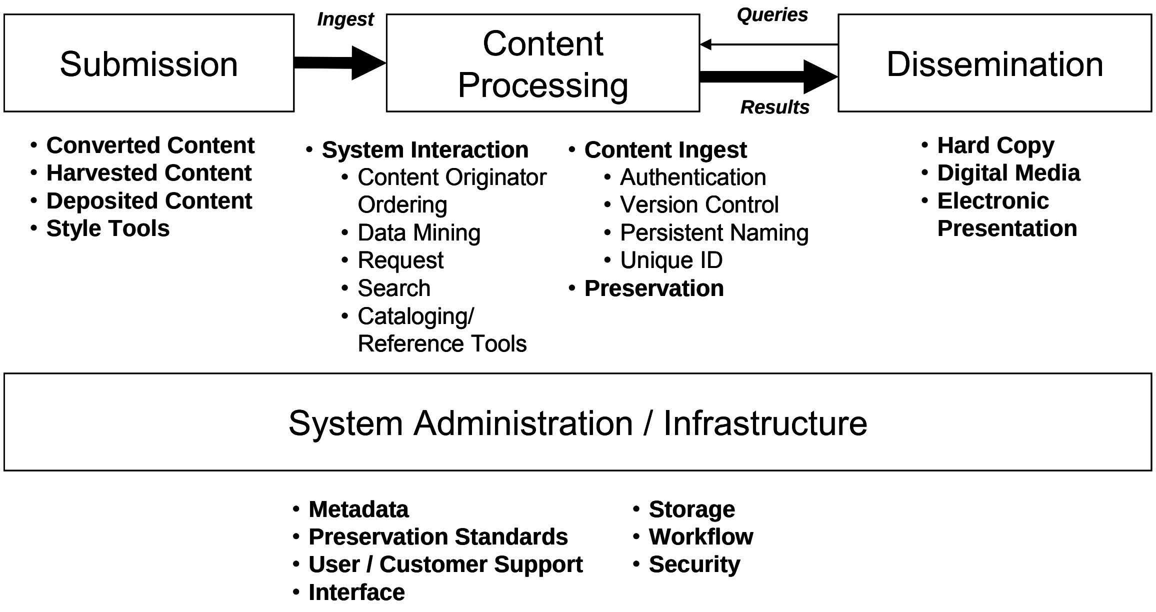


Figure 1 – Functional Reference Model

2.1 System Context

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

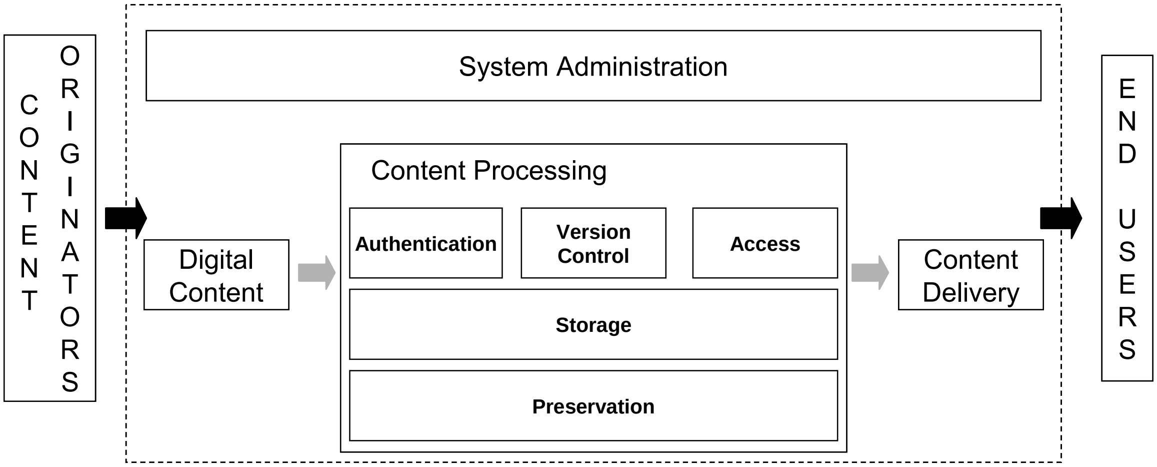


Figure 2 – System Architecture – User Context

2.1.1 Proposed System Attributes

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

- *Infrastructure independence*: Preserves content independent of any specific hardware and software;
- *Modularity*: Uses plug-in components that can be replaced with minimal impact to remaining components as workload and technology change;
- Policy neutrality: Accommodates 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;
- *Scalability*: Accommodates growth and manages differing sizes of repositories and ever increasing volumes of content;
- *Extensibility*: Handles additional kinds of content over time, not limited to specific types that exist today;
- *Comprehensiveness*: Provides support for content management lifecycle processes for all types of content; and
- *Flexibility*: Enables GPO to implement progressive improvements in its business processes over time and to tailor content-based services to suit customer needs.

2.1.2 Proposed System Capabilities

GPO has adopted the use of the OAIS reference model for an archival system that is dedicated to preserving and maintaining access to digital information.

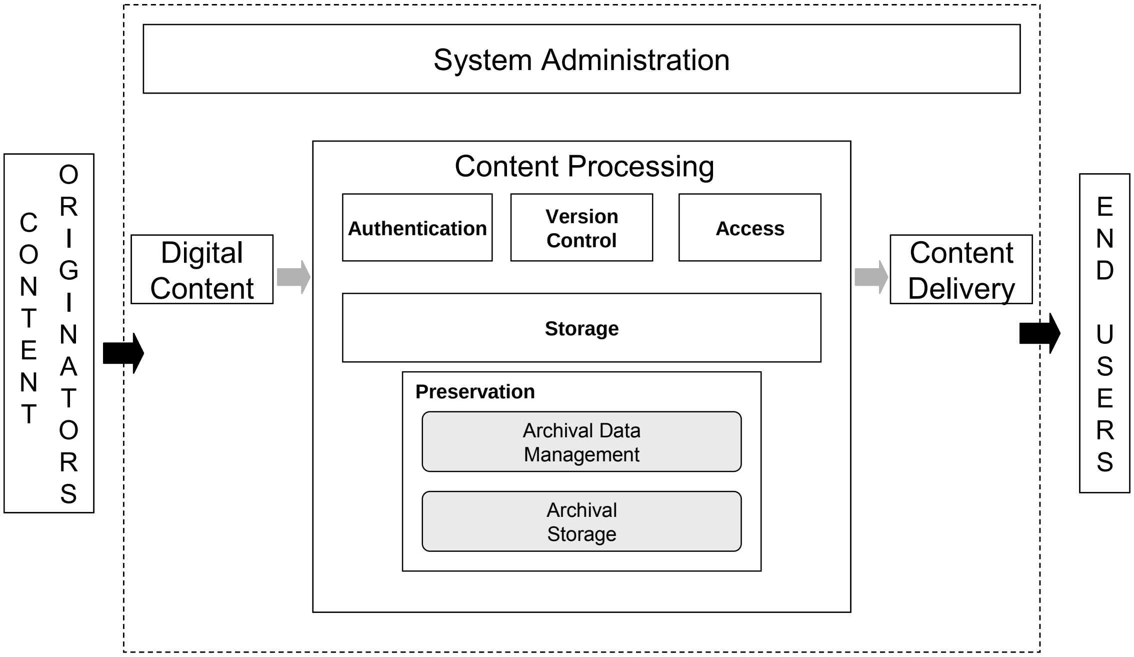


Figure 3 – Functional Reference Model, which is an adaptation of the OAIS reference model.

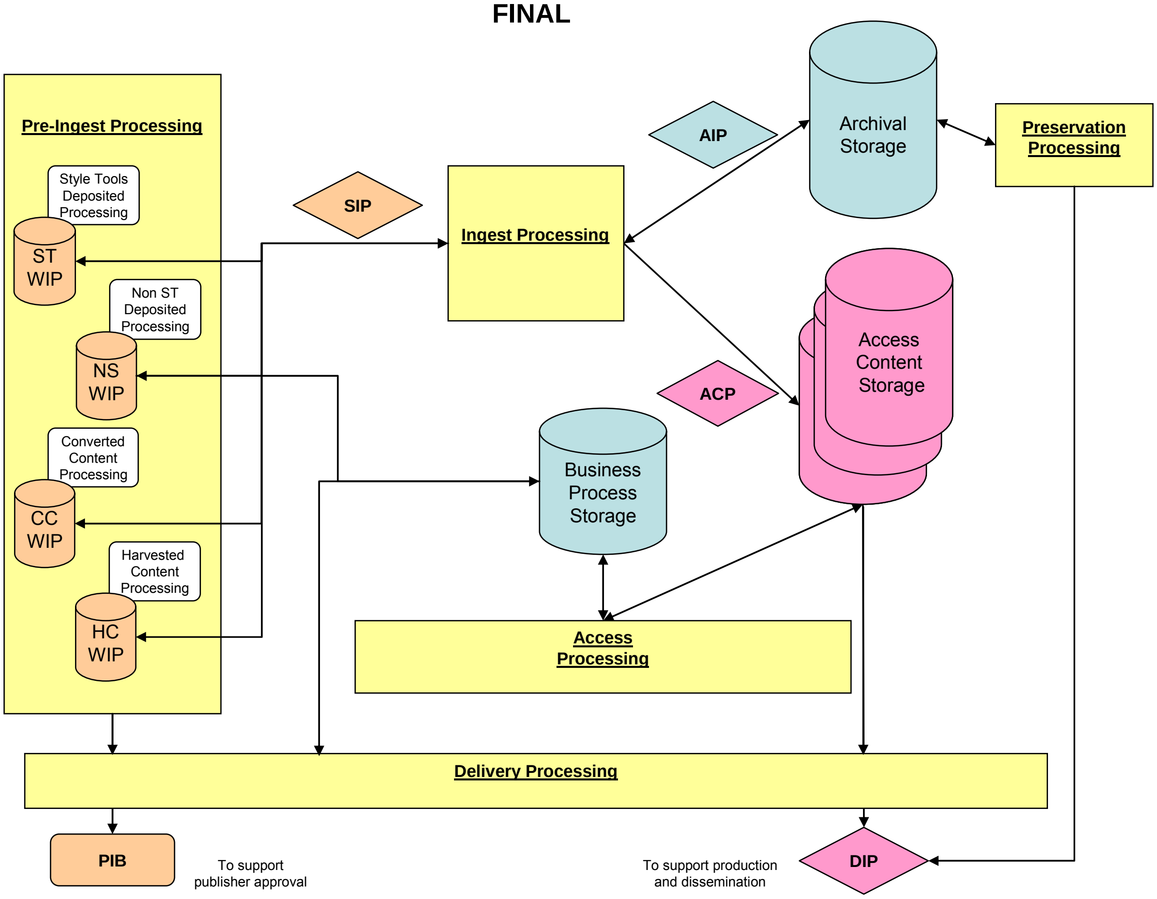


Figure 4 – Content Packages, Processing, and Storage

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

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

- Identify the essential characteristics of the content that is being preserved for the purposes of authentication and certification.

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

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

2.2 Major System Conditions

A list of general high-level Conditions:

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

2.3 Major System Constraints

A list of general high-level Constraints follows:

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

2.4 User Characteristics

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

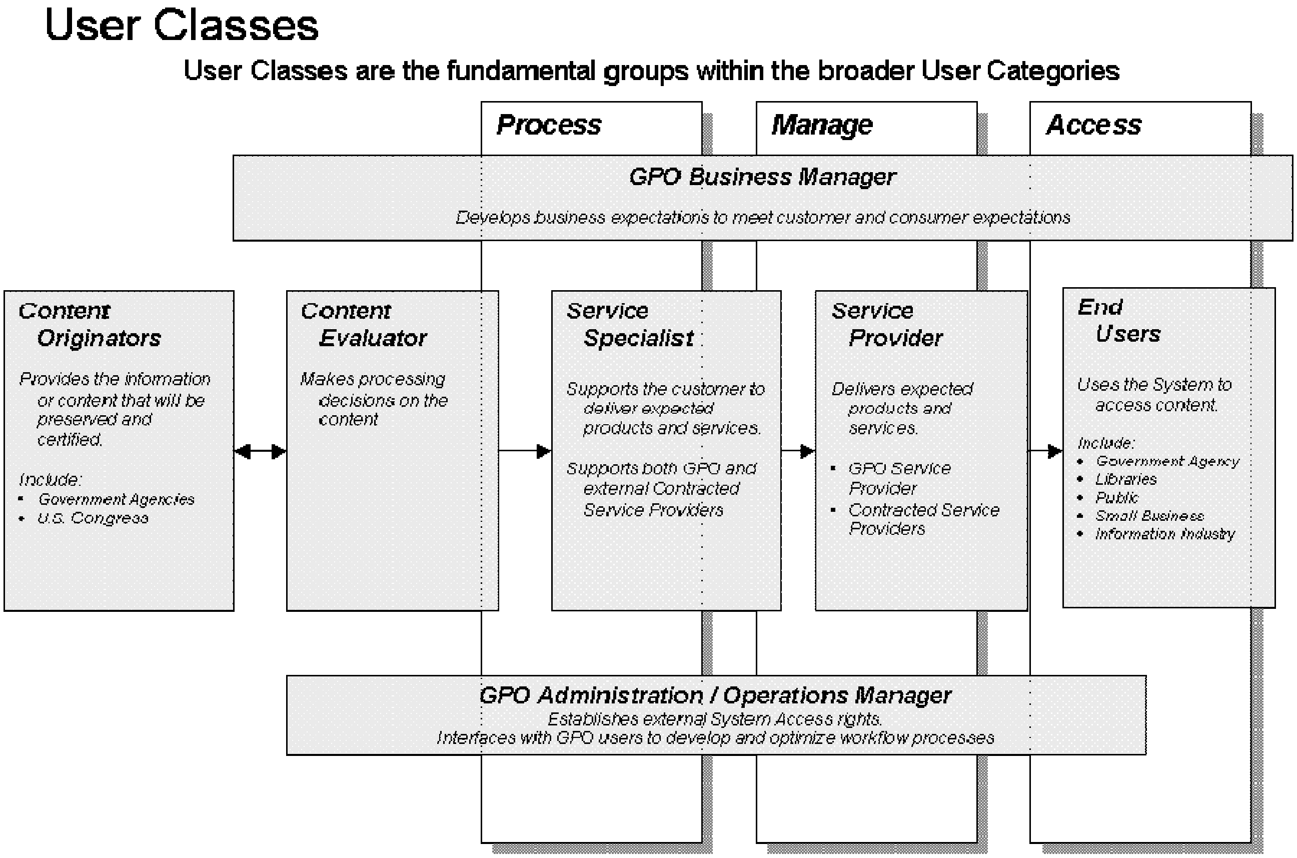

User Classes
User Classes are the fundamental groups within the broader User Categories
Process
Manage
Access
GPO Business Manager
Develops business expectations to meet customer and consumer expectations
Content Originators
Provides the information or content that will be preserved and certified.
Include: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

Figure 5 – User Classes

The major user classes identified for the system include

- Content Originator – Develops information and content and generates requests for GPO services. The Content Originator works with the Content Evaluator to define the parameters of the Preservation and Dissemination Plan. Content Originators provide the content that will be transferred to the system for subsequent certification and preservation.
- Content Evaluator – Collaborates with the Content Originator to determine if the content is within scope for GPO Dissemination Programs. The Content Evaluator establishes/defines the Preservation and Dissemination Plan and determines/makes decisions on what processing will occur, whether to use

internal production or external contracting, and whether to include information in the Sales Program and/or FDLP.

- Service Specialist – Supports the customer by performing contracting, administrative, and content management functions (e.g., creative services, contract writing and awarding, vendor certification, quality control, cataloguing and indexing, preservation management, dispute resolution.)
- Service Provider – Delivers expected services and products after receiving contract award (e.g., orders for hard copy output, design services, scanning).
- Business Manager – Develops business plans to meet Content Originator and End User expectations. Also works with GPO Sales Group to repurpose content in order to provide value added services.
- Systems Administration/Operations Manager – Supports the overall operations and integrity of the system and its use and conducts such system activities as managing user access rights, monitoring system performance, and scheduling reports. The Operations Manager interfaces with GPO personnel and makes decisions, including approval of workflow processes. The Operations Manager reviews system recommendations and makes decisions on when and how lifecycle activities related to specific records occur and who will perform the work. The Operations Manager has ultimate responsibility for the completion of tasks and the quality of the products.
- End User – Uses the system to search for and access records, submit content requests, request assistance via mediated searches, communicate with GPO, and invoke system services.

2.5 *Operational Scenarios*

Please reference FDsys RD v1.0.

3.0 Requirements

3.1 *Assumptions*

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

- GPO's dissemination and preservation activities will be based on a collection of content.
- GPO must actively capture content for that collection; all content can/will not be pushed to GPO.
- Selection for that collection can be automated.
- GPO must evolve into the role of publisher in addition to the traditional role of service provider.
- Repurposing of content for specific markets is a logical and beneficial business opportunity for GPO.
- The volume of traditional print work will continue to decline.
- Tangible digital media (e.g. CDs, DVDs) will continue to be used as a delivery channel
- Content will be delivered in a greater variety of forms, and will be discoverable at a wider variety of levels of granularity.

3.2 *Requirements List*

The requirements listed in this section are the result of a thorough analysis of the ideas proposed in the *Future Digital System ConOps.* The requirements are organized into the six solution clusters (Content Access, Content Delivery, Content Preservation, Content Processing, Content Submission, and Infrastructure) which were presented at GPO's October 2005 Industry Day, plus overall system requirements, Content Package descriptions, and Metadata. This RD should be reviewed together with the *ConOps* Section 5.3: Description of Proposed System for a complete understanding of the proposed system.

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

Each requirement is identified by the Release in which we anticipate its implementation (Release 1A, 1B, 1C, 2, and 3). Each requirement also features the attribute of Criticality.

- 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.

3.2.1 System, General

System, General provides core capabilities inherent to all areas of the system in order to ensure interoperability. The system will use open standards to ensure interoperability into the future. The system will be infrastructure independent, modular, policy neutral, scalable, extensible, comprehensive and flexible.

3.2.1.1 Current Situation

Under legal authority of Title 44, Chapters 17, 19, and 41 of the United States Code, GPO's Office of Information Dissemination (Superintendent of Documents) administers various dissemination programs with the mission of providing permanent public access to official Federal Government information. These include the Federal Depository Library Program (FDLP), GPO Sales Program, and GPO Access public Web site. The FDLP distributes electronic and tangible publications to a network of Federal Depository libraries across the country. Electronic versions of many, but not all, publications are delivered to the public via GPO Access in PDF, ASCII text, and HTML file formats. These formats are manually converted from the files supplied to GPO for printing.

Agencies currently submit content to GPO via digital media, camera copy, or film. There is not a system in place for GPO to electronically deliver this content to Service Providers.

GPO and external Service Providers regularly deliver hard copy publications and removable digital media to agency customers, libraries participating in the FDLP and end user requests from the GPO Sales Program. Many agency customers also request digital files that they can place online for viewing and/or download from GPO, and GPO's affiliated external Service Providers. Few files are currently supplied to GPO for strictly digital output.

GPO's current environment consists of legacy systems and manual operations to support GPO's operations. These are incapable of providing the breadth and depth of functionality that the proposed system will provide. Currently no single system or group of systems exists that will provide the capabilities envisioned for the proposed system.

GPO's implementation of new products and services has been conducted in an ad-hoc manner, which has resulted in the development of disparate systems. These systems do not interface on a common platform and are written in a number of different programming languages.

3.2.1.2 Requirements for System, General

1.2.1 The system shall provide for the use of internal and external open interfaces. (Release 1A; Must)

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.

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 1A; Must)

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 1A; Must)

1.2.4 The system shall accommodate changes in hardware, software, communication technology, processes, policy, personnel, locations, etc. without requiring major re-engineering or design changes. (Release 1A; Must)

1.2.5 The system shall be capable of accommodating growth and managing differing sizes of repositories and ever increasing volumes of content. (Release 1A; Must)

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 1A; Must)

1.2.7 The system shall provide support for content management lifecycle processes for all types of content. (Release 1A; Must)

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 1A; Must)

1.2.9 The system shall have the ability to transform content and metadata into packages that are compliant with open standards, including but not limited to XML. (Release 1A; Must)

1.2.10 The system shall be available for use at all GPO locations. (Release 1A; Must)

1.2.11 The system shall have the capability to support 20,000 concurrent users. (Release 1A; Must)

1.2.12 The system shall have the capability to support an overall sustained weekly average uptime greater than or equal to 99.0%. (Release 1A; Must)

1.2.12.1 The system shall have the capability to support a sustained weekly average uptime for peak periods greater than or equal to 99.7%. Peak time periods include all times with the exception of midnight to 6 am Eastern Time on Saturday and midnight to 6 am on Sunday. (Release 1A; Must)

1.2.12.2 The system shall have the capability to support uptime for off-peak time periods greater than or equal to 90%. Off-peak times may be changed as needed to provide Congress the appropriate level of service. (Release 1A; Must)

1.2.13 The system shall have the capability to have a response time to deliver digital services on a sustained weekly average of less than 2 Seconds. (Release 1A; Must)

3.2.2 Content Metadata

Actions or processes in the Future Digital System require and/or create information about target content. This information is recorded, stored, and subsequently used as content metadata. Content metadata is a structured representation of information that facilitates interpretation, management, and location by describing essential attributes and significant properties of content. Generally, content metadata describes how, when, and by whom a particular content package was collected, what the content is, where it resides, and how it is formatted.

Content metadata creates a systematic approach to expressing information derived or discerned from the content itself or from processes associated with the content. It encompasses static properties (e.g., those related to the specific instance or version of the content being processed, queried, or preserved) as well as the temporal aspects of the lifecycle of the object, a continuum extending from creation through system ingest, preservation, content processing, access, and use.

Content metadata is generally classified in the following broad categories, according to its function:

- Descriptive - such as bibliographic information describing, classifying, and characterizing the identity and context of the content.
- Administrative - describing rights, source, ownership, provenance, conditions of use and business rules.
- Technical - describing file format, computer environment, functionality, etc., in which the content was created or acquired and the attributes of the technical environment necessary to render the content meaningfully.
- Structural - describing interrelationships and hierarchies of files and content.
- Preservation - information necessary to maintain viability (the bit stream is intact and readable), renderability (translation of the bit stream into a form useable by humans), and understandability (the rendered content can be interpreted and understood by the intended user). Preservation metadata draws heavily on the other four categories. Metadata in FDsys must record essential properties and attributes which can be mapped to the major elements in the FDsys metadata model, which is broadly adapted from the OAIS metadata model.

GPO will adopt the most current version of the Metadata Encoding and Transmission Standard (METS) as the encoding standard for content packages in the system.

It is important to make the distinction that these requirements will describe content metadata and how it will behave within the system. The following requirements will not address the use of Business Process Information and system metadata. These metadata types are described in the glossary and in other appropriate parts of the Requirements Document.

3.2.2.1 Current Situation

GPO currently employs content metadata mainly to support cataloging, dissemination, and permanent public access. Machine Readable Cataloging (MARC) is used as the standard for all cataloging records created for the Federal Depository Library Program and the Cataloging and Indexing Program. Dublin Core is also used in metadata fields in the header code of high-level HTML pages on GPO Access.

3.2.2.2 Requirements for Content Metadata

2.2.1 Content Metadata Core Capabilities

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 1A; Must)

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 1A; Must)

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 1A; Must)

2.2.1.4 The system shall employ interoperable programming interfaces which are compliant with open standards, including, but not limited to, Extensible Markup Language (XML). (Release 1A; Must)

2.2.1.5 The system must provide the capability to link content metadata with system metadata. (Release 1A; Must)

2.2.1.6 The system must provide the capability to link content metadata with business process information. (Release 1A; Must)

2.2.2 Content Metadata Types

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 1A; Must)

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 1A; Must)

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 1A; Must)

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 1A; Must)

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 1A; Must)

2.2.2.3.2.1 Publication-specific metadata (e.g., Federal Register, Code of Federal Regulations, United States Code, U.S. Reports)

2.2.2.3.2.2 Document-specific metadata (e.g., Congressional Bills, Congressional Reports, Congressional Documents, proposed rules, business cards, envelopes, agency strategic plans)

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 1A; Must)

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 1A; Must)

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 1A; Must)

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 1A; Must)

2.2.2.5 The system shall employ metadata which relates the context of a digital object and relationship to other objects. (Release 1A; Must)

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 1A; Must)

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 1A; Must)

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 1A; Must)

2.2.3 Content Metadata Schema

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 1A; Must)

2.2.3.2 In general, GPO shall refer to metadata schema rather than embed data elements in the METS wrapper. (Release 1A; Must)

2.2.3.3 Deleted in RD v2.1

2.2.3.4 The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including but not limited to:

2.2.3.4.1 Machine Readable Cataloging (MARC) (Release 1A; Must)

2.2.3.4.2 Metadata Object Description Schema (MODS) (Release 1A; Must)

2.2.3.4.3 Dublin Core (Release 1A; Must)

2.2.3.4.4 Encoded Archival Description (EAD) (Release 1C; Could)

2.2.3.4.5 Text Encoding Initiative (TEI) (Release 1A; Could)

2.2.3.4.6 Data Document Initiative (DDI) (Release 1C; Could)

2.2.3.4.7 Federal Geographic Data Committee (FGDC) (Release 1C; Could)

2.2.3.4.8 Premis (Release 1A; Must)

2.2.3.4.9 MPEG 21 (Release 1B; Should)

2.2.3.4.10 JPEG 2000 (Release 1B; Should)

2.2.3.4.11 ONIX (Release 1B; Must)

2.2.3.4.12 MIX (NISO Metadata for Images) (Release 1A; Must)

2.2.3.5 The system shall employ a registry of extension schema and input standards in use. (Release 1A; Must)

2.2.3.6 Authorized users shall have the capability to manage the registry of schema employed by the system. (Release 1A; Must)

2.2.3.7 The system shall have the capability to employ new schema and add them to the registry. (Release 1A; Must)

2.2.3.8 The system shall use the following criteria to determine what schema shall be included in the registry. (Release 1A; Must)

2.2.3.8.1 The schema must interact with METS.

2.2.3.8.2 The schema must map to specific function(s), content type, or content formats within the system.

2.2.3.8.3 The schema must be a recognized standard managed by a trusted and recognized authority (e.g., Library of Congress, W3C).

2.2.3.8.4 The schema must not conflict with other schema in use by the system.

2.2.3.9 The system shall be capable of using extension schema developed by GPO. (Release 1B; Must)

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 1A; Must)

2.2.4 Content Metadata Import and Export

2.2.4.1 The system shall have the capability to acquire existing metadata from sources external to the system. (Release 1A; Must)

2.2.4.2 The system shall have the ability to export metadata with or without associated content, including but not limited to: (Release 1B; Must)

2.2.4.2.1 The ability to export metadata one record at a time.

2.2.4.2.2 The ability to export metadata in batches.

2.2.4.3 The system shall have the ability to export metadata compliant with multiple standards including but not limited to: (Release 1B; Must)

- Open Archival Interfaces (OAI)
- MARC
- ONIX

2.2.5 Content Metadata Management

2.2.5.1 The system shall have the ability to manage metadata regardless of its source. (Release 1A; Must)

2.2.5.2 The system shall have the ability to create metadata meeting the requirements of multiple schema. (Release 1A; Must)

2.2.5.3 The system shall provide the capability for GPO to designate metadata elements as mandatory. (Release 1A; Must)

2.2.5.4 The system must provide the capability for content metadata and system metadata to interact (e.g., a time and date stamp of a content authentication process). (Release 1A; Must)

2.2.5.5 The system must provide the capability for content metadata and Business Process Information to interact. (Release 1A; Must)

2.2.5.6 The system shall log all additions, deletions, and changes to content metadata within the system. (Release 1A; Must)

3.2.3 CONTENT PACKAGES

3.2.3.1 Submission Information Packages (SIP)

This section specifies the packaging details for the Submission Information Package (SIP), and describes how digital content and its associated metadata are logically packaged for submission to FDsys.

A SIP contains the target digital object(s) and associated descriptive and administrative metadata. It will be the vehicle whereby content packages are submitted to FDsys by Content Originators. The concept of the SIP in the OAIS (Open Archival Information System) model provides a starting point for the specification of content and associated metadata, but it does not specify how it is packaged. It is necessary that a SIP follow pre-specified rules so that FDsys can validate and accept the content for ingest.

Associated with the SIP are three types of information:

- Content Information (digital object(s) and Representation Information),
- Packaging Information, and
- Descriptive Information.

Packaging Information is the information that binds or encapsulates the Content Information. To accomplish this, a SIP will include a binding metadata file (sip.xml) that relates the digital objects and metadata together to form a system-compliant SIP. The Metadata Encoding and Transmission Standard (METS) schema shall be adopted as the encoding standard for the sip.xml file, and GPO will specify profiles for METS to drive its implementation for FDsys.

Descriptive Information is the metadata that allows users to discover the Content Information in the system.

All file components of the SIP will be populated within a structured file system directory hierarchy and are then aggregated into a single file or entity for transmission and ingest into the system.

3.2.3.1.1 Current Situation

GPO currently receives content from agencies in a variety of formats, intended for a variety of output products. This diversity influences the treatment content receives in the course of processing by GPO. Content may be received by GPO in digital form, structured for hard or soft copy output, or in analog form from which digital files for printing are created by GPO staff. Digital inputs may range from structured files intended for producing hardcopy output or web presentations, to minimally structured ASCII text to be loaded into a searchable database. GPO's practice has been to accommodate agency requirements by not limiting input forms.

3.2.3.1.2 Requirements for SIP

3.1.2.1 SIP - Deposited Content

3.1.2.1.1 The SIP Deposited Object shall consist of digital object(s) associated with a document or publication, including at least one of the following categories of files: (Release 1A; Must)

- Native Files: original format in which the content was submitted
- Preservation Copy: fully faithful copy expressed in a format that is capable of being preserved (e.g., XML).
- Access Copies: copies of the content that are optimized for access and maintain acceptable presentation quality (e.g., screen-optimized, searchable, press/print-optimized PDF)

3.1.2.1.2 The metadata for deposited content in the SIP shall consist of fundamental representation information, any necessary DTD's (or schema), style sheets, and submission level metadata. (Release 1A; Must)

3.1.2.2 SIP - Harvested Content

3.1.2.2.1 The SIP Harvested Object shall consist of digital object(s) as harvested, including at least one of the following categories of files: (Release 1A; Must)

- Native Files: original format in which the content was harvested.
- Preservation Copy: fully faithful copy expressed in a format that is capable of being preserved (e.g., XML).
- Access Copies: copies of the content that are optimized for access and maintain acceptable presentation quality (e.g., screen-optimized, searchable, press/print-optimized PDF).

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. (Release 1A; Must)

3.1.2.3 SIP - Converted Content

3.1.2.3.1 The SIP Converted Object shall consist of digital object(s) as obtained by scanning or other method, including at least one of the following categories of files: (Release 1A; Must)

- Native Files: original format in which the content was created (e.g., TIFF).
- Preservation Copy: fully faithful copy expressed in a format that is capable of being preserved (e.g., XML).
- Access Copies: copies of the content that are optimized for access and maintain acceptable presentation quality (e.g., screen-optimized, searchable, press/print-optimized PDF).

3.1.2.3.2 The metadata for converted content in the SIP shall refer to full technical information on the conversion, using NISO Z 39.87-2002 as a guideline, in addition to submission level metadata. (Release 1A; Must)

3.1.2.4 Core SIP Requirements

3.1.2.4.1 A SIP shall contain one content unit (e.g., publication) that may consist of one or more digital objects. (Release 1A; Must)

3.1.2.4.2 A SIP shall contain a binding METS file, named **sip.xml**, which describes the SIP as a whole and the relationships between digital objects and metadata. (Release 1A; Must)

3.1.2.4.3 A SIP shall contain one or more metadata files associated with the content. (Release 1A; Must)

3.1.2.4.4 All metadata files shall be encoded in XML and conform to schema that are adopted by FDsys, according to the FDsys metadata requirements. (Release 1A; Must)

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 1A; Must)

3.1.2.5 Requirements for sip.xml File

3.1.2.5.1 The sip.xml file shall conform to the most current version of the METS schema. (Release 1A; Must)

3.1.2.5.2 The sip.xml shall conform to the most current GPO profile for METS schema. (Release 1A; Must)

3.1.2.5.3 In general, digital objects shall be referred to, but not directly embedded in, the sip.xml file. (Release 1A; Must)

3.1.2.5.4 In general, metadata files shall be referred to, but not directly embedded in, the sip.xml file. (Release 1A; Must)

3.1.2.5.5 A metadata file must be associated with one or more digital objects in the sip.xml file. (Release 1A; Must)

3.1.2.6 Structural Layout for SIPs

3.1.2.6.1 The SIP shall contain the **sip.xml** file and two directories at the top level of the structure layout. The two top directories should be named as **content** and **metadata**. (Release 1A; Must)

3.1.2.6.2 All digital objects for the content of a SIP shall be placed in the content directory. (Release 1A; Must)

3.1.2.6.2.1 The content directory shall contain one or more sub-directories that will reflect the category of content included in the SIP.

3.1.2.6.3 All metadata files shall be placed in the metadata directory. (Release 1A; Must)

3.1.2.6.3.1 The metadata directory shall contain one or more sub-directories that will reflect the metadata included in the SIP.

3.1.2.6.4 Each content category file shall have one corresponding metadata file expressed in the Metadata Object Description Schema (MODS) that includes descriptive metadata about that content. (Release 1A; Must)

3.1.2.6.5 Each content category file shall have one or more corresponding metadata files that comply with an extension schema and that include administrative metadata appropriate to the class of object. (Release 1A; Must).

3.1.2.7 Packaging of SIPs

3.1.2.7.1 All file components of the SIP shall be assembled into a structured file system directory hierarchy and then aggregated into a single file or entity for transmission and ingest into the system. (Release 1A; Must)

3.1.2.8 SIP Descriptive Metadata Requirements

3.1.2.8.1 For descriptive metadata elements, GPO shall employ Metadata Object Description Schema (MODS) records external to the binding METS file (sip.xml). (Release 1A; Must)

3.1.2.8.2 All MODS elements and sub-elements shall be considered valid in the SIP. (Release 1A; Must)

3.1.2.8.3 The following MODS descriptive metadata elements shall be considered mandatory and shall be present and valid in order for a SIP to be eligible for ingest: (Release 1A; Must)

- OriginInfo:publisher
- OriginInfo:dateIssued, Captured, Created, Modified, Valid, or Other
- Language
- Identifier
- Location
- PhysicalDescription:internetMediaType
- PhysicalDescription:digitalOrigin
- PhysicalDescription:extent
- TypeOfResource
- RecordInfo

3.1.2.9 SIP Administrative Metadata Requirements

3.1.2.9.1 The SIP shall include administrative metadata as needed, expressed in extension schema appropriate to the class of object, including but not limited to: (Release 1A; Must)

- Technical metadata (e.g., JPEG2000 for video, TEI for encoded text).
- Rights metadata
- Source metadata
- Provenance metadata

3.2.3.2 Archival Information Package (AIP)

Archival Information Packages (AIPs) are preservation copies of digital objects with associated technical, descriptive, and preservation metadata. AIPs will be stored in a secure environment and acted upon by FDsys preservation processes to enable permanent public access to the official version(s) of U.S. Government publications in digital formats.

This document specifies the packaging details for the Archival Information Package (AIP), and describes how digital content and its associated metadata are logically packaged. Associated with the AIP are four types of information:

- Content Information (digital object(s) and Representation Information),
- Preservation Description Information,
- Packaging Information, and
- Descriptive Information.

Preservation Description Information (PDI) is the information needed to accurately describe the Content Information and provide an understanding of the environment in which the Content Information was created. The PDI includes several types of additional information that are needed to help preserve the Content Information. These are:

- Reference: How users can uniquely identify the Content Information from any other Content Information.
- Provenance: Who has had custody of the Content Information and what was its source. This would include the processing that generated it.
- Technical environment
- Context: How the Content Information relates to other information objects, such as why it was created and how it may be used with other information objects.
- Fixity: Information and mechanisms used to protect the Content Information from accidental change.

Packaging Information is the information that binds or encapsulates the Content Information and Preservation Description Information for transmission between subsystems.

Descriptive Information is the metadata that allows users to discover the Content Information in the system.

An AIP is composed of target digital object(s) and metadata about the digital object(s), and a binding metadata file (aip.xml) that relates the digital objects and metadata together to form a system-compliant AIP. The Metadata Encoding and Transmission Standard (METS) schema shall be adopted as the encoding standard for the aip.xml file, and GPO will specify profiles for METS to drive its implementation for FDsys.

3.2.3.2.1 Current Situation

GPO presently has no integrated system for preservation or permanent storage of digital content. The content that is archived typically does not meet preservation standards for data structure or metadata; instead it usually consists of harvested access derivatives or text data bases.

Access copies of digital publications, typically in PDF, HTML, or ASCII format are stored on, and may be accessed from, several platforms. These include:

- GPO Access
- GPO’s archival server, http://www.permanent.access.gpo.gov
- OCLC’s digital archive
- Library partner sites, such as the University of North Texas’ *Cybercemetery*
- Agency partner sites, such as the Department of Energy’s *Information Bridge*

Routine backup of GPO-managed data is performed under contract by Iron Mountain.

The only preservation process currently in use is refreshment. There is no defined AIP in the current environment.

3.2.3.2.2 Requirements for AIP

3.2.2.1 AIP Core Capabilities

3.2.2.1.1 AIPs shall be capable of including the digital object(s) in its native format. (Release 1A; Must)

3.2.2.1.2 AIPs shall be capable of including the digital object(s) and corresponding XML version(s) including associated DTD, style sheet(s), and schema. (Release 1A; Must)

3.2.2.1.3 AIPs shall include the Representation Information for content. (Release 1A; Must)

3.2.2.1.4 The system shall support the creation of AIPs which are independent of any particular hardware and software component. (Release 1A; Must)

3.2.2.1.5 The system will provide the capability for authorized users to access AIPs for the purpose of executing preservation processes or dissemination of AIPs. (Release 1A; Must)

3.2.2.1.6 The AIP shall be expressed using METS. (Release 1A; Must)

3.2.2.1.7 The AIP shall contain a binding METS file, named aip.xml, which describes the AIP as a whole and the relationships between digital objects and metadata. (Release 1A; Must)

3.2.2.1.8 The AIP shall contain one or more metadata files associated with the content. (Release 1A; Must)

3.2.2.2 Requirements for aip.xml File

3.2.2.2.1 The aip.xml file shall conform to the most current version of the METS schema. (Release 1A; Must)

3.2.2.2.2 The aip.xml shall conform to the most current GPO profile for METS schema. (Release 1A; Must)

3.2.2.2.3 In general, digital objects shall be referred to, but not directly embedded in, the aip.xml file. (Release 1A; Must)

3.2.2.2.4 In general, metadata files shall be referred to, but not directly embedded in, the aip.xml file. (Release 1A; Must)

3.2.2.2.5 A metadata file must be associated with one or more digital objects inside the aip.xml file. (Release 1A; Must)

3.2.2.3 Structural Layout for AIPs

3.2.2.3.1 The AIP shall contain the **aip.xml** file and two directories at the top level of the structure layout. The two top directories should be named as **content** and **metadata**. (Release 1A; Must)

3.2.2.3.2 All digital objects for the content of an AIP shall be placed in the content directory. (Release 1A; Must)

3.2.2.3.2.1 The content directory shall contain one or more sub-directories that will reflect the category of content included in the AIP.

3.2.2.3.3 All metadata files shall be placed in the metadata directory. (Release 1A; Must)

3.2.2.3.3.1 The metadata directory shall contain one or more sub-directories that will reflect the metadata included in the AIP.

3.2.2.3.4 Each content category file shall have one corresponding metadata file expressed in the Metadata Object Description Schema (MODS) that includes descriptive metadata about that content. (Release 1A; Must)

3.2.2.3.5 Each content category file shall have one corresponding metadata file that complies with an extension schema that includes administrative metadata about that content. (Release 1A; Must)

3.2.2.4 AIP Metadata

3.2.2.4.1 All metadata files shall be encoded in XML and conform to schema that are adopted by FDsys, according to the FDsys metadata requirements. (Release 1A; Must)

3.2.2.4.2 The AIP shall include PDI that identifies the essential attributes of the content that is being preserved so it can be rendered usably and understandably. (Release 1A; Must)

3.2.2.4.3 The AIP shall include preservation metadata to record preservation processes, from ingest into the repository through disposal. (Release 1A; Must)

3.2.2.4.4 The AIP shall refer to extension schema for descriptive metadata, including, but not limited to, MODS and MARC. (Release 1A; Must)

3.2.2.4.4.1 The AIP shall incorporate the mandatory descriptive metadata elements from the SIP.

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 1A; Must)

3.2.2.4.6 The AIP shall include administrative metadata as needed, expressed in extension schema appropriate to the class of object, including but not limited to: (Release 1A; Must)

- Technical metadata
- Rights metadata
- Source metadata
- Provenance metadata

3.2.2.5 AIP Unique ID

3.2.2.5.1 The AIP shall include the unique identification number assigned to the content in the SIP. Release 1A; Must)

3.2.2.5.1.1 The system shall have the capability to assign a unique identification number to any new AIP resulting from preservation processes. (Release 1C; Must)

3.2.3.3 Access Content Package (ACP)

Access Content Packages (ACPs) are internal system copies of digital objects with associated content metadata to support access and delivery. The ACP may include access copies, native tiles, and optimized copies of content (e.g. XML) to facilitate and optimize access and delivery to End Users. As necessary, ACPs should follow the concept of a content package as outlined in the OAIS (Open Archival Information System) model, but more importantly, ACPs should address GPO's business needs including the following:

- Provide timely and efficient access to official Federal Government information through search, cataloging, and reference tools.

- Deliver content and metadata in a way that meets Content Originator and End User expectations for structure, format, and presentation as specified through Content Originator ordering and End User request.

The ACP is created as part of ingest processing and may be modified a part of preservation processing and access processing. ACPs will be stored in high availability / high access storage (ACS), as necessary, to enable timely search and retrieval. The system must have the capability to send ACPs to delivery processing for creation of DIPs that are then delivered to users.

The ACP consists of digital objects and content metadata about the digital objects, including descriptive information to facilitate access. The ACP may also include a binding metadata file that relates the digital objects and content metadata together to form a package. The Metadata Encoding and Transmission Standard (METS) schema has been adopted for the SIP and AIP and may be used as the encoding standard for the binding metadata file, if a binding metadata file is required by the system.

3.2.3.3.1 Current Situation

GPO provides access to electronic content on GPO Access in HTML, minimally structured ASCII text, and PDF formats. Most content on GPO Access has been indexed into the legacy Wide Area Information Server (WAIS) application. GPO provides access to content that is in scope for the Federal Depository Library Program through an Online Public Access Catalog (OPAC) that is part of GPO's integrated library system (ILS). In addition, access copies of digital publications are also stored on GPO's archival server <http://permanent.access.gpo.gov>, OCLC's digital archive, agency partner sites, and library partner sites.

3.2.3.3.2 Requirements for ACP

3.3.2.1 ACP Core Capabilities

3.3.2.1.1 The ACP shall have the capability to include digital objects associated with a document or publication, from one or more of the following: (Release 1B; Must)

- Access copies of digital objects: copies of the content that are optimized for access and maintain presentation quality that is acceptable to GPO and/or Content Originators (e.g., screen, print, or press optimized PDF; ASCII text; HTML).
- Optimized copies of digital objects: fully faithful copies of the content that are expressed in a format which includes structural and descriptive metadata (e.g., XML) including associated DTD, style sheets, and schema for the purpose of timely and efficient search, retrieval, and delivery.
- Native Files: copies of the content in the original format in which the content was created or submitted (e.g., TIFF, Microsoft Office formats, Adobe InDesign formats, QuarkXPress formats, HTML).

3.3.2.1.2 The ACP shall have the capability to include the following: (Release 1B; Must)

3.3.2.1.2.1 Ephemera (e.g., letterhead, envelopes, business cards).

3.3.2.1.2.2 Derivatives not included in the AIP but created from the AIP.

3.3.2.1.2.3 Derivatives created from access copies, native files, or optimized copies.

3.3.2.1.2.4 Derivatives created from derivatives (e.g., thumbnail images).

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 1B; Must)

3.3.2.1.4 The ACP shall have the capability to include all digital objects included in its corresponding AIP. (Release 1B; Must)

3.3.2.1.5 The ACP metadata shall have the capability to include descriptive, structural, technical, administrative, and packaging metadata for access, content transformation, content management, content processing, derivation, and delivery. (Release 1B; Must)

3.3.2.1.6 The ACP shall have a structural layout that facilitates access and delivery. (Release 1B; Must)

3.3.2.1.7 The ACP shall have the capability to replicate the structural layout of an AIP. (Release 1B; Could)

3.3.2.1.8 The system shall have the capability to package ACPs in such a way to facilitate access and delivery. (Release 1B; Must)

3.3.2.1.9 The ACP shall have the capability to refer to or embed one or more metadata files associated with the content. (Release 1B; Must)

3.3.2.1.10 The ACP shall have the capability to refer to or embed one or more digital objects associated with metadata. (Release 1B; Must)

3.3.2.1.11 The ACP shall have the capability to include all metadata files included in its corresponding AIP. (Release 1B; Must)

3.3.2.2 ACP Binding Metadata File

3.3.2.2.1 If required by the system, the ACP shall have the capability to employ a binding metadata file which describes the ACP as a whole and the relationships between digital objects and content metadata to support access and delivery. (Release 1B; Could)

3.3.2.2.1.1 If required by the system, the binding metadata file shall conform at a minimum to the most current version of the METS schema to support access and delivery.

3.3.2.2.1.2 The system must provide the capability to embed or refer to digital objects (e.g., XML, OCR-ed text) as required to support access and delivery.

3.3.2.2.1.3 The system must provide the capability to embed or refer to metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support access and delivery.

3.3.2.2.1.4 The system must provide the capability to associate metadata files with one or more digital objects in the ACP.

3.3.2.3 ACP Metadata

3.3.2.3.1 The system shall have the capability to encode metadata files in XML and conform to schema adopted by FDsys, according to FDsys Content Metadata requirements. (Release 1B; Must)

3.3.2.3.2 The ACP shall have the capability to embed or refer to metadata for access and delivery. (Release 1B; Must)

3.3.2.3.3 The system must provide the capability to add structural and descriptive metadata for digital objects at a level of granularity that facilitates access to content at speeds that are at or above current industry standards for search and retrieval. (Release 1B; Must)

3.3.2.3.4 The system must provide the capability to add structural and descriptive content metadata for digital objects at the specified level of granularity. (Release 1B; Must)

3.3.2.3.5 The ACP shall have the capability to use extension schema for descriptive metadata for access, including, but not limited to the following: (Release 1B; Must)

- MODS
- MARC
- ONIX
- Dublin Core
- Premis

3.3.2.3.6 The ACP shall have the capability to include mandatory descriptive metadata elements from the AIP and SIP. (Release 1B; Must)

3.3.2.3.7 The ACP shall have the capability to embed or refer to extension schema for additional structural metadata as appropriate to the class of object and as necessary for access and delivery. (Release 1B; Must)

3.3.2.3.8 The ACP shall have the capability to embed or refer to extension schema for administrative metadata as appropriate to the class of object and as necessary for access and delivery, including but not limited to the following: (Release 1B; Must)

- Technical metadata
- Rights metadata

- Source metadata
- Provenance metadata

3.3.2.3.9 The ACP shall have the capability to embed or refer to extension schema for other metadata as appropriate to the class of object and as necessary for access and delivery, including but not limited to the following: (Release 1B; Must)

- Publication-specific metadata (e.g., Federal Register, Code of Federal Regulations, United States Code, U.S. Reports)
- Document-specific metadata (e.g., Congressional bill, Congressional report, Congressional document, proposed rule, business card, envelop, agency strategic plan)
- Business process information
- System metadata

3.3.2.3.10 The ACP must have the capability to include the unique ID assigned to the SIP and AIP in metadata. (Release 1B; Must)

3.2.3.4 Dissemination Information Package (DIP)

Dissemination Information Packages (DIPs) are transient copies of digital objects, associated content metadata, and business process information that are delivered from the system to fulfill End User requests and Content Originator orders. As necessary, DIPs should follow the concept of a DIP as outlined in the OAIS (Open Archival Information System) model.

The DIP is created as part of delivery processing and digital objects may be adjusted based on orders and requests to support the delivery of hard copy output, electronic presentation, and digital media.

The DIP should include all digital objects and/or metadata necessary to fulfill requests and orders. The DIP may also include a binding metadata file that relates the digital objects and metadata together to form a package. The Metadata Encoding and Transmission Standard (METS) schema has been adopted for the SIP and AIP and may be used as the encoding standard for the binding metadata file, if a binding metadata file is created.

3.2.3.4.1 Current Situation

GPO disseminates official Federal Government information in print and electronic formats from all three branches of the Federal Government. Electronic versions of many, but not all, publications are delivered to the public via GPO Access in PDF, ASCII text, and HTML, and are usually by-products of GPO's printing processes.

3.2.3.4.2 Requirements for DIP

3.4.2.1 DIP Core Capabilities

3.4.2.1.1 The DIP shall have the capability to include digital objects, associated content metadata, and business process information to fulfill End User requests and Content Originator orders. (Release 1B; Must)

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)

3.4.2.1.3 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)

3.4.2.1.4 The DIP shall have the capability to refer to or embed one or more metadata files associated with the content. (Release 1B; Must)

3.4.2.1.5 The DIP shall have the capability to refer to or embed one or more digital objects associated with metadata. (Release 1B; Must)

3.4.2.1.6 The system must provide the capability to delivery DIPs that only include content metadata. (Release 1B; Must)

3.4.2.1.7 The DIP shall have the capability to be an exact replica of the AIP. (Release 1B; Must)

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)

3.4.2.1.9 The DIP shall have a structural layout that facilitates delivery. (Release 1B; Must)

3.4.2.1.10 The system shall have the capability to package DIPs in such a way to facilitate delivery. (Release 1B; Must)

3.4.2.2 DIP Binding Metadata File

3.4.2.2.1 If required by the system, the DIP shall have the capability to employ a binding metadata file which describes the DIP as a whole and the relationships between digital objects and content metadata to support delivery. (Release 1B; Could)

3.4.2.2.1.1 If required by the system, the binding metadata file shall conform at a minimum to the most current version of the METS schema to support delivery.

3.4.2.2.1.2 The system must provide the capability to embed or refer to digital objects (e.g., XML, OCR-ed text) as required to support delivery.

3.4.2.2.1.3 The system must provide the capability to embed or refer to metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support delivery.

3.4.2.2.1.4 The system must provide the capability to associate content metadata files with one or more digital objects in the DIP.

3.4.2.3 DIP Metadata

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)

3.4.2.3.2 The DIP shall have the capability to embed or reference metadata for delivery. (Release 1B; Must)

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)

3.4.2.3.4 The DIP shall have the capability to use extension schema for descriptive metadata for delivery, including, but not limited to the following: (Release 1B; Must)

- MODS
- MARC
- ONIX
- Dublin Core
- Premis

3.4.2.3.5 The DIP shall have the capability to embed or refer to extension schema for additional structural metadata as appropriate to the class of object and as required for delivery. (Release 1B; Must)

3.4.2.3.6 The DIP shall have the capability to embed or refer to extension schema for administrative metadata as appropriate to the class of object and as required for delivery, including but not limited to the following: (Release 1B; Must)

- Technical metadata
- Rights metadata
- Source metadata
- Provenance metadata

3.4.2.3.7 The DIP shall have the capability to embed or refer to extension schema for other metadata as appropriate to the class of object and as required for delivery, including but not limited to the following: (Release 1B; Must)

- Business process information
- System metadata

3.4.2.3.8 The system must provide the capability to include information generated as a result of Content Originator ordering. (Release 1C; Must)

3.4.2.3.9 The system must provide the capability to include information generated as a result of an End User request. (Release 1B; Must)

3.4.2.3.10 The DIP must have the capability to include the unique ID assigned to the SIP, ACP, and AIP in metadata. (Release 1B; Must)

3.4.2.3.11 The system shall have the capability to support the Open Archives Initiative Protocol. (Release 1B; Must)

3.2.4 CONTENT PROCESSING

FDsys content processing identifies the processes that must be managed for functions to identify, manage, and verify digital content as it moves through the system, from creation to dissemination and archiving. Content processing consists of pre-ingest processing, ingest processing, access processing, preservation processing and delivery processing.

Pre-ingest processing prepares content for ingest into the system. During pre-ingest processing, the system shall execute and manage the following functions:

- Version control processes
- Content Originator ordering processes
- Assign unique IDs to content
- Assign unique IDs to system jobs
- Scope assessment processes, per the Information Dissemination Scope Determination policy.
- Integrity checking processes on content
- Accessibility assessment processes
- Accept content submitted from deposited processing, Content Originator ordering, style tools, conversion processes and harvesting.

Ingest processing compares submitted content to established criteria, and either accept the content and create initial Access Content Packages and Archival Information Packages or reject it. During ingest processing, the system shall execute and manage the following functions:

- Accept and validate SIPs
- Create AIPs from SIPs
- Create initial ACPs from SIPs
- Apply digital time stamping to content

Access processing facilitates the finding, analyzing, ordering, and retrieving content and content metadata. During access processing, the system shall execute and manage the following functions:

- Manage ACPs
- Cataloging and reference tools processes
- Assign persistent names to content packages

Delivery processing facilitates the transfer from the stored form of a digital object in a repository to a user. During delivery processing, the system shall execute and manage the following functions:

- Create DIPs for service providers and end users.
- Create pre-ingest bundles (PIBs) from content in pre-ingest WIP to support the publisher approval process (e.g., proofing).
- Apply accessibility processes to create DIPs compliant with GPO accessibility policies.
- Apply integrity marks to DIPs to create packages compliant with GPO authentication policies.

Preservation processing facilitates the maintenance of publications for use, either in their original form or in some verifiable, usable form. During preservation processing, the system shall execute and manage the following functions:

- Manage AIPs through refreshment, migration, and emulation.
- Manage ACPs.
- Create DIPs from AIPs.

For a visual of content processing, please see Figure 4 - Content Packages, Processing, and Storage in section *2.1.2 Proposed System Capabilities*.

3.2.4.1 Pre-ingest Processing

FDsys pre-ingest processing includes the processes necessary for functions to identify, manage, and verify digital content as it moves into the system.

Pre-Ingest processing manages the functions that prepare content for ingest into the system. Content Originators and Service Specialists have the capability to submit content to WIP storage. Content can be submitted from deposited processing, Content Originator ordering, style tools, conversion processes and harvesting. The system will assign unique identifiers, identify versions, detect duplicate content, and allow for publisher approval processes. Pre-ingest processing performs the following functions:

- Version control processes
- Content Originator ordering functions
- Assign unique IDs to content
- Assign unique IDs to system jobs
- Scope assessment processes, per the Information Dissemination Scope Determination policy.
- Integrity checking processes on content
- Accessibility assessment processes
- Style tool, non-style tool, converted content, harvested content processing to create a SIP
- Publisher approval processes (i.e., proofing) to move content to ingest processing.

3.2.4.1.1 Requirements for Pre-ingest Processing

4.1.1.1 Pre-ingest Processing

4.1.1.1.1 The system shall accept content from Content Originators. (Release 1A; Must)

4.1.1.1.2 The system shall accept jobs from Content Originator ordering. (Release 1C; Must)

4.1.1.1.3 The system shall accept deposited content without style tools. (Release 1A; Must)

4.1.1.1.4 The system shall accept deposited content from style tools. (Release 1C; Could / Release 2; Must)

4.1.1.1.5 The system shall accept converted content. (Release 1A; Must)

4.1.1.1.6 The system shall accept harvested content. (Release 1A; Must)

4.1.1.1.7 The system shall have the capability to apply version control. (Release 1A; Must)

4.1.1.1.8 The system shall detect duplicate content in the system and notify authorized users. (Release 1A; Must)

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)

4.1.1.1.8.2 The system shall have the capability to reject duplicate content.

4.1.1.1.9 The system shall have the capability to store content in WIP before job order information is received. (Release 1A; Must)

4.1.1.1.10 The system shall have the capability to assign a unique ID to content. (Release 1A; Must)

4.1.1.1.11 The system shall have the capability to assign a unique ID to jobs. (Release 1A; Must)

4.1.1.1.12 The system shall populate the Identifier field in the corresponding MODS record with the content unique ID. (Release 1A; Must)

4.1.1.1.13 The system shall link related jobs, business process information (BPI), and content through the content unique ID. (Release 1A; Must)

4.1.1.1.14 The system shall allow Content Evaluators to make scope determinations. (Release 1A; Must)

4.1.1.1.15 The system shall have the capability to perform integrity checking. (Release 1A; Must)

4.1.1.1.16 The system shall have the capability to apply a digital time stamp to content. (Release 1A; Must)

4.1.1.1.17 The system shall have the capability to perform accessibility assessments. (Release 1A; Must)

4.1.1.1.18 The system shall have the capability to support the creation of a pre-ingest bundle (PIB). (Release 1C; Must)

4.1.1.1.19 The system shall have the capability to accept modified DIPs from the Service Provider after publisher approval. (Release 1B; Must)

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)

4.1.1.1.21 The system shall accept publisher approval information for SIP creation. (Release 1A; Must)

4.1.1.1.22 The system shall have the capability to assemble content into SIPs. (Release 1A; Must)

4.1.1.1.23 The system shall have the capability to create a log of all transactions and activities. (Release 1A; Must)

3.2.4.2 Ingest Processing

FDsys ingest processing includes the processes necessary for functions to identify, manage, and verify digital content as it moves into the system.

Ingest processing is the function that manages content and content metadata as it is received into the system as a Submission Information Package (SIP). Content Originators and Service Specialists will have the capability to submit SIPs created from deposited, harvested, and converted content and content created using GPO style tools. Ingest processing creates AIPs and ACPs from SIPs and transfers the resulting content packages to storage.

3.2.4.2.1 Requirements for Ingest Processing

4.2.1.1 Ingest Processing Core Capabilities

4.2.1.1.1 Ingest processing performs the following functions:

4.2.1.1.1.1 Accept and validate SIPs (Release 1A; Must)

4.2.1.1.1.2 Create AIPs from SIPs (Release 1A; Must)

4.2.1.1.1.3 Create ACPs from SIPs (Release 1B; Must)

4.2.1.1.1.4 Apply digital time stamping to content (Release 1A; Must)

4.2.1.2 Ingest Processing

4.2.1.2.1 The system shall allow Content Originators and Service Specialists to submit content to ingest once content has been approved for release by the publisher. (Release 1A; Must)

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 1A; Should)

4.2.1.2.2 The system shall validate that SIPs conform to the requirements for a system compliant SIP, including but not limited to: (Release 1A; Must)

4.2.1.2.2.1 The system shall verify that the SIP includes all mandatory metadata elements.

4.2.1.2.2.2 The system shall verify that the METS file is valid.

4.2.1.2.2.3 The system shall verify that at least one digital object is present.

4.2.1.2.2.4 The system shall verify that all digital objects are operational with its intended supporting application.

4.2.1.2.3 The system shall provide the capability to reject non-conforming SIPs. (Release 1A; Must)

4.2.1.2.3.1 The system shall direct exceptions to Service Specialists.

4.2.1.2.4 The system shall provide the capability to notify users that a SIP is nonconforming. (Release 1A; Must)

4.2.1.2.5 The system shall provide the capability to notify users of the reasons a SIP is nonconforming. (Release 1A; Must)

4.2.1.2.6 The system shall allow the use of automatic file format verification against a format registry (e.g., the DROID software to check the PRONOM technical registry). (Release 1A; Must)

4.2.1.2.7 The system shall have the capability to verify content integrity (e.g., checksum). (Release 1A; Must)

4.2.1.2.8 The system shall pass the AIP to archival information storage after creation. (Release 1A; Must)

4.2.1.2.9 The system shall pass the ACP to access content storage after creation. (Release 1B; Must)

4.2.1.2.10 The system shall have the capability to create a log of all transactions and activities. (Release 1A; Must)

3.2.4.3 Preservation Processing

FDsys preservation processes will enable comprehensive, timely, permanent public access to the official version(s) of U.S. Government publications in digital formats. Only content in scope for GPO's dissemination programs will be accepted into FDsys archival storage and managed by preservation processes.

Preservation copies of digital publications, Archival Information Packages (AIPs), with associated technical metadata, will be maintained in FDsys Archival Storage.

Inputs

AIPs are content information and associated Preservation Descriptive Information (PDI) needed to preserve the content over the long term, bound together by packaging information. Content Information is functional digital files with behaviors controlled by applications.

Outcomes

In order of preference, the outcomes desired are:

- Faithfully duplicated files, rendered using the original application.
- Files which faithfully reproduce content, behavior and presentation of the original, rendered using other software than the original application.
- Files which exactly convey the content but may alter behavior and/or presentation, rendered using other software than the original application.

Preservation Strategies

Refreshment (copying) of content to new media. Refreshment is the systematic transfer of stored digital information to newer, fresher media.

Migration of data in formats or versions that are in danger of becoming or have become obsolete, to newer versions of that application or format. Migration is a process in which the underlying information is retained but older file formats and internal structures are replaced by newer.

Emulation preserves the essential behaviors and attributes of digital objects by using current software to mimic the original environment.

Hybrids of these approaches, or new approaches.

The preservation process employed in any given situation should be the least intrusive; i.e. that which alters the original AIP the least. See Figure 6 - Preservation Processes Flow Chart for a sample preservation decision process.

Criteria which Trigger Preservation Processes

Preservation processes are triggered by an assessment. Assessment criteria for initiating a process include:

- Schedule
- Application Failure (loss of functionality)
- System-detected loss of content, functionality, or metadata
- Managed request (from a service specialist)
- Request for new type of derivative for access
- Scheduled random sampling of content in AIP storage

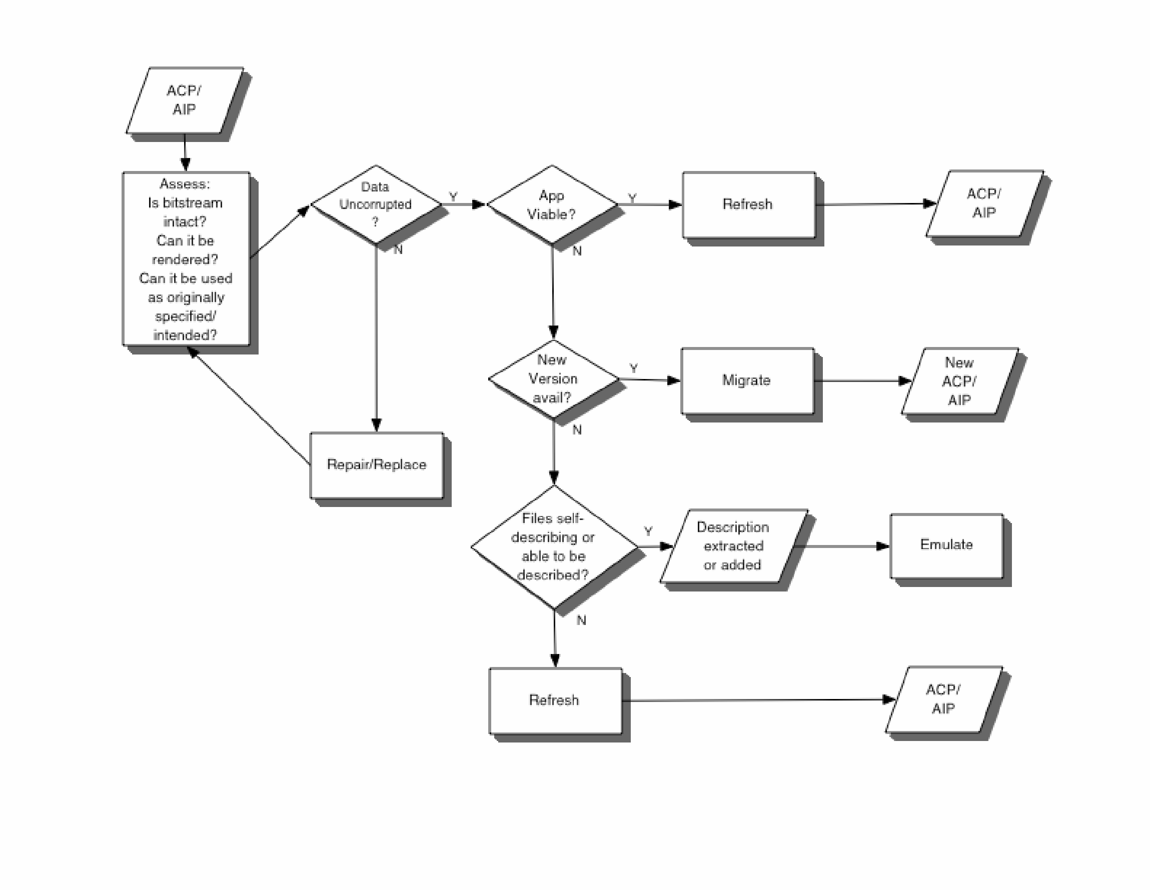
Selection of Preservation Processes

The specific preservation processes required by GPO are a policy determination. FDsys must be capable of supporting activities necessary to keep content accessible and usable, including:

- Migration
- Refreshment
- Emulation

The following Figure models the FDsys preservation process workflow. A viable application refers to application software which retains all of its original functionality. For example, an Archival Information Package (AIP) includes content in Microsoft Word 97 format. Word 97 is considered a viable application for GPO’s purposes if it will work without loss of functionality in the current FDsys operating system environment.

Figure 6 - Preservation Processes Flow Chart



Content Management of Archived Content

Content management functions and decisions associated with preservation processes include:

- File backup/redundant storage.
- Duration of preservation (can range from none to permanent).
- Validation of ACP against the AIP to ensure that the ACP is accurate.

Content disposition options include:

- Permanent retention in FDsys.
- Transfer to the National Archives and Records Administration (NARA).
- Scheduled removal of selected content from FDsys.
- Pushing or disseminating content to preservation partners, such as the Library of Congress or depository libraries.

3.2.4.3.1 Current Situation

GPO presently has no integrated system for preservation or permanent storage of digital content. The content that is archived typically does not meet preservation standards for data structure or metadata; instead it usually consists of harvested access derivatives or text data bases.

Access copies of digital publications, typically in PDF, HTML, or ASCII format are stored on, and may be accessed from, several platforms. These include:

- GPO Access
- GPO's archival server, http://www.permanent.access.gpo.gov
- OCLC's digital archive
- Library partner sites, such as the University of North Texas' *Cybercemetery*
- Agency partner sites, such as the Department of Energy's *Information Bridge*

Routine backup of GPO-managed data is performed under contract by Iron Mountain. Content mirrored on multiple Akamai servers functions as a failsafe. The only preservation process currently in use is refreshment.

3.2.4.3.2 Requirements for Preservation Processing

4.3.2.1 Preservation Processing Core Capabilities

4.3.2.1.1 The system shall have the ability to store AIPs in a preservation repository environment. (Release 1A; Must)

4.3.2.1.1.1 AIPs must remain free from corruption and remain accessible as GPO undergoes changes in information technology and infrastructure.

4.3.2.1.2 The system shall manage preservation processes. (Release 1C; Must)

4.3.2.1.2.1 Preservation process management includes the scheduled assessments, and resulting actions based on the attributes of the digital objects, their essential behaviors, etc., and applies the appropriate processes.

4.3.2.1.3 The system shall maintain the integrity of content throughout preservation processes. (Release 1C; Must)

4.3.2.1.3.1 When compared to the original AIP, the content is fully intelligible and unchanged in meaning and representation.

4.3.2.1.4 The system shall preserve all essential behaviors of digital content. (Release 1C; Must)

4.3.2.1.4.1 The system shall maintain content functionality associated with content presentation.

4.3.2.1.5 The system shall preserve all significant properties and attributes of digital content. (Release 1C; Must)

4.3.2.1.5.1 The system shall maintain content context.

4.3.2.1.5.2 The system shall maintain content structure.

4.3.2.1.5.3 The system shall maintain hyperlinks to content within the target document.

4.3.2.1.6 The system shall have the capability to produce DIPs which faithfully replicate AIPs. (Release 1B; Could / Release 1C; Must)

4.3.2.1.6.1 The system shall have the capability to produce DIPs which are interoperable with other OAIS-based repositories.

4.3.2.1.7 The system shall be capable of scheduling or executing preservation processes on individual AIPs or on classes of archival content. (Release 1C; Must)

4.3.2.2 Preservation Processing

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 1C; Must)

4.3.2.2.1.1 The system shall assure that the files resulting from migrations will be in a format free of proprietary restrictions. (Release 1C; Should / Release 2; Must)

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 1C; Must)

4.3.2.2.1.3 The system shall provide logs that record the results of migrations. (Release 1C; Must)

4.3.2.2.1.4 The system shall have the ability to produce notification of incomplete or unsuccessful migrations. (Release 1C; Must)

4.3.2.2.2 The system shall have the ability to preserve bitstreams in their native or received form by refreshment. (Release 1C; Must)

4.3.2.2.2.1 The system shall have the ability to verify that the refreshed file retains specified attributes and behaviors, i.e. is authentic and faithful.

4.3.2.2.2.2 The system shall provide logs that record the results of refreshment processes.

4.3.2.2.2.3 The system shall have the ability to produce notification of incomplete or unsuccessful refreshments processes.

4.3.2.2.3 The system shall have the ability to support emulation to preserve access to content. (Release 1C; Must)

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.

4.3.2.2.4 The system shall support the transformation of AIPs into ACPs. (Release 1B; Must)

4.3.2.2.5 When a preservation process results in the creation of a modification of an AIP, the system shall be capable of retaining the original AIP as it was accepted into the repository. (Release 1C; Must)

4.3.2.3 Preservation Processing - Assessment

4.3.2.3.1 The system shall have the ability to assess ingested content and determine preservation processes based on the assessments. (Release 1C; Must)

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.

4.3.2.3.1.2 There shall be no limit set on the number or frequency of assessments.

4.3.2.3.1.3 The system shall have the ability to re-assess content stored in the system.

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 1C; Could)

4.3.2.4 Preservation Processing - Administration

4.3.2.4.1 The system shall support scheduling the automatic execution of preservation processes. (Release 1C; Must)

4.3.2.4.2 The system shall support batch preservation processing of content. (Release 1C; Must)

4.3.2.4.3 The system shall support preservation processing on an item-by-item basis. (Release 1C; Must)

4.3.2.4.4 The system shall maintain an audit trail of preservation processes. (Release 1C; Must)

4.3.2.4.5 The system shall support the ability for authorized users to request preservation processes. (Release 1C; Must)

4.3.2.5 Preservation Processing - Storage

4.3.2.5.1 The system shall provide a digital archival repository environment which is based on open-standards architecture. (Release 1A; Must)

4.3.2.5.1.1 The repository environment shall keep AIPs separate from working or production copies.

4.3.2.5.1.2 The system shall ensure that the content in a working or production copy is synchronized with the AIP.

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.

4.3.2.6 Preservation Processing - Metadata

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 1A; Must)

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 1A; Must)

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 1A; Must)

4.3.2.7 Preservation Processing - Security

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 1A; Must)

3.2.4.4 Unique Identifier

Unique identifiers are character strings that uniquely identify all content within the system throughout the content lifecycle. Content managed by the system will be assigned an identifier that exists only once and thus is linked indefinitely to the corresponding content. The uniqueness of the assigned identifier ensures that the identifier will refer to only one object.

The system will create and assign unique IDs to content as defined by GPO business rules.

- Digital Objects: A unique ID will be assigned to all digital objects upon ingest into the system.
- Content Packages: A unique ID will be assigned to Content Packages (SIP, ACP, AIP)
- Jobs: A unique ID will be assigned to Jobs.

Style tools will assign unique ID's to digital objects, which will be passed to ingest. The system will assign unique IDs to content not created using style tools at ingest. All assigned unique identifiers will be recorded and used in metadata. Once assigned, a unique ID cannot be reused within the system.

3.2.4.4.1 Current Situation

Prior to FDsys, no unique IDs as defined in ConOps were in place, but some tracking mechanisms were in use as listed below:

- Jacket numbers (repeats every 3 years) (xxx-xxx) (Agency Publishing and Production)
    - Requisition numbers (agencies)
    - Purchase orders (Agency Publishing)
- ACSIS- assigns unique IDs

Granularity is currently at the jacket/purchase order level (generally 1 record per document/publication).

3.2.4.4.2 Requirements for Unique Identifier

4.4.2.1 Unique ID Core Capabilities

4.4.2.1.1 The system shall have the capability to organize file(s) into digital objects at a level of granularity appropriate to the content and as defined by GPO. (Release 1A; Must)

4.4.2.1.1.1 The system shall have the capability to assign unique IDs to publications. (Release 1A; Must)

4.4.2.1.1.2 The system shall have the capability to assign unique IDs to publications down to paragraph level. (Release 1C; Should / Release 2; Must)

4.4.2.1.1.3 The system shall have the capability to assign unique IDs to individually provided graphical elements at the individual element level. (Release 1A; Must)

4.4.2.1.1.4 The system shall have the capability to assign unique IDs to embedded graphical elements at the individual element level. (Release 1C; Should / Release 2; Must)

4.4.2.1.1.5 The system shall have the capability to assign unique IDs to video content. (Release 1A; Must)

4.4.2.1.1.6 The system shall have the capability to assign unique IDs to video content at a level of granularity as required by the system and GPO business units. (Release 3; Could)

4.4.2.1.1.7 The system shall have the capability to assign unique IDs to audio content. (Release 1A; Must)

4.4.2.1.1.8 The system shall have the capability to assign unique IDs to audio content at a level of granularity as required by the system and GPO business units. (Release 2; Could)

4.4.2.1.2 The system must create and assign a 9 character alphanumeric identifier (ANI) for each unique digital object. (Release 1A; Must)

4.4.2.1.2.1 Unique IDs must be non-intelligent.

4.4.2.1.2.2 Unique ID characters must include numbers 0-9 and letters A – Z (minus I and O).

4.4.2.1.2.3 Unique IDs must start with the character “A” (technical requirement).

4.4.2.1.2.4 Unique IDs must not conflict with other identifiers within FDsys.

4.4.2.1.2.5 The number of digital objects will be in accordance with the FDsys System Sizing document.

4.4.2.1.3 The system shall have the ability to assign and accept a unique ID to a related or continuous piece of content in context. (Release 1A; Must)

4.4.2.1.3.1 Scanned publications and submission level metadata

- A 9 character alpha numeric unique ID following the Code 39 barcoding standard (ANSI: BC1-1995)
- The first character is the fixed letter “A” which enables validation for METS

Example: A12345678

4.4.2.1.3.2 Scanned publications at the page level

- Publication unique ID followed by an underscore and a sequential 5 digit identifier representing each scanned image.
- 5 digit identifier does not correspond with the physical page number.

Example: A12345678_00001

4.4.2.1.4 Unique IDs must not conflict with other identifiers within FDsys. (Release 1A; Must)

4.4.2.1.5 The system shall store unique IDs in metadata. (Release 1A; Must)

4.4.2.2 Job ID

4.4.2.2.1 The system must create and assign a unique ID for each job. (Release 1A; Must)

4.4.2.2.2 The system must provide the capability to assign unique IDs to Content Originator orders of content jobs. (Release 1C; Must)

4.4.2.2.3 The system must provide the capability to assign unique IDs to Content Originator orders of service jobs. (Release 1C; Must)

4.4.2.2.4 The system must provide the capability to assign unique IDs to non-Content Originator order related jobs. (Release 1A; Must)

4.4.2.2.5 The system must not re-use Job unique IDs. (Release 1A; Must)

4.4.2.3 Content Package ID

4.4.2.3.1 The system must create and assign a unique ID for each Content Package. (Multiple Releases; Must)

4.4.2.3.1.1 The system must create and assign a unique ID to each SIP (Release 1A; Must)

- Converted Content Packages
  - 3 x 3 by publication (9 digits total xxx xxx xxx)
  - UID_Image # (14 digits total – xxx xxx xxx_xxxxx)
- Harvested Content Packages
- Deposited Content Packages

4.4.2.3.1.2 The system must create and assign a unique ID to each AIP (Release 1A; Must)

4.4.2.3.1.3 The system must create and assign a unique ID to each ACP (Release 1B; Must)

4.4.2.3.1.4 The system must create and assign a unique ID to each DIP (Release 1B; Must)

4.4.2.3.2 The system must not re-use Content Package unique IDs. (Release 1A; Must)

4.4.2.3.3 The system must record package unique ID's in metadata. (Release 1A; Must)

4.4.2.4 User Interface for Unique ID

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 1A; Must)

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).

3.2.4.5 Persistent Name

In order for the digital content managed by FDsys to be easily found and shared by a wide range of users with different needs and using different systems, there must be a simple way of reliably and unambiguously identifying each resource independent of its location.

Persistent naming allows for an interoperable schema of identifiers that uniquely identify content, support permanent access to that content, and support access to information about the content. A resolution system will locate and provide access to content and metadata associated with assigned persistent names.

The system will assign persistent names to content packages at ingest. All assigned persistent names will be recorded and used in metadata. Once assigned, a persistent name cannot be reused within the system.

3.2.4.5.1 Current Situation

Since 1998, GPO has assigned unique Persistent Uniform Resource Locators, or PURLs, which provide online access to electronic publications published by U.S. Government agencies. Assigning persistent names to electronic federal resources is seen as a key element in providing permanent public access to these resources for the FDLP, as the value of these documents is reduced and maintenance issues increase if they cannot be identified reliably, found, and accessed when referenced in bibliographic records. If the references to the electronic files are not constant it could become a difficult maintenance issue.

Access to electronic texts is maintained by updating electronic address information (uniform resource locators, or URLs) in GPO's PURLs server. Instead of pointing directly to the location of an Internet resource, a PURL points to this intermediate resolution service. The resolution service associates the PURL with the actual URL and returns that URL to the client, which can then complete the transaction in the normal fashion.

3.2.4.5.2 Requirements for Persistent Name

4.5.2.1 Persistent Name Core Capabilities

4.5.2.1.1 The system shall assign persistent names to all in-scope published versions during access processing. (Release 1B; Must)

4.5.2.1.1.1 Persistent name must not conflict with other identifiers within FDsys.

4.5.2.1.2 The system shall comply with standards and best practices pertaining to persistent naming. (Release 1B; Must)

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 1B; Should)

4.5.2.1.4 The system shall accommodate OpenURL syntax to enable federated searching. (Release 1B; Must)

4.5.2.1.5 The system shall arbitrate between Content Originator naming and global naming standards. (Release 1B; Must)

4.5.2.1.5.1 The system shall defer to a persistent name assigned by GPO or by a GPO naming authority.

4.5.2.1.6 The system shall assign persistent names that are location independent. (Release 1B; Must)

4.5.2.1.7 The system shall assign persistent names that are protocol independent. (Release 1B; Must)

4.5.2.1.8 The system must not reuse persistent names. (Release 1B; Must)

4.5.2.1.9 The system shall have the capability to assign intelligent persistent names. (Release 1B; Must)

4.5.2.1.10 The system shall have the capability to assign non-intelligent persistent names. (Release 1B; Could)

4.5.2.1.11 The system shall have the capability to incorporate existing identifiers into the persistent naming string. (Release 1B; Could)

4.5.2.1.12 The system shall have the capability to record the date and time of persistent name creation. (Release 1B; Must)

4.5.2.1.13 The system shall have the capability to create reports about persistent name management. (Release 1C; Could)

4.5.2.1.14 The system shall associate persistent names to existing legacy GPO naming schemes, including but not limited to GPO-assigned PURLs. (Release 1B; Must)

4.5.2.1.15 The system shall be scalable in terms of persistent name assignment and resolvability. (Release 1B; Must)

4.5.2.2 Persistent Name Resolution

4.5.2.2.1 The system shall use a resolution system to locate and provide access to content with persistent names. (Release 1B; Must)

4.5.2.2.1.1 The resolution process shall resolve an assigned name into a resource or the resource metadata.

4.5.2.2.1.2 The resolution process must allow for persistent name recognition within standard browsers.

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 1B; Must)

4.5.2.2.3 The system shall support resolution of a single persistent name to multiple distributed locations. (Release 1B; Should)

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.

4.5.2.2.4 The system shall support resolution of a single persistent name to multiple content versions. (Release 1B; Should)

4.5.2.2.4.1 The system shall determine the most appropriate version based attributes including, but not limited to, access privileges, format, location, date.

4.5.2.3 Persistent Name Metadata

4.5.2.3.1 The system shall record persistent names associated with content. (Release 1B; Must)

4.5.2.3.2 The system shall record existing persistent names associated with content. (Release 1B; Must)

4.5.2.3.3 The system shall provide the capability to associate metadata with the persistent name (Release 1B; Must)

3.2.4.6 Authentication

The content authentication functional element will assure users that content made available by GPO through FDsys is authentic and/or official. This includes identifying content that has been approved by, contributed by, or harvested from an official source such as a Federal publishing agency, its business partner, or other trusted source. GPO generally defines its products as official if the content was issued by the United States Government at Government expense or as required by law. However, not all of these products are deemed official in the legal sense and may not be sufficient for use in court. For example, the Federal Register is recognized as official in both online and tangible formats whereas the U.S. Code can only be cited in court in its paper format. For situations where Content Originators have designated that specific content delivery methods, file formats, or content presentations must be used for the purpose of legal citation, GPO will record information about this designation (intended use) in metadata.

The content authentication functional element will help GPO establish a clear chain of custody for deposited, harvested, and converted content that is ingested into the system, and chain of custody information will be made available to End Users. Content authentication will assure users that content is authentic meaning that it has been verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator.

The system will verify content integrity by assuring users that content has not been altered or destroyed in an unauthorized manner. The system will verify content integrity at various points throughout the content lifecycle including transmission from the Content Originator to the system, while resident within the system, and upon certification and delivery from the system. If content is modified, the content authentication functional element will have the ability to notify designated users when, where, by whom, and what changes were made to content. Furthermore, the system will have the capability to certify content at both the document and granular levels, and certification will be conveyed to users through the use of integrity marks such as digital signatures and watermarks.

3.2.4.6.1 Current Situation

In “A Strategic Vision for the 21st Century,” the Public Printer identified the need to authenticate all known Federal documents whether printed or born digital. GPO recognizes that as the amount of electronic Federal Government information increases, there is a need to ensure that information is disseminated from an official source and that content is protected against unauthorized modification or substitution.

In response to this need, GPO has established an operational Public Key Infrastructure (PKI). A Public Key Infrastructure includes the hardware, software, personnel, and operational policies that can be used to verify document authenticity and integrity, authenticate users, and secure transactions. For example, processes exist to use GPO’s PKI to issue personal user digital certificates to Federal agency customers, in compliance with Federal Government PKI standards. In addition, GPO's PKI is cross-certified with the Federal Bridge Certification Authority (FBCA). Cross-certification ensures that business, administrative, and technical processes related to GPO's PKI will interoperate with other Federal agencies and user communities that are part of the Federal Bridge. The FBCA is a fundamental element of the trust infrastructure that provides the basis for intergovernmental and cross-governmental secure information transmission.

As a step prior to the establishment of the FDsys, GPO plans to use authentication technologies including digital certificates and digital signatures to verify the authenticity and integrity of the electronic U.S. Government documents that it disseminates through the Federal Depository Library Program (FDLP). GPO plans to use these technologies to add GPO's Seal of Authenticity to Adobe Acrobat Portable Document Format (PDF) documents that are available from the GPO Access web site. The GPO Seal of Authenticity will provide verification that a document has not been altered since it was authenticated and disseminated by GPO. The Seal will also help assure users that the document has, in fact, been disseminated by GPO.

Additional content authentication needs and requirements for both Content Originators and End Users are being addressed as part of FDsys. While current authentication efforts are focused on content delivery, FDsys aims to extend authentication benefits and safeguards throughout the entire content lifecycle.

GPO is poised to begin manually applying digital signatures to PDF files that are available from the GPO Access Web site, and a procurement is pending for the automated application of digital signatures to PDF files in bulk quantity. In addition, processes exist to use GPO’s PKI to issue personal user digital certificates to Federal agency customers, in compliance with Federal government PKI standards. GPO is also cross-certified with the Federal Bridge and would like to become a Shared Service Provider under the Federal E-Authentication initiative.

3.2.4.6.2 Requirements for Authentication

4.6.2.1 Authentication Core Capabilities

4.6.2.1.1 The system must provide the capability to verify content as authentic meaning that it is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator. (Release 1A; Must)

4.6.2.1.2 The system must provide the capability to certify content as official meaning that the content has been approved by, contributed by, or harvested from an official source such as a Federal publishing agency, its business partner, or other trusted source. (Release 1A; Must)

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.

4.6.2.1.3 The system must provide the capability to certify content at levels of granularity defined in GPO. (Release 1A; Must)

4.6.2.1.4 The system must provide the capability to convey certification by means of an integrity mark. (Release 1A; Must)

4.6.2.1.5 The system shall provide the capability to use GPO's Public Key Infrastructure (PKI) wherever optimal. (Release 1A; Should)

4.6.2.1.6 The system must comply with GPO and Federal privacy policies. (Release 1A; Must)

4.6.2.1.7 The system must comply with GPO and Federal authentication policies. (Release 1A; Must)

4.6.2.1.8 The system must use public key cryptography, digital certificates, encryption or other widely accepted information security mechanisms. (Release 1A; Must)

4.6.2.2 Authentication - Content Pre-ingest and Ingest

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 1A; Must)

4.6.2.2.1.1 The system shall verify Content Originator identity and authority to publish for content that is deposited with the system.

4.6.2.2.1.2 Valid proof of the Content Originator's identity shall be logged by the system.

4.6.2.2.1.3 The source of the deposited content shall be recorded in metadata.

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 Content Originator to the system, and information about content integrity should be recorded in metadata.

4.6.2.2.1.5 The system shall verify that the sender (Content Originator) and the recipient (GPO) were, in fact, the parties who claimed to send or receive content, respectively, and this information should be recorded in metadata.

4.6.2.2.1.6 The system shall have the capability to record intended use in metadata.

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.

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 1A; Must)

4.6.2.2.2.1 The system shall examine harvested content for the purpose of verifying the source of the harvested content.

4.6.2.2.2.2 The source of harvested content shall be recorded in metadata.

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.

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 1A; Must)

4.6.2.2.3.1 The source of converted content shall be recorded in metadata.

4.6.2.2.3.2 The source of tangible content that was used to create the converted content shall be recorded in metadata.

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 Service Provider to the system, and information about content integrity should be recorded in metadata.

4.6.2.2.3.4 The system shall verify that the sender (Service Provider) and the recipient (GPO) were, in fact, the parties who claimed to send or receive content, respectively and this information should be recorded in metadata.

4.6.2.2.3.5 The system shall have the capability to record intended use in metadata.

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.

4.6.2.2.4 The system must provide the capability to recognize and validate integrity marks at pre-ingest. (Release 1A; Must)

4.6.2.2.4.1 The system shall have the capability to retain integrity marks in accordance with GPO business rules.

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.

4.6.2.2.5 The system shall provide the capability to process encrypted files at pre-ingest. (Release 1A; Could / Release 2: Must)

4.6.2.2.6 The system must verify chain of custody at pre-ingest. (Release 1A; Must)

4.6.2.2.6.1 Chain of custody information shall be recorded in metadata.

4.6.2.2.6.2 The system shall have the ability to gather relevant information from integrity marks (e.g., digital signatures, digital certificates) for use as part of the chain of custody.

4.6.2.2.7 The system must provide the capability to perform redundancy checking (e.g., checksum) on content at ingest. (Release 1A; Must)

4.6.2.2.7.1 The system must provide the capability to record checksum type and value in metadata.

4.6.2.2.8 The system must provide the capability to apply a digital timestamp to content at ingest. (Release 1A; Must)

4.6.2.2.9 The system must update chain of custody information in metadata at ingest. (Release 1A; Must)

4.6.2.3 Authentication - User Credentials

4.6.2.3.1 The system must provide the capability to verify the identity of the Content Originator. (Release 1A; Must)

4.6.2.3.2 The system must provide the capability to verify the Content Originator's authority to publish. (Release 1A; Must)

4.6.2.4 Authentication - Content Integrity

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 1A; Must)

4.6.2.4.2 The system must assure integrity of content within the system. (Release 1A; Must)

4.6.2.4.2.1 The system shall have the capability to assure integrity of content within the system at a definable frequency.

4.6.2.4.2.2 The system shall have the capability to assure integrity of content in a timeframe based on GPO business rules.

4.6.2.4.2.3 The system shall not allow critical transaction and system log files to be adjusted by any unauthorized party.

4.6.2.4.2.4 The system shall have the capability to assure integrity of content during backup and other system processes.

4.6.2.4.3 The system must assure integrity of pre-ingested and ingested content. (Release 1A; Must)

4.6.2.4.3.1 Content integrity shall be maintained during transmission from the Content Originator to the system.

4.6.2.4.3.2 The system shall have the capability to verify and 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.

4.6.2.4.4 The system must have the capability to assure integrity of delivered content. (Release 1B; Must)

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.

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.

4.6.2.4.5 The system must provide the capability to provide notification that a change has occurred to content within the system. (Release 1A; Must)

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.

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.

4.6.2.4.5.3 The system shall provide the capability to notify designated users when changes were made to content.

4.6.2.4.5.4 The system shall provide the capability to notify designated users where changes were made to content.

4.6.2.4.5.5 The system shall provide the capability to notify designated users by whom changes were made to content.

4.6.2.4.5.6 The system shall provide the capability to notify designated users what changes were made to content.

4.6.2.4.5.7 The system shall log changes to content in metadata.

4.6.2.4.6 The system must provide the capability of demonstrating continued integrity of content packages when authorized changes are made (such as to the metadata). (Release 1A; Must)

4.6.2.5 Authentication - Time Stamps

4.6.2.5.1 The system must support digital time stamping. (Release 1A; Must)

4.6.2.5.2 The system must provide the capability to provide date and time verification. (Release 1A; Must)

4.6.2.5.3 The system must 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 1A; Must)

4.6.2.6 Authentication - Integrity Marks

4.6.2.6.1 The system must support the use of integrity marks. (Release 1A; Must)

4.6.2.6.2 Integrity marks must include certification information. (Release 1A; Must)

4.6.2.6.3 Integrity marks must employ widely accepted information security mechanisms (e.g., public key cryptography, digital certificates, digital signatures, XML signatures, digital watermarks, or traditional watermarks). (Release 1A; Must)

4.6.2.6.4 The system must support the capability to manually add integrity marks to content. (Release 1B; Could)

4.6.2.6.5 The system must support the capability to automatically add integrity marks to content. (Release 1B; Must)

4.6.2.6.6 The system must support the use of visible integrity marks. (Release 1B; Must)

4.6.2.6.7 The system must support the use of invisible integrity marks. (Release 1B; Could / Release 2; Must)

4.6.2.6.8 The system must provide flexibility regarding where the integrity mark is applied through automated and manual processes. (Release 1B; Must)

4.6.2.6.9 The system must 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 1B; Must)

4.6.2.6.10 The system must support the application of multiple integrity marks on the same content. (Release 1B; Must)

4.6.2.6.11 The system must support the application of security policies, such that integrity marks can be applied to content in particular sequences depending on levels of authority. (Release 1B; Must)

4.6.2.7 Authentication - Content Delivery

4.6.2.7.1 The system must provide the capability for users to validate the authenticity, integrity, and official status of the content packages that are delivered from the system. (Release 1B; Must)

4.6.2.7.2 The system must 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 1B; Must)

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:

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 1B; Could)

4.6.2.7.3.2 The integrity mark must include certification information including the following but not limited to the following: (Release 1B; Must)

- Certifying organization
- Date on the signer's digital certificate
- Digital time stamp
- Public key value
- Hash algorithm used
- Reason for signing
- Location
- Contact information
- Name of entity that certified the content
- Expiration date of the digital certificate

4.6.2.7.3.3 Wherever feasible, the values for the above fields shall be extracted from the digital certificate that was used to create the digital signature. (Release 1B; Must)

4.6.2.7.3.4 The system shall provide the flexibility to add new fields. (Release 1B; Must)

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 1B; Must)

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 1B; Must)

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 1B; Must)

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 1B; Should / Release 2; Must)

4.6.2.7.3.9 For electronic presentation, validation shall be done automatically without End User intervention. (Release 1B; Should / Release 2; Must)

4.6.2.8 Re-authentication of Content

4.6.2.8.1 The system must provide the capability to re-authenticate content that has already been authenticated (e.g., expired certificate). (Release 1A; Could)

4.6.2.8.2 The system must provide the capability to notify GPO System Administrators when content needs to be re-authenticated. (Release 1A; Could)

4.6.2.8.3 The system must provide the capability for GPO to change or revoke the authentication status of content. (Release 1A; Must)

4.6.2.9 Authentication Standards/Best Practices

4.6.2.9.1 The system must have the capability to support RSA Digital Signature in accordance with IETF RFC 3447. (Release 1A; Must)

4.6.2.9.2 The system must have the capability to support PKCS #1 for RSA key pair for digital signatures. (Release 1A; Must)

4.6.2.9.3 The system must have the capability to support IEFT Public Key Infrastructure (PKIX) X. 509 v. 3 standards for certificate compatibility. (Release 1A; Must)

4.6.2.9.4 The system must have the capability to support PKCS #1, #7, #11, and #12. (Release 1A; Must)

4.6.2.9.5 The system must have the capability to support ITU X.509 version 3 standard for certificate format. (Release 1A; Must)

4.6.2.9.6 The system must have the capability to support up to 2048-bit RSA public/private key generation (asymmetric algorithm). (Release 1A; Must)

4.6.2.9.7 The system must have the capability to support cryptographic standards in accordance with the FIPS 140 series. (Release 1A; Must)

4.6.2.9.7.1 The system must have the capability to comply with HMS FIPS 140-2.

4.6.2.9.8 The system must have the capability to support FIPS 180-2 for SHA-1, SHA-256, SHA-384, and SHA-512. (Release 1A; Must)

4.6.2.9.9 The system must have the capability to support Redundancy Checking including Cyclic Redundancy Checking (CRC) and checksum. (Release 1A; Must)

4.6.2.9.10 The system must have the capability to support XML Digital Signature standards RFC 3275 and XMLDSIG. (Release 1A; Must)

4.6.2.9.11 The system must have the capability to support AES encryption standard FIPS 197. (Release 1A; Must)

4.6.2.9.12 The system must have the capability to support XML Encryption standard XMLENC. (Release 1A; Must)

4.6.2.9.13 The system must have the capability to support TDES ANSI X9.52. (Release 1A; Must)

4.6.2.9.14 The system must have the capability to support SSL / TLS. (Release 1A; Must)

4.6.2.9.15 The system must have the capability to support LDAP IETF RFC 2251. (Release 1A; Must)

4.6.2.9.16 The system must have the capability to support ITU X.500. (Release 1A; Must)

4.6.2.9.17 The system must have the capability to support SAML. (Release 1A; Must)

4.6.2.9.18 The system must be based on open standards including ITU, ISO, PKCS, IETF, ANSI and other open standards. (Release 1A; Must)

4.6.2.9.19 The system must accommodate updates to the above cryptographic standards. (Release 1A; Must)

4.6.2.9.20 The system must have the capability to comply with current electronic signature guidance from the National Archives and Records Administration including “Records Management Guidance for Agencies Implementing Electronic Signature Technologies.” (Release 1A; Must)

4.6.2.10 Authentication Records Management

4.6.2.10.1 The system must create administrative records of authentication processes. (Release 1A; Must)

4.6.2.10.2 The system must create transaction records of administrative processes. (Release 1A; Must)

4.6.2.10.3 The system must support an audit capability for content certification. (Release 1A; Must)

4.6.2.10.4 The system must support an audit capability for content validation. (Release 1A; Must)

4.6.2.10.5 The system must comply with GPO and Federal records management policies. (Release 1A; Must)

4.6.2.11 Authentication Metadata

4.6.2.11.1 The system must provide the capability to include authentication and certification information in metadata. (Release 1A; Must)

4.6.2.11.1.1 Authenticity metadata shall have the capability to include the following: (Release 1A; Must)

- Source of deposited, harvested, and converted content.
- Content Originator identity and authority to publish for deposited content.
- Source of tangible content that was used to created converted content.
- Chain of custody information excluding information about End User chain of custody.

4.6.2.11.1.2 Integrity metadata shall have the capability to include the following: (Release 1A; Must)

- Information about any pre-ingest and ingest integrity checks for transmission to the system and any integrity checks within the system.
- What changed (e.g., deleted text, no changes).
- Changed by (e.g., unknown user/Joe Smith/system).
- Where (e.g., page 7).
- When (e.g., 10/272006 6:01 am).

4.6.2.11.1.3 Non-repudiation metadata shall have the capability to include the following: (Release 1A; Must)

- Sender (identity and proof).
- Recipient (identity and proof).

4.6.2.11.1.4 Intended Use metadata shall have the capability to include the following: (Release 1A; Must)

- Content Originators have designated that specific content delivery methods, file formats, or content presentations must be used for the purpose of citation in a court. Examples include print, PDF, current version, content harvested from specific site, content digitized from a specific collection.

3.2.4.7 Version Control

Version control is a strategic goal to be met by FDsys. Version control in the FDsys will evaluate and establish the version of a piece of content and subsequently track it through its entire life cycle.

Version control will be called upon to analyze Content Packages and assign the appropriate version identifier, consistent with requirements for version triggers and chain of custody. The chain of custody will be reflected in metadata.

Serials control, which uses metadata to identify and manage the relationships among the issues or volumes of serially-issued publications, is a bibliographic control issue and is addressed in the cataloging and reference tools requirements. The Monthly Labor Review is an example of a serially-issued title, in which each individual issue is related to those before and after it, but is comprised of different content.

Other relationships between iterations of specific content, such as the progression from a congressional bill to a public law in slip form to publication in the United States Code, are content management issues, and are addressed in the overview of the content processing section.

Users, including all categories in the FDsys User Class model, want to be certain that they are using the version of information that meets their needs and to be able to track the history of changes that may have occurred. In the case of Federal information, multiple versions of Government publications may be available on public Web sites. This can be confusing and potentially damaging to users who are not aware of the version status of the content. Version control is a necessary operation in the management and dissemination of digital content to ensure that users are accessing the appropriate or desired content.

Version control is a critical function of GPO's FDsys. But in order for this functionality to work in the system context, GPO will need to fully define what constitutes a unique manifestation of a publication across all publication formats (e.g., monograph, serial).

GPO envisions that the process of version control will include acquiring, cataloging, storing, preserving, indicating relationships among, and retrieving different versions of content. This process may be accomplished by assessing various document attributes (e.g., structure, content, and format), creating metadata about these attributes, monitoring changes to the attributes, updating the metadata to indicate changes to the attributes, and creating links to related documents. The version control process within the FDsys will be automated whenever possible, but subjective evaluation and interpretation by Service Specialists may be a critical requirement at various points through the process.

3.2.4.7.1 Current Situation

Version control at GPO is currently combined with GPO's bibliographic processes, as well as the ILS and currently operational PKI systems.

GPO provides bibliographic control by observing a set of international rules and standards, as well as local practices to create and maintain bibliographic records. The standards, rules, terminology, and definitions were originally formulated to address "book format" terminology and the traditional relationships within the book industry with publishers, distributors, and libraries. GPO's current functional requirements for bibliographic control are derived from the Machine-Readable Cataloging (MARC) 21 standards. Elements of version control, in particular chain of custody functionalities, are being addressed to some degree by GPO's planned rollout of PKI.

3.2.4.7.2 Requirements for Version Control

4.7.2.1 Version Control Core Capabilities

4.7.2.1.1 The system shall have the ability to assign unique version identifiers to content packages that do not already contain version identifiers. (Release 1A; Should / Release 1C; Must)

4.7.2.1.1.1 Version identifiers will be created at the time the version detection mechanism has activated a version trigger and detected a new version.

4.7.2.1.2 The system shall record existing version identifiers. (Release 1A; Must)

4.7.2.1.2.1 Recorded version identifiers will be human and machine readable.

4.7.2.1.3 The system must allow authorized users to input, view, and manage version information. (Release 1A; Must)

4.7.2.1.4 The system shall have the capability to alert a Service Specialist and Content Originators when duplicate content is rejected. (Release 1A; Should / Release 1B; Must)

4.7.2.1.5 The system shall log all version history. (Release 1A; Must)

4.7.2.1.5.1 The version history log shall be incorporated into the package's metadata.

4.7.2.1.6 The system shall provide the capability to apply version control to work in progress content. (Release 1A; Could / Release 1C; Should; Release 2; Must)

4.7.2.2 Version Triggers

4.7.2.2.1 The system must apply rules for version triggers. (Release 2; Must)

4.7.2.2.1.1 The system shall apply rules for version triggers to groups of related content as defined by GPO business units.

4.7.2.2.1.2 Content Evaluators must be able to modify rules for version triggers.

4.7.2.2.2 The system shall detect version triggers as defined by GPO business units. Version triggers include, but are not limited to, the following: (Release 2; Must)

- Modifications to the content

- Changes to the “last updated” date
- Changes to a publication’s title
- Changes to a publication’s edition statement
- Changes in the issuing agency of a publication
- Changes in file format (e.g., TIFF to JPEG)
- Changes to the publication’s numbering scheme (e.g., volume 100, issue 50, year 2005, etc.)
- Version designation changes by Content Originator

4.7.2.2.3 The system shall provide the capability to alert users when version triggers have been activated. (Release 2; Must)

4.7.2.2.3.1 This will be done through channels that include push and pull technologies (e.g., notifications lists, RSS feeds).

4.7.2.2.4 The system shall provide the capability to notify designated GPO Service Specialists when a version cannot be determined. (Release 2; Must)

4.7.2.3 Version Detection

4.7.2.3.1 The system shall determine if version identifiers are present in content packages. (Release 1A; Must)

4.7.2.3.1.1 Version identifiers will be stored in metadata.

4.7.2.4 Version Metadata

4.7.2.4.1 The system shall express version information in metadata. (Release 1A; Must)

4.7.2.4.1.1 The system will update the metadata to indicate changes to attributes (e.g., structure, content, format, etc.).

4.7.2.4.2 The system shall record chain of custody in metadata (e.g., who created the content, when it was created, who approved the content for release, etc.). (Release 1A; Must)

4.7.2.5 Version Relationships

4.7.2.5.1 The system shall determine and record relationships between versions (e.g., version links). (Release 1A; Must)

4.7.2.5.1.1 The system will establish links to related documents identified through version information in metadata.

4.7.2.5.1.2 Reference to these relationships will be permanently available.

4.7.2.5.1.3 The system must be able to render relationship information so that it is human-readable.

4.7.2.6 Version Notification

4.7.2.6.1 The system shall have the capability to notify users which version of content they are accessing. (Release 1B; Must)

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 1B; Must)

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 1B; Must)

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 1B; Must)

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)

4.7.2.6.1.5 The system shall have the capability to notify users that access to a version is restricted. (Release 1B; Must)

3.2.5 INFRASTRUCTURE

3.2.5.1 Workflow

Workflows are utilized in the FDsys to automate business processes. Workflows will also allow manual interaction with the system if the business function requires such human interaction.

The system shall provide the capabilities to define, execute and monitor the workflows at various granularity levels. The system shall provide GUI tools for users to perform the workflow management tasks.

Traditionally, workflows are backed up by workflow engines that are mainly concerned with the flow patterns, tasks and their transitions within the workflow. Driven primarily by business needs, the BPM (Business Process Management) has emerged to address issues beyond the flow of work and execution of tasks that have been handled by workflow engines. Technically BPM can be considered a superset of workflow. It is concerned with the definition (BPMN, Business Process Modeling Notation), execution (BPEL, Business Process Execution Language) and management of business processes. Also BPM addresses application interfaces explicitly, and is capable of coordinating activities across multiple applications.

This document describes the overall requirements for workflows in the FDsys. A specific workflow shall be defined according to its concrete business requirements. Both the workflow engine based approach and the BPM approach should be evaluated to fulfill the specific business needs during the course of concept selection.

3.2.5.1.1 Current Situation

Currently, GPO accepts content from many different areas and runs various processes on the content. These processes are part of the various workflow tasks, but many of these tasks are manual and undocumented. The workflows that are documented are generally not defined in the same manner as workflows from other areas within GPO.

IT is currently working on defining workflows, and is looking at operation-based workflows for In-Plant Production. Recent workflows for the Plant have been created with Popkin, and some of these workflows may translate and/or be rolled over into FDsys workflows.

3.2.5.1.2 Requirements for Workflow

5.1.2.1 Workflow Core Capabilities

5.1.2.1.1 The system shall provide the capability to define workflows. (Release 1A; Must)

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.

5.1.2.1.1.2 The system shall provide the capability to validate workflow definitions against the established schema.

5.1.2.1.2 The system shall provide the capability to create new versions of existing workflows. (Release 1A; Must)

5.1.2.1.3 The system shall provide the capability to test new versions of existing workflows without interrupting the current workflow. (Release 1A; Must)

5.1.2.1.4 The system shall provide the capability to place new versions of workflow into production. (Release 1A; Must)

5.1.2.1.4.1 The system shall provide the capability to deploy newly developed or modified workflows without interruption to other workflows.

5.1.2.1.5 The system shall provide the capability to replace current versions of workflows with previous versions when required without interruption to other workflows. (Release 1A; Must)

5.1.2.1.6 The system shall provide the capability to manage business rules. (Release 1A; Must)

5.1.2.1.6.1 The business rules shall support user-defined hierarchy structure (e.g. related rules are self-aware of precedence).

5.1.2.1.7 The system shall provide the capability to manage manual activities. (Release 1A; Must)

5.1.2.1.8 The system shall provide the capability to manage automated activities. (Release 1A; Must)

5.1.2.1.9 The system shall provide the capability to assign comments on jobs/activities. (Release 1B; Must)

5.1.2.1.10 The system shall provide the capability for checkpointing critical workflow status and processes (e.g. taking a snapshot of the current system in the event of a system failure). (Release 1A; Must)

5.1.2.1.10.1 The system shall provide the capability for saved data from checkpointing to be portable to other failover locations.

5.1.2.1.10.2 The system shall provide the capability for the frequency of checkpointing the system to be controlled by the user.

5.1.2.1.10.2.1 The system shall provide the capability for checkpointing to be automated or manually controlled.

5.1.2.1.10.3 The system shall provide the capability for the user to control the scope of the data captured by checkpointing.

5.1.2.1.10.4 The checkpointing of the system shall be transparent to the user.

5.1.2.1.11 The system shall store information related to workflows in metadata. (Release 1A; Must)

5.1.2.1.11.1 The system shall store information about workflows in metadata.

5.1.2.1.11.2 The system shall store information about jobs in metadata.

5.1.2.1.11.3 The system shall store information about activities in metadata.

5.1.2.2 Workflow - Control of Execution

5.1.2.2.1 The system shall provide the capability to control the execution of activities. (Release 1A; Must)

5.1.2.2.1.1 The system shall provide the capability to sequence activities to optimize operations. (Release 1A; Could / Release 2; Must)

5.1.2.2.1.2 The system shall provide the capability to schedule for manual and automated activities. (Release 1A; Could / Release 1B; Must)

5.1.2.2.1.2.1 The system shall provide the capability to assign deadlines for jobs/activities.

5.1.2.2.1.2.2 The system shall provide the capability to assign estimated completion times for jobs/activities.

5.1.2.2.1.3 The system shall provide the capability to assign human resources to manual activities. (Release 1A; Could)

5.1.2.2.1.4 The system shall provide the capability to suspend and resume activities. (Release 1A; Must)

5.1.2.2.1.5 The system shall provide the capability to restart activities. (Release 1A; Must)

5.1.2.2.1.6 The system shall provide the capability to cancel activities. (Release 1A; Must)

5.1.2.2.1.7 The system shall provide the capability to log activities. (Release 1A; Must)

5.1.2.2.1.8 The system shall provide the capability to manage work lists of activities. (Release 1A; Must)

5.1.2.2.1.9 The system shall provide the capability to perform actions on a batch of activities. (Release 1A; Must)

5.1.2.2.2 The system shall provide the capability to control the execution of jobs. (Release 1A; Must)

5.1.2.2.2.1 The system shall provide the capability to sequence jobs to optimize operations. (Release 1A; Should)

5.1.2.2.2.2 The system shall provide the capability to suspend and resume jobs. (Release 1A; Must)

5.1.2.2.2.3 The system shall provide the capability to cancel a job. (Release 1A; Must)

5.1.2.2.2.4 The system shall provide the capability to adjust the priority of a job at any time. (Release 1A; Must)

5.1.2.2.2.4.1 The system shall provide the capability to adjust the priority of a job manually or automatically.

5.1.2.2.2.5 The system shall provide the capability to log jobs. (Release 1A; Must)

5.1.2.2.2.6 The system shall provide the capability to manage work lists of jobs. (Release 1A; Must)

5.1.2.2.2.7 The system shall provide the capability to perform actions on a batch of jobs. (Release 1A; Must)

5.1.2.3 Workflow - Monitoring

5.1.2.3.1 The system shall provide a monitoring tool for all workflow activities. (Release 1A; Must)

5.1.2.3.1.1 The monitoring tool shall provide the capability to visualize a set of activities. (Release 1A; Must)

5.1.2.3.1.2 The monitoring tool shall provide the capability for the user to customize views. (Release 1A; Could / Release 2; Must)

5.1.2.3.1.3 The monitoring tool shall provide the capability to save customized views for future use. (Release 1A; Could / Release 2; Must)

5.1.2.3.1.4 The monitoring tool shall provide the capability for users to monitor processing history. (Release 1A; Must)

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 1A; Could / Release 2; Must)

5.1.2.3.1.5 The monitoring tool shall report performance measures, including but not limited to: (Release 1A; Must)

- Throughput
- Delay
- Load

5.1.2.3.2 The system shall provide the capability for users to monitor jobs or groups of jobs. (Release 1A; Must)

5.1.2.3.2.1 The system shall provide the capability for users to monitor one or more jobs simultaneously.

5.1.2.3.2.2 The system shall provide the capability to monitor planned, scheduled and actual times for selected jobs.

5.1.2.3.2.3 The system shall provide the capability to group jobs with a defined status.

5.1.2.3.3 The system shall provide the capability for users to monitor activities or groups of activities. (Release 1A; Must)

5.1.2.3.3.1 The system shall provide the capability for users to monitor one or more activities simultaneously.

5.1.2.3.3.2 The system shall provide the capability to monitor planned, scheduled and actual times for selected activities.

5.1.2.3.3.3 The system shall provide the capability to group activities with a defined status.

5.1.2.4 Workflow - Resource Requirements

5.1.2.4.1 The system shall provide the capability to estimate resource requirements associated with internal workflow. (Release 1A; Could / Release 1B; Must)

5.1.2.4.2 The system shall provide the capability to estimate resource requirements associated with external workflow. (Release 1A; Could / Release 1B; Must)

5.1.2.4.3 The system shall provide the capability to estimate resource requirements for automated and manual activities. (Release 1A; Could / Release 1B; Must)

5.1.2.5 Workflow - Notification

5.1.2.5.1 The system shall provide the capability to associate notifications with workflows. (Release 1A; Must)

5.1.2.5.2 The system shall provide the capability to manage notifications attached to workflows. (Release 1A; Must)

5.1.2.5.3 The system shall send notifications including but not limited to e-mail and the user's screen. (Release 1A; Must)

5.1.2.5.4 The system shall provide the capability to configure the list of recipients of notifications. (Release 1A; Must)

5.1.2.5.5 The system shall provide the capability to escalate notifications. (Release 1A; Should)

5.1.2.6 Workflow - Security

5.1.2.6.1 The system shall provide the capability to have security controls on workflow activities. (Release 1A; Must)

5.1.2.6.1.1 The security control (allow or deny actions) shall be rule based. (Release 1A; Must)

5.1.2.6.1.2 Manual activities in the workflows shall be assigned with one or more security rules. (Release 1A; Must)

5.1.2.7 Workflow - User Interface

5.1.2.7.1 The system shall provide a Graphical User Interface (GUI) edit tool to manage workflow definitions and executions. (Release 1A; Must)

5.1.2.7.2 The Monitoring Tool shall contain a GUI for all workflow monitoring capabilities. (Release 1A; Must)

3.2.5.2 Storage Management

Storage management will provide and coordinate access, backup, and archiving of authentic and official Government information as well as ensure data reliability. Storage management will consist of facilities that are scalable and support increasing and changing storage requirements.

Storage Types

- Networked High Performance Storage – High performance, high availability storage.
- Networked Moderate Performance Storage - Moderate performance and availability storage for less critical information.
- Low Criticality - Low Cost Storage - Designed for high storage capacity and low cost, low criticality redundant storage.

- Failover Storage - Separate storage location to allow access to all data in the event of an emergency with primary storage.
- Back-up Retrieval Media Storage - Off-site backup of critical data.
- Mid-term Archival Storage - Moderate capacity of offline storage with archival capabilities for at least 10 years.
- Long-term Permanent Archival Storage - Large capacity of offline storage with archival capabilities for at least 100 years.

Storage Categories

- Work In Progress Storage (WIP)
- Archival Information Storage (AIS)
- Access Content Storage (ACS)
- Business Process Storage (BPS)

	WIP	**AIS**	**ACS**	**BPS**
Networked High Performance Storage	Yes	No	Yes	Yes
Networked Moderate Performance Storage	No	Yes	Yes	Yes
Low Criticality - Low Cost Storage	No	No	Yes	Yes
Failover Storage	Yes	Yes	Yes	Yes
Back-up Retrieval Media Storage	Yes	Yes	Yes	Yes
Mid-term Archival Storage	Yes	No	Yes	Yes
Long-term Permanent Archival Storage	No	Yes	Yes	Yes

3.2.5.2.1 Current Situation

GPO is currently running a Network Appliance NAS FAS940C Cluster in operation. This is the major component in the near term infrastructure according to Infrastructure Management. In general, GPO has a very heterogeneous storage environment across mainframe, Vax, and Unix environments.

3.2.5.2.2 Requirements for Storage Management

5.2.2.1 Storage Core Capabilities

5.2.2.1.1 The system shall support error-free retrieval of data to network storage at rated network speeds (e.g., 2 Gbps). (Release 1A; Must)

5.2.2.1.2 The system shall be capable of providing a secure repository environment for all storage. (Release 1A; Must)

5.2.2.1.3 The system shall provide the ability to move content into and between stores transparently. (Release 1A; Must)

5.2.2.2 Networked High Performance Storage

5.2.2.2.1 Networked High Performance Storage shall have the ability to store data dynamically in high performance-high availability stores and external Content Delivery Networks (CDN) based on hit rate/criticality of content. (Release 1A; Must)

5.2.2.2.1.1 Networked High Performance Storage shall have the capability to manage the threshold hit rate for content to automatically move to the Network High Performance Storage.

5.2.2.2.1.2 Networked High Performance Storage shall have the capability to manage the criticality of specific content for Network High Performance Storage.

5.2.2.2.2 The system shall have the capability to utilize external storage Service Providers. (Release 1A; Must)

5.2.2.2.3 Networked High Performance Storage shall have the capability to support direct application access with latency in application performance less than 1 second. (Release 1A; Must)

5.2.2.2.4 Networked High Performance Storage shall be able to support automated fail-over without buffer application data loss. (Release 1A; Must)

5.2.2.2.5 Networked High Performance Storage shall operate reliably to allow less than 0.1% downtime. (Release 1A; Must)

5.2.2.2.6 Networked High Performance Storage shall have record management capabilities. (Release 1A; Must)

5.2.2.2.7 Networked High Performance Storage shall have redundant components that will take over in the event of a hardware failure in the primary part. (Release 1A; Must)

5.2.2.2.7.1 The system shall allow the switchover to redundant components via either user action or automatic processes.

5.2.2.2.8 Networked High Performance Storage shall be able to support hot-spare standby drives (e.g. extra drives installed in the disk array that automatically come online in the event of a disk failure). (Release 1A; Must)

5.2.2.2.8.1 Networked High Performance Storage shall allow the switchover to redundant components via either user action or automatic in case of failure.

5.2.2.2.9 Networked High Performance Storage shall have a full-system battery backup to allow the disk array to remain operational in the event of a power outage. (Release 1A; Must)

5.2.2.3 Networked Moderate Performance Storage

5.2.2.3.1 Networked Moderate Performance Storage shall support static and dynamic storage assignment. (Release 1A; Must)

5.2.2.3.2 Networked Moderate Performance Storage shall have limited scalability (e.g., multi- tens of terabyte capacities). (Release 1A; Must)

5.2.2.3.3 Networked Moderate Performance Storage shall have open support (control of its resources) for a consolidated storage management back plane. (Release 1A; Must)

5.2.2.3.4 Networked Moderate Performance Storage shall operate reliably to allow less than 0.2% downtime. (Release 1A; Must)

5.2.2.3.5 Networked Moderate Performance Storage shall have the capability to support direct application access with latency in application performance less than 3 seconds. (Release 1A; Must)

5.2.2.4 Low Criticality- Low Cost Storage

5.2.2.4.1 Low Criticality - Low Cost Storage shall support low cost devices (e.g., Serial ATA storage drives). (Release 1A; Must)

5.2.2.4.2 Low Criticality - Low Cost Storage shall allow central control and allocation of storage resources. (Release 1A; Must)

5.2.2.4.3 Low Criticality - Low Cost Storage shall allow RAID 0 thru 5 configurations. (Release 1A; Must)

5.2.2.4.4 Low Criticality - Low Cost Storage shall allow scaling and partitioning. (Release 1A; Must)

5.2.2.4.5 Low Criticality - Low Cost Storage shall operate reliably with less than 0.3% downtime. (Release 1A; Must)

5.2.2.5 Failover Storage

5.2.2.5.1 Failover Storage shall have a fault tolerance-system able to survive local environmental casualties. (Release 1A; Must)

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 1A; Must)

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.

5.2.2.5.3 Failover Storage shall allow RAID 0 thru 5 configurations. (Release 1A; Must)

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 1A; Must)

5.2.2.6 Backup Retrieval Media Storage

5.2.2.6.1 Back-up Retrieval Media Storage shall be able to accomplish periodic backup on mass removable storage media. (Release 1A; Must)

5.2.2.6.1.1 Back-up Retrieval Media Storage shall allow users to manage periodic backup schedules.

5.2.2.6.1.2 Back-up Retrieval Media Storage shall allow backups on multiple types of mass removable storage media.

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 1A; Must)

5.2.2.6.2.1 Back-up Retrieval Media Storage shall allow users to manage which data is listed as critical.

5.2.2.6.2.2 Back-up Retrieval Media Storage shall allow users to manage the backup schedule.

5.2.2.6.2.3 Back-up Retrieval Media Storage shall not interfere with current system processes.

5.2.2.6.3 Back-up Retrieval Media Storage shall have battery backed-up cache (e.g., battery power that protects any data that happens to be in cache at the time of a power interruption). (Release 1A; Must)

5.2.2.6.4 Back-up Retrieval Media Storage shall support mirrored cache (e.g., the process of mirroring the write data in cache as a further method of data protection). (Release 1A; Must)

5.2.2.6.4.1 Back-up Retrieval Media Storage shall allow users to manage which data should be mirrored and where it should be stored.

5.2.2.6.5 Back-up Retrieval Media Storage shall have cache or disk scrubbing (e.g., a method of proactively testing data for errors even when the cache or disk is inactive, so that problems can be detected before they can disrupt data flow). (Release 1A; Must)

5.2.2.6.5.1 Back-up Retrieval Media Storage shall allow users the ability to both schedule and manually scrub disks/caches.

5.2.2.6.6 Back-up Retrieval Media Storage must be able to support remote mirroring, or the process of copying data to a second disk array, often housed in a separate location from the originating disk array. (Release 1A; Must)

5.2.2.7 Mid-term Archival Storage

5.2.2.7.1 Mid-term Archival Storage shall have off-line storage and indexing capability for 100's of Terabytes of data. (Release 1C; Must)

5.2.2.7.2 Mid-term Archival Storage shall preserve data integrity and quality for no less than 10 Years in a data center environment. (Release 1A; Must)

5.2.2.8 Long-term Permanent Archival Storage

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)

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 1A; Must)

5.2.2.8.3 Long-term Permanent Archival Storage site must preserve physical data integrity and quality for no less than 100 Years under controlled storage conditions (e.g., 70° F, 60% Humidity). (Release 1A; Must)

5.2.2.9 Functional Data Storage

5.2.2.9.1 Work In Progress (WIP) Storage (Release 1A; Must)

5.2.2.9.1.1 WIP Storage shall contain Networked High Performance Storage.

5.2.2.9.1.2 WIP Storage shall contain Mid-term Archival Storage.

5.2.2.9.1.3 WIP Storage shall contain Failover Storage.

5.2.2.9.1.4 WIP Storage shall contain Back-up Retrieval Media Storage.

5.2.2.9.1.5 WIP Storage shall contain both content and metadata.

5.2.2.9.2 Archival Information Storage (AIS) (Release 1A; Must)

5.2.2.9.2.1 AIS shall contain Networked Moderate Performance Storage.

5.2.2.9.2.2 AIS shall contain Long-term Permanent Archival Storage.

5.2.2.9.2.3 AIS shall contain Failover Storage.

5.2.2.9.2.4 AIS shall contain Back-up Retrieval Media Storage.

5.2.2.9.2.5 AIS shall exist in isolation of other system stores.

5.2.2.9.2.6 AIS content must remain free from corruption and remain accessible as GPO undergoes changes in information technology and infrastructure.

5.2.2.9.2.7 AIS shall contain both content and metadata.

5.2.2.9.3 Access Content Storage (ACS) (Release 1B; Must)

5.2.2.9.3.1 ACS shall contain Networked High Performance Storage.

5.2.2.9.3.2 ACS shall contain Networked Moderate Performance Storage.

5.2.2.9.3.3 ACS shall contain Low Criticality - Low Cost Storage.

5.2.2.9.3.4 ACS shall contain Mid-term Archival Storage.

5.2.2.9.3.5 ACS shall contain Long-term Permanent Archival Storage.

5.2.2.9.3.6 ACS shall contain Failover Storage.

5.2.2.9.3.7 ACS shall contain Back-up Retrieval Media Storage.

5.2.2.9.3.8 ACS shall contain both content and metadata.

5.2.2.9.4 Business Process Storage (BPS) (Release 1A; Must)

5.2.2.9.4.1 BPS shall contain Networked High Performance Storage.

5.2.2.9.4.2 BPS shall contain Networked Moderate Performance Storage.

5.2.2.9.4.3 BPS shall contain Low Criticality - Low Cost Storage.

5.2.2.9.4.4 BPS shall contain Mid-term Archival Storage.

5.2.2.9.4.5 BPS shall contain Long-term Permanent Archival Storage.

5.2.2.9.4.6 BPS shall contain Failover Storage.

5.2.2.9.4.7 BPS shall contain Back-up Retrieval Media Storage.

5.2.2.10 Storage System Standards

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 1A; Must)

5.2.2.10.2 The system shall support multiple file systems including but not limited to: Windows XP Filesystem, Linux File System, SunOS File System, Solaris Filesystem, Apple, FAT, FAT32, VFAT, NTFS, HPFS, EXT2. (Release 1A; Must)

5.2.2.10.3 The system shall utilize common Redundant Array of Independent Disks (RAID) Disk Data Format (DDF) architecture. (Release 1A; Must)

5.2.2.10.4 The system shall conform to common protocols, including but not limited to: Apple File Protocol (AFP), Network File System (NFS), SMB and CIFS protocols, Simple Network Management Protocol (SNMP), Internet Small Computer Systems Interface (iSCSI), Internet Fibre Channel Protocol (iFCP), Fibre Channel over IP (FCIP), Serial across SCSI (SAS), and Serial ATA. (Release 1A; Must)

5.2.2.10.5 The system shall allow interaction with management information bases (MIB) via SNMP, and must conform to or interoperate within Object-based Storage Device (OSD) specification. (Release 1A; Must)

5.2.2.10.6 The system storage shall support ANSI INCITS 388-2004 Storage Management Initiative Specification. (Release 1A; Must)

5.2.2.10.7 The system back-up tapes shall conform to Linear Tape-Open (LTO) standard. (Release 1A; Must)

5.2.2.11 Storage - Monitoring

5.2.2.11.1 The system shall have the capability to be monitored for real-time health of the system components. (Release 1A; Must)

5.2.2.11.2 Monitoring shall have the capability to have conditional thresholds customized to allow timely preventative maintenance. (Release 1A; Must)

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 1A; Must)

5.2.2.11.3.1 The system shall send notifications including but not limited to notifications on appropriate user screen and e-mail.

5.2.2.11.3.2 The system shall allow for the definition and management of different levels of notification by users.

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 1A; Must)

5.2.2.11.5 The system shall have the ability to monitor data access history and evaluate appropriate storage in terms of cost and performance, in accordance with the FDsys Data Mining requirements. (Release 1A; Must)

5.2.2.11.6 The system shall have the ability to monitor health of externally hosted data stores. (Release 1A; Must)

5.2.2.11.7 The system shall support user configurable RAID levels. (e.g., the ability to configure storage RAID levels in the field without vendor intervention). (Release 1A; Must)

5.2.2.12 Storage - Preventive Action

5.2.2.12.1 The system shall have the ability to have automated preventative actions configured to allow critical failures from causing data loss. (Release 1A; Must)

5.2.2.12.2 The system shall have the ability to allow hot swapping of components should a failure condition be detected. (Release 1A; Must)

5.2.2.12.3 The system shall have the ability to dynamically move data to improve system performance. (Release 1A; Must)

5.2.2.12.4 The system shall be able to execute non-disruptive microcode updates or replacements or the ability to update or replace the RAID controller microcode without having to shut down the disk array. (Release 1A; Must)

5.2.2.13 Storage - Data Integrity

5.2.2.13.1 The system shall allow for securing of partitions. (Release 1A; Must)

5.2.2.13.2 The system shall allow encryption of logical content. (Release 1A; Must)

5.2.2.13.3 The system shall have the capability to limit access to data via role-based security. (Release 1A; Must)

5.2.2.14 Storage - Allocation

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 1A; Must)

5.2.2.14.2 The system shall have capability to have conditional thresholds customized to allow automated reallocation of storage to meet application needs. (Release 1A; Must)

5.2.2.14.3 The system shall be able to allocate any compliant serial drive, and near-line storage devices. (Release 1A; Must)

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 1A; Must)

5.2.2.14.5 The system shall be able to immediately allocate newly added storage assets. (Release 1A; Must)

3.2.5.3 Security

The security functional element provides the appropriate confidentiality, integrity, and availability functions for FDsys information and processes. It also governs access to content (both authentication and authorization), assigning user rights (authorization), and maintaining system security (administration and auditing). Finally, the security element provides mechanisms for the necessary technical, operational, and management controls for FDsys, including interfaces that it will have with other systems.

There are several important metrics for security that are important for FDsys. These include:

1. Number of users
2. Number of documents (digital objects) to be managed
   a. number of objects to manage access authorization controls
3. Number of documents archived
   a. number of documents to ensure they are retained and are not compromised
4. Number of documents harvested from external sites
   a. federal agency sites (documents must be inspected for malicious code (e.g., viruses) before ingested to FDsys)

   b. non-federal agency sites (documents are potentially even less trust worthy than documents from federal agency electronic sources)

5. Number of transactions for content dissemination
   a. financial transactions associated with FDsys operations and content management functions
6. Number of IT systems that make up FDsys
   a. each system will require resources to properly secure for the following aspects:
      i. operating system configuration
      ii. system software patching
      iii. virus scanning and protection

NOTE: These metrics are important to the magnitude of resources required, in terms of personnel, equipment and processing power, required to properly secure FDsys for effective operations.

3.2.5.3.1 Current Situation

Security subsystems are implemented and operational at GPO at both network and application levels. Most security subsystems for GPO applications and business processes are currently stove-piped, with little integration or information sharing between the security levels. Content management, ingest and dissemination are currently controlled from a security perspective as separate elements.

GPO has an existing information technology (IT) and content management environment. Both environments have elements that require significant modernization to facilitate achieving GPO's mission. FDsys must have certain inherent system security capabilities which must be satisfied and work in harmony with the agency IT and IT security environment. The purpose of this document is to describe those capabilities and requirements, and also broadly articulate the ways in which the GPO IT and information security environment will relate to FDsys.

Existing GPO IT Security Environment

The GPO IT and information security environment that FDsys will integrate to has the following major system elements:

1. Network perimeter security systems
   a. Firewalls
2. Network and system intrusion monitoring
   a. Network Intrusion Detection Systems (NIDs)
   b. Host Intrusion Detection Systems (HIDs)
3. Anti-Virus protection and malware (spyware, etc.) protection

4. Vulnerability Assessment system

These systems will provide essential security functions that will serve FDsys.

FDsys Security Environment

FDsys will supply the required application level security capabilities to meet GPO requirements, while the GPO IT environment will supply the required infrastructure level security capabilities.

In general, FDsys will provide the following security capabilities to meet GPO and applicable federal security requirements:

1. Application level security
   a. Application audit logging
   b. Application user access controls
   c. Application authentication controls
   d. Application user administration systems and controls

3.2.5.3.2 Requirements for Security

5.3.2.1 Security - System User Authentication

5.3.2.1.1 The system shall have the capability to authenticate users based on a unique user identity. (Release 1A; Must)

5.3.2.1.1.1 The system shall authenticate system and security administrators.

5.3.2.1.1.1.1 The system shall support user ID and password authentication.

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).

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).

5.3.2.1.2 The system shall permit users to create a unique user identity for access to the system. (Release 1A; Must)

5.3.2.1.2.1 The system shall enforce uniqueness of user identity. No two users shall be allowed to use the exact same user identity.

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.

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.

5.3.2.1.2.3 A user shall only be allowed to manage attributes associated with their own user identity.

5.3.2.1.3 The system shall display a message to users if they fail to authenticate. (Release 1A; Must)

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 1A; Must)

5.3.2.1.5 The system shall verify the identity and authority of the Content Originator. (Release 1A; Must)

5.3.2.2 Security - User Access Control

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 1A; Must)

5.3.2.2.1.1 The system shall permit authorized system administrators to create and assign customized roles. (Release 1A; Must)

5.3.2.2.1.1.1 The system shall provide access control limitations to support data mining (Release 1C; Must).

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 1A; Must)

5.3.2.2.1.3 The system shall allow the use of standards based LDAP technology for the role based access model. (Release 1A; Must)

5.3.2.2.2 The system shall manage user accounts. (Release 1A; Must)

5.3.2.2.3 The system shall provide the capability to create user accounts. (Release 1A; Must)

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.

5.3.2.2.4 The system shall provide the capability to access user accounts. (Release 1A; Must)

5.3.2.2.5 The system shall provide the capability to delete user accounts. (Release 1A; Must)

5.3.2.2.6 The system shall provide the capability to suspend user accounts. (Release 1A; Must)

5.3.2.2.7 The system shall provide the capability to reactivate suspended user accounts. (Release 1A; Must)

5.3.2.2.8 The system shall provide the capability for the renewal of user registrations. (Release 1A; Must)

5.3.2.2.9 The system shall have the capability to expire user accounts. (Release 1A; Must)

5.3.2.2.10 The system shall provide the capability for users to cancel their accounts. (Release 1A; Must)

5.3.2.2.11 The system shall provide the capability for users to update their account information. (Release 1A; Must)

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 1A; Must)

5.3.2.2.13 The system shall securely store personal information (e.g. user names and passwords). (Release 1A; Must)

5.3.2.2.14 The system shall provide the capability for authorized users to manage (add, modify, delete) information. (Release 1A; Must)

5.3.2.2.15 The system shall have the capability to provide secure interfaces for FDsys operations. (Release 1A; Must)

5.3.2.3 Security - Capture and Analysis of Audit Logs

5.3.2.3.1 The system shall keep an audit log of all transactions in the system. (Release 1A; Must)

5.3.2.3.1.1 Audit logs shall contain logged events which each contain: (Release 1A; Must)

- Date - The date the event occurred.
- Time - The time the event occurred.
- Source - The software module 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.
- Category - A classification of the event by the event source.
- Type - 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.
- Event - A number identifying the particular event type.
- User - The user name of the user on whose behalf the event occurred.
- System Name - The name (IP address and DNS name) of the system on which the event occurred.

5.3.2.3.1.2 Audit logs shall contain a description of the event containing the following: (Release 1A; Must)

- Error - Significant problems, such as a loss of data or loss of functions.
- Warning - Events that are not necessarily significant, but that indicate possible future problems.
- Information - Infrequent significant events that describe successful operations of major server services.
- Success Audit - Audited security access attempts that were successful.
- Failure Audit - Audited security access attempts that failed.

5.3.2.3.1.3 Audit logs shall contain additional data fields where binary data can be displayed in bytes or words. (Release 1A; Must)

5.3.2.3.1.4 The system shall maintain a system log containing events logged by the system components. (Release 1A; Must)

5.3.2.3.1.4.1 The system shall allow system logs to be viewed by all authorized users.

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 1A; Must)

5.3.2.3.1.5.1 The system shall allow security logs to be viewed by all authorized users.

5.3.2.3.1.6 The system shall maintain an application log containing events logged by applications. (Release 1A; Must)

5.3.2.3.1.6.1 The system shall allow applications logs to be viewed by all authorized users.

5.3.2.3.1.7 The system shall have an Audit Log manager for system administrator functions. (Release 1A; Must)

5.3.2.3.1.7.1 The Audit Log manager must be searchable.

5.3.2.3.1.8 The system shall have the capability to reconstruct complete transactions. (Release 1A; Must)

5.3.2.3.1.9 The system shall keep an audit log of user ordering (request) transactions. (Release 1A; Must)

5.3.2.3.1.10 The system shall keep an audit log of system administration transactions. (Release 1A; Must)

5.3.2.3.1.11 The system shall keep an audit log of security administrator transactions. (Release 1A; Must)

5.3.2.3.1.12 The system shall keep an audit log of system access rights. (Release 1A; Must)

5.3.2.3.1.13 The system shall keep an audit log of preservation processes. (Release 1C; Must)

5.3.2.3.1.14 The system shall keep an audit log of deposited, harvested and converted content activities. (Release 1A; Must)

5.3.2.3.1.15 The system shall keep an audit log of Content Originator ordering activities. (Release 1C; Must)

5.3.2.3.1.16 The system shall keep an audit log of content authentication activities. (Release 1A; Must)

5.3.2.3.1.17 The system shall keep an audit log of version control activities. (Release 1A; Must)

5.3.2.3.1.18 The system shall keep an audit log of cataloging activities. (Release 1A; Must)

5.3.2.3.1.19 The system shall keep an audit log of support activities (e.g., support status). (Release 1A; Must)

5.3.2.3.1.20 The system shall keep an audit log for data mining. (Release 1C; Must)

5.3.2.3.2 The system shall have the capability to maintain integrity of audit logs. (Release 1A; Must)

5.3.2.3.2.1 It shall not be possible for users to adjust the data in the audit logs.

5.3.2.3.2.2 The system shall detect user attempts to edit audit logs.

5.3.2.3.3 The system shall keep an audit log of attempts to access the system. (Release 1A; Must)

5.3.2.3.3.1 The system shall keep an audit log of any detected breaches of security policy.

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 1A; Must)

5.3.2.3.4.1 The system shall save audit logs as specified in *GPO Publication 825.33*.

5.3.2.4 Security - User Privacy

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 1B; Must)

5.3.2.4.1.1 The system shall conform to guidelines set forth in *GPO Publication 825.33*.

5.3.2.4.1.2 The system shall support compliance outlined in Title 5 USC Sec. 552a (Records maintained on individuals).

5.3.2.4.1.3 The system shall support the capability of maintaining access privacy (e.g., Search, Request).

5.3.2.4.1.4 The system shall support the capability of maintaining support privacy (e.g., user identity).

5.3.2.4.1.5 The system shall support the capability of maintaining Content Originator ordering privacy.

5.3.2.4.1.6 The system shall provide measures that preclude a single authorized administrator from listing a end user's orders.

5.3.2.5 Security - Confidentiality

5.3.2.5.1 The system shall support the capability of maintaining confidentiality of user data (e.g., passwords). (Release 1A; Must)

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.

5.3.2.5.1.1.1 FIPS certified encryption algorithms shall be used to provide confidentiality. Triple DES or AES shall be supported.

5.3.2.5.1.1.2 For symmetric encryption, 128 bit keys are the minimum key length to be used.

5.3.2.5.1.2 The system shall have the capability to provide confidentiality of user data, including user authentication data stored within the system (e.g., passwords).

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 1A; Must)

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.

5.3.2.6 Security - Administration

5.3.2.6.1 The system shall provide an administrative graphical user interface to perform user administration and security administration. (Release 1A; Must)

5.3.2.6.2 The system shall have the capability for authorized security administrators to set and maintain system security policy. (Release 1A; Must)

5.3.2.6.2.1 System security policy parameters shall include, but not be limited to the following:

- authorized user and administrator authentication methods
- minimum password lengths

- authorized encryption algorithms

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 1A; Must)

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 1A; Must)

5.3.2.6.4.1 The system shall provide the capability to support separation of functions between system administrators, policy makers, security administrators and auditors.

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.

5.3.2.6.4.3 The system shall provide the capability to limit security administrator's authority to assigned logical elements.

5.3.2.7 Security - Availability

5.3.2.7.1 The system shall provide appropriate backup and redundant components to ensure availability to meet customer and GPO needs. (Release 1A; Must)

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 1A; Must)

5.3.2.7.1.1.1 The system shall return to normal operations post-disaster.

5.3.2.7.1.2 The system shall adhere to GPO's Continuity of Operations (COOP) plans. (Release 1A; Must)

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*.

5.3.2.7.1.2.2 The system shall adhere to guidelines set forth in *Federal Preparedness Circular 65*.

5.3.2.7.1.3 The system shall have appropriate failover components. (Release 1A; Must)

5.3.2.7.1.4 The system shall be operational at appropriate GPO alternate facilities. (Release 1A; Must)

5.3.2.7.1.5 The system shall back up system and data at a frequency as determined by business requirements. (Release 1A; Must)

5.3.2.7.1.5.1 The system applications and data shall be backed up at off-site storage location.

5.3.2.7.1.6 The system shall interface with designated GPO Service Providers (e.g. Oracle). (Release 1A; Must)

5.3.2.7.1.7 The system shall maintain data integrity during backup processing. (Release 1A; Must)

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 1A; Must)

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 1A; Must)

5.3.2.7.1.9.1 Mutually authenticated, high speed connection between GPO offices and hosting site shall be utilized.

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.

5.3.2.8 Security - Integrity

5.3.2.8.1 The system shall have the capability to assure integrity of business process information (BPI). (Release 1A; Must)

5.3.2.8.2 The system shall check content for malicious code (e.g., worms and viruses) prior to ingest to maintain system integrity. (Release 1A; Must)

5.3.2.8.2.1 If malicious code is detected in content, it shall be placed into a quarantine area for GPO inspection.

5.3.2.9 Security Standards

5.3.2.9.1 The system must have the capability to support the following industry integrity standards. (Release 1A; Must)

- RSA Digital Signature in accordance with IETF RFC 3447.
- Public Key Infrastructure (PKI).
- International Telephone Union (ITU) X.509.
- Public Key Infrastructure Exchange (PKIX).
- Message Authentication Code (MAC).
- Cyclical Redundancy Checking (CRC).
- FIPS 180-2 Secure Hash Algorithm (SHA)

5.3.2.9.2 The system must have the capability to support the following confidentiality standards. (Release 1A; Must)

- FIPS 197 Advanced Encryption Standard (AES)

- ANSI X9.52 Triple Data Encryption Standard (TDES)
- Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

5.3.2.9.3 The system must have the capability to support the following access control standards. (Release 1A; Must)

- Lightweight Directory Access Protocol (LDAP) Internet Engineering Task Force (IETF) Request for Comments (RFC) 2251
- International Telephone Union (ITU) X.500
- Security and Access Markup Language (SAML)

3.2.5.4 Enterprise Service Bus

The system shall consist of many internal individual functional elements (i.e. services), each specializing in a business functional area. The system shall also provide the capability to interact with external applications. The concept of the Enterprise Service Bus (ESB) is the preferred approach and shall be employed to facilitate flexible and scalable integrations between the services and applications.

The system shall provide the capability to plug-in services or applications deployed in different hardware and software platforms. The interoperability is facilitated by the underlying integration infrastructure – the ESB. The system shall provide the capability to add, replace or remove service components declaratively via configurations in XML. The system shall provide the administrative GUI tool to manage the integrated internal and external service components.

The ESB is a relatively new technology in the enterprise integration field. It is standards based, depending heavily on XML, and related Extensible Stylesheet Language Transformations (XSLT), XPath and XQuery technologies. Because of its flexibility and capability to enable a highly scalable system, it has become a preferred approach to build the Service-Oriented Architecture in enterprise applications.

3.2.5.4.1 Current Situation

GPO has recently set up the beginning stages of an ESB with the FedEx Kinkos Convenience Printing project, which is part of the GPOExpress initiative. Through this ESB, information is received from Kinkos and is input into the ESB where it is saved in a persistent store in native XML. The fields are then transformed and transported via FTP to the mainframe. Eventually, the ESB will also be setup to talk to Oracle for billing processes. Oracle functionality should be ready in the near future.

3.2.5.4.2 Requirements for Enterprise Service Bus

5.4.2.1 ESB Core Capabilities

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 1A; Must)

5.4.2.1.1.1 The supported operating systems shall include: Microsoft Windows Server 2003 and higher versions, Linux (Red Hat Enterprise Advanced Server 2.1 and above), Solaris 9 and above, Apple OS X.2 and above.

5.4.2.1.1.2 The supported programming languages shall include: C/C++, J2EE, .NET in C#. PERL, Python.

5.4.2.1.2 The system shall provide the capability to integrate internal and external services or applications. (Release 1A; Must)

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 1A; Must)

5.4.2.1.4 The system shall provide the capability to integrate existing (or legacy) services or applications. (Release 1A; Must)

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 1A; Must)

5.4.2.1.6 The system shall provide the capability to support synchronous and asynchronous communications between services or applications. (Release 1A; Must)

5.4.2.1.6.1 The system shall provide the capability to queue communications between services and applications.

5.4.2.1.7 The system shall provide the capability to run process transactions. (Release 1A; Must)

5.4.2.1.7.1 The system shall provide the capability to manage process transactions declaratively via system configurations.

5.4.2.1.7.2 The system shall provide the capability to execute pre-defined process transactions.

5.4.2.1.7.3 The system shall provide the capability to manually commit and roll back process transactions.

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 1A; Must)

5.4.2.1.8.1 The system shall provide the capability to validate communications against the appropriate published schema.

5.4.2.1.8.2 The system shall provide the capability to transform communications to different published schemas.

5.4.2.1.9 The system shall provide the capability to perform XML document-based routing between services or applications. (Release 1A; Must)

5.4.2.1.10 The system shall provide the capability to support incremental implementations. (Release 1A; Must)

5.4.2.1.11 The system shall provide the capability to support exception handling. (Release 1A; Must)

5.4.2.1.11.1 The system shall provide the capability to generate compensating transactions for exceptions where possible. (Release 1B; Should)

5.4.2.1.12 The system shall store information related to the ESB in metadata. (Release 1A; Must)

5.4.2.1.12.1 The system shall store information about schemas in metadata.

5.4.2.1.12.2 The system shall store information about transactional operations in metadata.

5.4.2.1.12.3 The system shall store information about communications in metadata.

5.4.2.1.12.4 The system shall store information about business processes in metadata.

5.4.2.2 ESB Configuration

5.4.2.2.1 The system shall provide the capability to perform integration configurations. (Release 1A; Must)

5.4.2.2.1.1 The system shall provide the capability to perform integration configurations in XML.

5.4.2.2.2 The system shall provide the capability to add redundancy to critical ESB functions. (Release 1A; Must)

5.4.2.3 ESB Administration

5.4.2.3.1 The system shall provide the capability to impose rule-based security control over administrative tasks. (Release 1A; Must)

5.4.2.3.2 The system shall provide the capability to manage services or applications dynamically. (Release 1A; Must)

5.4.2.3.3 The system shall provide the capability to enable and disable services dynamically. (Release 1A; Must)

5.4.2.3.4 The system shall provide the capability to manage business processes. (Release 1A; Must)

5.4.2.3.5 The system shall provide the capability to terminate, suspend and resume business processes. (Release 1A; Must)

5.4.2.3.6 The system shall provide the capability to monitor ESB processes. (Release 1A; Must)

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.

5.4.2.3.6.2 The system shall provide the capability to monitor communication latencies.

5.4.2.3.6.3 The system shall provide the capability to send notifications in the event of problems with ESB functions.

5.4.2.4 ESB User Interface

5.4.2.4.1 The system shall provide the capability to perform configuration tasks via a Graphical User Interface (GUI) tool. (Release 1A; Must)

5.4.2.4.2 The system shall provide the capability to perform administrative tasks via a GUI tool. (Release 1A; Must)

3.2.5.5 Data Mining

Data mining consists of the tools and processes for the extraction, analysis, and presentation of business process information (BPI), content metadata, and system metadata to enhance internal and external business efficiencies. BPI is administrative, non-content specific information that is used within the business process and package description to support access aids and data mining. Content metadata is descriptive, technical, structural, administrative, and preservation information about content. System metadata is data generated by the system that records jobs, processes, activities, and tasks of the system.

GPO will provide intuitive data mining capabilities, including access to selected external data repositories (e.g., Oracle). The data mining functional element will need to extract and analyze information from all GPO Systems.

FDsys will be able to capture the use history of various dissemination tools (e.g., access and downloads from Web sites and databases, the path users took through the site), subject to privacy and legal restrictions. The ability to track monetary transactions will also be required.

The data mining resources of the FDsys will allow for the following:

- Extracting BPI in multiple formats from the entire collection.
- Normalizing data based on administrator defined parameters (e.g., identify missing values or metadata, data formats, types and discrepancies, anomalies).
- Performing multirelational analyses on BPI (e.g., cross tabulations, categorization, clusterization, regression analysis, data patterns and relationships).
- Presenting BPI according to user preferences and GPO business rules (e.g., views based on access levels, exporting of results, linking of results to data).

- Mining BPI within the system at multiple levels of aggregation and granularity (e.g., Service Provider performance history, customer agency billing information, ordering habits, preferences of customers and users).
- Predicting future trends (visualization capability) in order to adjust workflow or anticipate demand.

3.2.5.5.1 Current Situation

GPO uses various disparate systems and methods to collect and analyze business process information. Access to a particular data repository is sometimes limited by geography, and few systems are able to share data. The current methods of data collection and analysis are discussed below by the user class the activity supports.

Public End Users

In order to track the success of online dissemination efforts, GPO uses analysis of log files to track the number of document downloads from GPO Access Web pages and databases, as well as the number and types of referrals to GPO Access Web pages from external Web sites. Some of these reports are distributed to library partners and other Federal government agencies.

GPO is able to track sales through the GPO Sales Program with a mainframe system tied to order processing systems, which tracks sales from orders received through the Web, telephone, mail, and fax. For online orders, a daily cumulative file is uploaded that contains all data from orders received from the U.S. Government Online Bookstore. However, with the current manual order processing and the various databases in use within Customer Service and Plant Operations, automated methods of gathering extensive information about agency customers are lacking.

GPO also collects information relating to depository distribution of titles in electronic only and tangible formats. A monthly report includes listings of classes broken up into the following reports: Lists of Classes in All Formats, Electronic Only Classes, Classes Available in Multiple Formats, and Added and Dropped Classes.

Content Originating Agencies

GPO’s content originating agency ordering information is organized in GPO's Procurement Integrated Control System (PICS), which transfers data to and receives data from various databases. The information stored in PICS can be accessed agency-wide. GPO Central Office is currently working with GPO Procurement (GPOPROC) Web-based specification writing system.

Various Regional Printing Procurement Offices use MS Access databases to generate specifications, print orders, and purchase orders. Search capabilities using MS Access at the local level can provide specific information (Product Titles, Ordering History, Specific Product Descriptions). Other offices cannot readily access all of this information on the network because only a portion is transferred to PICS. Regional Printing Procurement Offices also have an existing decentralized configuration consisting of one primary and one backup server in each office. These servers run the same databases but are not connected. Due to the current workflow at all offices, in which orders originate and are processed from hard copy into localized databases, large-scale interfacing is not possible.

When Content Originating agencies submit orders to GPO, Service Specialists manually input the information into PICS, MS Access, and GPOPROC. Agencies want GPO to accept and process data directly from their systems, which will eliminate redundant key-stroking and improve efficiency.

Plant Operations uses a Work In Progress system and a Production Estimating Planning System to track workflow of print jobs.

GPO has an inventory of more than a hundred mainframe-generated reports. An example of these reports is the Billing Address Code (BAC) report, which lists the Requisition number, Jacket number, program/print order number, actual billing amount for each order, and total orders with billed amount. Another example is the Cumulative Award Stats report, which provides total awards for offices, dollar amount, contractors, and term contract statistics.

3.2.5.5.2 Requirements for Data Mining

5.5.2.1 Data Mining - Data Extraction

5.5.2.1.1 The system shall be capable of extracting data from the entire collection of BPI. (Release 1C; Must)

5.5.2.1.2 The system shall be capable of extracting data from the entire collection of metadata. (Release 1C; Must)

5.5.2.1.3 The system shall be capable of extracting data from select GPO data sources (e.g., Oracle). (Release 1C; Must)

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)

5.5.2.1.5 The system shall be able to extract data according to user parameters (e.g., date range, action type). (Release 1C; Must)

5.5.2.1.6 The system shall be able to extract random samples of data. (Release 1C; Could / Release 2; Must)

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)

5.5.2.1.7.1 The system shall allow users to upload files from which data will be extracted for analysis.

5.5.2.1.7.2 The system shall allow users to enter data.

5.5.2.1.7.3 The system shall allow users to restrict access to supplemental data.

5.5.2.1.7.4 The system shall allow users to store supplemental data for future use.

5.5.2.1.8 The system shall be capable of extracting data from multiple formats (e.g., XML, PDF, XLS). (Release 1C; Must)

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)

5.5.2.2 Data Mining - Data Normalization

5.5.2.2.1 The system shall be able to normalize data based on administrator defined parameters, including but not limited to: (Release 1C; Must)

5.5.2.2.1.1 The system shall be able to identify missing values or metadata elements.

5.5.2.2.1.2 The system shall be able to identify data anomalies in BPI and metadata.

5.5.2.2.1.3 The system shall be able to identify data formats.

5.5.2.2.1.4 The system shall be able to identify format discrepancies.

5.5.2.2.1.5 The system shall be able to identify standard data elements.

5.5.2.2.1.6 The system shall be able to identify data types.

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 1C; Must)

5.5.2.3 Data Mining - Data Analysis and Modeling

5.5.2.3.1 The system shall be able to perform single variable and multivariable analysis operations on extracted data. (Release 1C; Must)

5.5.2.3.1.1 The system shall be able to calculate averages (mean, median, mode). (Release 1C; Must)

5.5.2.3.1.2 The system shall be able to perform cross tabulations. (Release 1C; Could / Release 2; Must)

5.5.2.3.1.3 The system shall be able to perform clusterization. (Release 1C; Could/ Release 2; Must)

5.5.2.3.1.4 The system shall be able to perform categorization. (Release 1C; Could/ Release 2; Must)

5.5.2.3.1.5 The system shall be able to perform association and link analyses. (Release 1C; Could/ Release 2; Must)

5.5.2.3.1.6 The system shall be able to perform regression analysis. (Release 1C; Could / Release 2; Must)

5.5.2.3.1.7 The system shall be able to expose hierarchical or parent/child relationships. (Release 1C; Could/ Release 2; Must)

5.5.2.3.1.8 The system shall be able to expose sequential relationships and patterns. (Release 1C; Could/ Release 2; Must)

5.5.2.3.1.9 The system shall be able to expose temporal relationships and patterns. (Release 1C; Could/ Release 2; Must)

5.5.2.3.1.10 The system shall be able to expose inferences and rules that led to a result set. (Release 1C; Should / Release 2; Must)

5.5.2.3.2 The system shall be able to prompt users attempting illogical operations (e.g., calculating averages out of categorical data). (Release 1C; Could)

5.5.2.3.2.1 The system shall be capable of showing the user the rule violation that led to the prompt of the operation.

5.5.2.3.3 The system shall allow users to suspend, resume, or restart analysis (Release 1C; Should / Release 2; Must)

5.5.2.3.4 The system shall be capable of providing the user with an estimated analysis time. (Release 1C; Could)

5.5.2.4 Data Mining - Report Creation and Data Presentation

5.5.2.4.1 The system shall be able to produce reports summarizing the analysis of BPI and metadata. (Release 1C; Must)

5.5.2.4.1.1 The system must allow users to choose from the data types available in BPI and metadata and choose operations performed on that data.

5.5.2.4.1.2 The system must be able to produce a report summarizing system usage for a user-defined time range.

5.5.2.4.1.3 The system must be able to produce a report analyzing the usage of search terms.

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)

5.5.2.4.3 The system shall allow a set of default report templates to be accessible for each user class. (Release 1C; Must)

5.5.2.4.3.1 The system shall allow System Administrators to manage the default templates.

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)

5.5.2.4.5 The system shall be capable of real-time population of report templates. (Release 1C; Should / Release 2; Must)

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)

5.5.2.4.6.1 The system shall allow users to request notification that a scheduled report is available.

5.5.2.4.6.2 The system shall enable GPO users to restrict view/modify access to customized report templates.

5.5.2.4.7 The system shall be capable of delivering reports to users. (Release 1C; Could / Release 2; Must)

5.5.2.4.7.1 The system shall allow users to specify delivery method (e.g., e-mail, RSS, FTP).

5.5.2.4.8 The system shall be capable of supporting real-time reporting. (Release 1C; Should / Release 2; Must)

5.5.2.4.9 The system shall allow users to create alerts or notifications based on real-time analysis of BPI or metadata. (Release 1C; Should / Release 2; Must)

5.5.2.4.10 The system shall be able to link analysis results to data. (Release 1C; Could)

5.5.2.4.11 The system shall be able to expose analysis criteria and algorithms. (Release 1C; Could)

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 1C; Must)

5.5.2.4.13 The system shall support customization and personalization functions as defined in the FDsys access, search, request, user interface, cataloging and reference tools, and user support requirements. (Release 1C; Must)

5.5.2.5 Data Mining - Security and Administration

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 1A; Must)

5.5.2.5.2 The system shall log all user interactions with the system in metadata. (Release 1A; Must)

5.5.2.5.2.1 Whenever possible, each log entry shall include at least the user identification, user class, date, time, action, and referring page, subject to GPO privacy rules.

5.5.2.5.3 The system shall log all processes in metadata. (Release 1A; Must)

5.5.2.5.4 The system shall perform records management functions on logs. (Release 1A; Must)

5.5.2.6 Data Mining - Storage

5.5.2.6.1 The system shall store extracted data. (Release 1C; Must)

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.

5.5.2.6.2 The system shall store metadata, supplemental data, reports, report templates, analysis criteria, and algorithms in Business Process Storage. (Release 1A; Must)

5.5.2.6.2.1 The system shall have a records management process (e.g., delete files and reports at a defined time).

3.2.6 CONTENT SUBMISSION

Content submission accepts digital content and creates compliant SIPs for ingest into the system. Digital content includes:

- Deposited content: content intentionally submitted to GPO by Content Originators
- Harvested content: content within the scope of dissemination programs that is gathered from Federal agency websites
- Converted content: digital content created from a tangible product

Content submission also includes toolsets for creating, collaborating, and approving content. These toolsets are referred to as style tools.

Content submission also includes a system interface for Content Originators referred to as Content Originator ordering. Content Originators may submit content, order and re-order content, and specify delivery of content through Content Originator ordering.

3.2.6.1 Requirements for Content Submission

6.1.1 Content Submission Core Capabilities

6.1.1.1 The system shall accept digital content and metadata. (Release 1A; Must)

6.1.1.2 The system shall create a SIP from content and metadata. (Release 1A; Must)

6.1.2 Content Submission - System Administration

6.1.2.1 The system shall have the capability to accept and process encrypted files. (Release 2; Could)

6.1.2.2 The system shall provide notification to the submission agency/authority that the content has been received. (Release 1A; Must)

6.1.2.3 The system shall provide notification to the submission agency/authority that the content has been released. (Release 1A; Could / Release 1B; Must)

6.1.2.4 The system shall identify files with security restrictions upon submission. (Release 1A; Must)

6.1.2.4.1 Information about the files will be recorded in metadata.

- Content Originator

- Reason for exception
- Date of exception
- Follow-up action

6.1.2.5 The system shall identify content that has copyright limitations. (Release 1A; Must)

6.1.2.5.1 Copyright information will be recorded in metadata.

6.1.2.6 The system shall provide WIP storage for content prior to ingest. (Release 1A; Must)

6.1.2.7 The system shall check content prior to ingest. (Release 1A; Must)

6.1.2.7.1 Content must be checked for malicious code (e.g., viruses).

6.1.2.7.1.1 In case of a virus or other malicious code, content will follow processes as described in the FDsys security requirements.

6.1.2.7.2 Zipped files (.zip) shall be unzipped.

6.1.2.7.3 Stuffed files (.sit) shall be unstuffed.

6.1.2.8 The system shall accept content with specialized character sets (e.g., non-Roman, scientific notations). (Release 1A; Must)

6.1.3 Content Submission Metadata

6.1.3.1 The system shall accept all administrative and descriptive metadata supplied by the submission agency/authority. (Release 1A; Must)

6.1.3.1.1 The system shall provide the capability to record Title or caption of content.

6.1.3.1.2 The system shall provide the capability to record content identifiers assigned to content including but not limited to:

- Persistent names
- Filenames
- ISBN/ISSN
- Agency requisition numbers

6.1.3.1.3 The system shall provide the capability to record Author/Creator of the content.

6.1.3.1.4 The system shall provide the capability to record Publisher/Authority of the content.

6.1.3.1.5 The system shall provide the capability to record Rights Owner of the content.

6.1.3.1.6 The system shall provide the capability to record version information of the content.

6.1.3.1.7 The system shall provide the capability to record relationships between content packages and digital objects.

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).

6.1.3.1.8 The system shall provide the capability to record content description information (e.g., abstract, summary).

6.1.3.1.9 The system shall provide the capability to record Structure Information of the content.

6.1.3.1.10 The system shall provide the capability to record Intended Output of the content.

6.1.3.1.11 The system shall provide the capability to record Intended Audience of the content.

6.1.3.1.12 The system shall provide the capability to record 13 Digit ISBN Numbers to content.

6.1.3.2 The system shall accept and capture the following elements when available and applicable. (Release 1A; Must)

6.1.3.2.1 Elements relating to documents including but limited to: (Release 1A; Must)

- Software applications and versions used to create the digital objects (e.g., InDesign 3.0, Photoshop 9.0)
- Publication size (e.g., page size)
- Trim size
- Number of pages
- File formats
- File sizes
- Fonts
  - Furnished or embedded
  - Font types (PostScript Type 1, TrueType, OpenType)
- Color mode(s) used (RGB, CMYK [Four Color Process], Spot Colors [Pantone, TOYO], Grayscale, Black and white, Multi-tone [e.g., duotone, tri-tone])
- Bleed required/provided for
- Construction information (e.g., pockets, tabs, die cuts)
- Image resolutions

- Language (e.g., English, Spanish)
- File compression

6.1.3.2.2 Elements relating to audio including but limited to: (Release 1A; Must)

- File formats
- File sizes
- Audio playing time
- Language (e.g., English, Spanish)
- File compression

6.1.3.2.3 Elements relating to video including but limited to: (Release 1A; Must)

- File formats
- File sizes
- Closed captioning
- Video runtime
- Video encoding scheme
- Language (e.g., English, Spanish)
- File compression

6.1.3.2.4 Elements relating to other formats to be determined (Release 1A; Must)

3.2.6.2 Deposited Content

Deposited content is content intentionally submitted to GPO by Content Originators. The Submission Information Package (SIP) for deposited content will include the digital object received from the Content Originator as well as corresponding customer processing requirements and additional metadata.

GPO will identify and utilize best practices for preparing and submitting deposited content, including metadata to capture all the customers' requirements. FDsys must be able to accept all content submitted by Content Originators, including content furnished in proprietary formats. FDsys must be able to assemble content into a compliant SIP for ingest into the system.

3.2.6.2.1 Current Situation

GPO recommends that agencies follow the best practices outlined in GPO Publication 300.6. GPO currently accepts files from agencies in any format including content created using professional desktop publishing applications, word processors, spreadsheets, and databases. The majority of content is submitted to GPO for hard copy output.

3.2.6.2.2 Requirements for Deposited Content

6.2.2.1 Deposited Content Core Capabilities

6.2.2.1.1 The system shall accept digital content and metadata provided by Content Originators. (Release 1A; Must)

6.2.2.1.2 The system shall have the capability to inform Content Evaluators that new content has been submitted. (Release 1A; Must)

6.2.2.2 Deposited Content Metadata

6.2.2.2.1 The system shall accept “approved for release” information provided by the content originating agency. (Release 1A; Must)

- Approver authority name, agency, and contact information
- Submission date and time
- Content release date and time

6.2.2.3 Deposited Content User Interfaces

6.2.2.3.1 Deposited content user interface shall enable Congressional Content Originators and Agency Content Originators to: (Multiple Releases; Must)

6.2.2.3.1.1 Submit digital content and metadata (Release 1A; Must)

6.2.2.3.1.2 Submit content chain of custody information to the system (Release 1A; Must)

6.2.2.3.1.3 Submit intended use information to the system (Release 1A; Must)

6.2.2.3.1.4 Submit “approved for release” information (Release 1A; Must)

6.2.2.3.1.5 Receive notification of receipt of content and content ID (Release 1A; Must)

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 1A; Must)

6.2.2.3.1.7 Receive notification of release of content (Release 1B; Must)

6.2.2.3.1.8 Support Content Originator ordering (Release 1C; Must)

6.2.2.3.2 Deposited content user interface shall enable GPO Service Providers and external Service Providers to: (Multiple Releases; Must)

6.2.2.3.2.1 Submit digital content and metadata (Release 1A; Must)

6.2.2.3.2.2 Receive notification of receipt of content and content ID (Release 1A; Must)

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 1A; Must)

6.2.2.3.2.4 Support Content Originator ordering (Release 1C; Must)

3.2.6.3 Converted Content

Converted content is digital content created from a tangible product. Tangible publications are defined for products such as ink-on-paper, microforms, CD-ROM, or DVDs, characterized by content recorded or encoded on a physical substrate. The digital collection created from this process will be made available to the public for permanent public access through GPO's dissemination programs. In addition to GPO's efforts, the agency will continue to work with various user communities including Federal agencies, the Library of Congress, National Archives and Records Administration (NARA) and the library community on digitizing a comprehensive collection of legacy materials.

In addition to traditional scanning, other techniques of digitization currently exist and could evolve in the future. There may also be instances in which a successful conversion and/or Optical Character Recognition (OCR) for a given tangible legacy document becomes improbable or impossible due its physical condition and/or characteristics. In these cases, it may be most practical to manually recreate these documents (e.g. using manual text encoding).

GPO recognizes that non-text based formats also exist in the legacy collection. These formats include analog audio and video. Specifications will be developed on a case-by-case basis for the creation of these files.

The desired outcome of the conversion process will be to produce a Submission Information Package (SIP) that includes the electronic preservation master files and submission level metadata that will be ingested into FDsys. Specific SIP functional requirements are outlined in Appendix B: Operational Specification for Converted Content.

3.2.6.3.1 Current Situation

The objective of the current situation is to establish a prototype conversion activity to develop workflow processes and metrics to create all conversion elements that are required for the creation of a SIP. Known as Release 0, this evolving converted content workflow is a manual process to date.

3.2.6.3.2 Requirements for Converted Content

6.3.2.1 Converted Content Core Capabilities

6.3.2.1.1 The system shall accept digital content and metadata provided by converted content processes. (Release 1A; Must)

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.

6.3.2.2 Converted Content User Interface

6.3.2.2.1 Converted content user interface shall enable GPO Service Providers and external Service Providers to: (Multiple Releases; Must)

6.3.2.2.1.1 Submit approved content, metadata, and BPI (Release 1A; Must)

6.3.2.2.1.2 Receive notification of receipt of content and content ID (Release 1A; Must)

6.3.2.2.1.3 Provide notification of release of content (Release 1B; Must)

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 1A; Must)

6.3.2.2.1.5 Manage converted content (Release 1A; Must)

3.2.6.4 Harvested Content

Harvested content is content within the scope of dissemination programs that is gathered from Federal agency Web sites. Discovery, assessment, and harvesting tools will be used to harvest in-scope content, and will collectively be referred to as the “harvester” in this document.

The harvester will consist of discovery, assessment, and harvesting tools. The discovery tools will locate electronic content from targeted Web sites and provide information to the assessment tool. The assessment tool determines if the discovered content is within the scope of GPO dissemination programs, and whether other versions of the content already exist in the system. The assessment tool also identifies the applicable relationships between versions. The harvesting tool gathers content and available metadata.

3.2.6.4.1 Current Situation

Over the past few years, GPO has become increasingly aware that many publications being published by Federal agencies are not being included in the Federal Depository Library Program (FDLP). These documents have come to be known as “fugitive publications.” With increasing frequency, agencies are publishing information only in electronic formats and, when this occurs, they frequently fail to inform GPO of these new publications for inclusion in the FDLP and National Bibliography. In addition, agencies sometimes procure their printing directly from private sector companies or use in-house facilities and fail to inform GPO of these publications, In light of the large number of publications that have become fugitive, GPO will implement a set of automated tools that will identify and harvest fugitive documents and publications from agency Web sites.

GPO's Web harvesting has been a largely manual process to date. For the past few years, GPO has used tools to capture copies of targeted digital publications on Federal agency Web sites. The harvested copy is downloaded and sent to an archive server. GPO maintains full control of the harvested content and metadata in the archive and controls access privileges and mechanisms.

3.2.6.4.2 Requirements for Harvested Content

6.4.2.1 Harvested Content Core Capabilities

6.4.2.1.1 The system shall accept digital content and metadata delivered by the harvesting function. (Release 1A; Must)

6.4.2.2 Harvested Content Metadata

6.4.2.2.1 The system shall provide the capability to record the date and time of harvest of content. (Release 1A; Must)

6.4.2.3 Harvester Requirements

6.4.2.3.1 The harvester shall have the capability to discover, assess, and harvest in-scope content from targeted Web sites. (Release 1B; Must)

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 1B; Could / Release 2; Must)

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 1B; Could / Release 2; Must)

6.4.2.3.4 The harvester shall have capability to perform simultaneous harvests. (Release 1B; Must)

6.4.2.3.5 The harvester shall locate and harvest all levels of Web pages within a Web site. (Release 1B; Must)

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 1B; Should / Release 2; Must)

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 1B; Must)

6.4.2.3.8 The harvester shall stop the discovery process when a linked Web page does not contain in-scope content. (Release 1B; Should / Release 2; Must)

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 1B; Must)

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 1B; Must)

6.4.2.3.11 The harvester shall collect in-scope discovered content and available metadata. (Release 1B; Must)

6.4.2.3.11.1 The harvester shall deliver all in-scope content and metadata to WIP storage.

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.

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 1B; Must)

6.4.2.3.13 The harvester shall have the ability to maintain the directory structure of Web sites that constitute entire publications. (Release 1B; Must)

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 1B; Must)

6.4.2.3.15 The harvester must be able to harvest hidden Web information. (Release 1C; Could / Release 2; Must)

6.4.2.3.15.1 The harvester must be able to harvest content contained in query-based databases.

6.4.2.3.15.2 The harvester must be able to harvest content contained in agency content management systems.

6.4.2.3.15.3 The harvester must be able to harvest content contained on dynamically generated Web pages.

6.4.2.3.15.4 The harvester must be able to harvest content contained on FTP servers.

6.4.2.3.15.5 The harvester must be able to harvest content contained behind proxy servers.

6.4.2.3.15.6 The harvester must be able to harvest content contained behind firewalls.

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: (Release 1B; Must)

- 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.

6.4.2.3.17 The harvester shall have the capability to time and date stamp content that has been harvested. (Release 1B; Must)

6.4.2.4 Metadata Requirements for Harvester

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 1B; Must)

6.4.2.4.2 The harvester shall have the ability to locate and collect unique ID and title/caption information. (Release 1B; Must)

6.4.2.4.3 The harvester shall have the ability to locate and collect author/creator, publisher/authority, and rights owner information. (Release 1B; Must)

6.4.2.4.4 The harvester shall have the ability to locate and collect topical information and bibliographic descriptions. (Release 1B; Must)

6.4.2.4.5 The harvester shall have the ability to locate and collect version, fixity, relationship, and provenance information. (Release 1B; Must)

6.4.2.4.6 The harvester shall have the ability to locate and collect technical, structural, file format, packaging and representation information. (Release 1B; Must)

6.4.2.4.7 The harvester shall have the ability to locate and collect administrative metadata. (Release 1B; Must)

6.4.2.4.8 The harvester shall have the capability to record the time and date of harvest. (Release 1B; Must)

6.4.2.5 Harvester Rules and Instructions

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 1B; Must)

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 1B; Must)

6.4.2.5.3 The harvester must be able to create and store rule and instruction profiles for individual targeted Web sites. (Release 1B; Could / Release 2; Must)

6.4.2.6 Harvester User Interface

6.4.2.6.1 The harvester shall provide a user interface to accommodate workflow management and scheduling of harvesting activities. (Release 1B; Must)

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 1B; Must)

6.4.2.6.2.1 Must accommodate the scheduling of harvests, including but not limited to hourly, daily, weekly, biweekly, monthly, and yearly.

6.4.2.6.3 The user interface must be able to manage rule and instruction profiles. (Release 1B; Could / Release 2; Must)

6.4.2.7 System Administration for Harvester

6.4.2.7.1 The harvester shall provide quality control functions to test accuracy/precision of rule application. (Release 1B; Could / Release 2; Must)

6.4.2.7.2 The harvester shall be able to incorporate results of quality control functions into rule and instruction creation/refinement. (Release 1B; Could / Release 2; Must)

6.4.2.7.3 The harvester shall have the capability to log and produce reports on harvesting activities.

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 1B; Must)

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 1B; Must)

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 1B; Must)

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 1B; Must)

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 1B; Must)

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 1B; Could / Release 2; Must)

6.4.2.7.4 The discovery and harvesting tools shall have the ability to identify GPO as the owner of the tools. (Release 1B; Must)

6.4.2.7.5 The harvester’s method of identification shall not be intrusive to targeted Web site. (Release 1B; Must)

6.4.2.7.6 The harvester shall have the ability to collect integrity marks associated with content as it is being harvested. (Release 1B; Must)

3.2.6.5 Style Tools

Style tools will allow Content Originators to prepare content in pre-ingest processing. The goal of style tools is to move GPO upstream in the content origination process. Style tools accept content and provide composition, collaboration, and approval tools.

3.2.6.5.1 Current Situation

GPO currently accepts files from agencies in any format including content created using professional desktop publishing applications, word processors, spreadsheets, and databases. The majority of content is submitted to GPO in .qxd (QuarkXPress), .ind (Adobe InDesign), .doc (Microsoft Word), and .pdf (Adobe Acrobat) formats.

3.2.6.5.2 Requirements for Style Tools

6.5.2.1 Style Tools Core Capabilities

6.5.2.1.1 Style tools shall accept content from authorized Content Originators, Service Providers, and Service Specialists for document creation. (Release 1C; Could / Release 3; Must)

6.5.2.1.2 Style tools shall accept metadata from authorized users (e.g., title, author). (Release 1C; Could / Release 3; Must)

6.5.2.1.3 Style tools shall provide the capability for users to create new content for document creation. (Release 1C; Could / Release 3; Must)

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 1C; Could / Release 3; Must)

6.5.2.1.4.1 Style tools shall allow users to compose content based on pre-defined design rules.

6.5.2.1.4.2 Style tools shall allow users to compose content using templates based on rules (e.g., agency style manuals).

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.

6.5.2.1.5 Style tools shall allow multiple users to work collaboratively on the same content, prior to publication. (Release 1C; Could / Release 3; Must)

6.5.2.1.5.1 Style tools shall allow authorized users to approve/reject content changes made by collaborators.

6.5.2.1.5.1.1 Style tools shall track approval/rejection of changes to content, prior to publication.

6.5.2.1.5.1.2 Style tools shall allow for approval of content.

6.5.2.1.5.1.3 Style tools shall allow for approval of content presentation.

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 1C; Could / Release 3; Must)

6.5.2.1.7 Style tools shall provide the capability to track and undo changes to WIP content. (Release 1C; Could / Release 3; Must)

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 1C; Could / Release 3; Must)

- PDF
- Desktop printer
- PDA or other digital media device

6.5.2.1.9 Style tools shall interface with Content Originator ordering. (Release 1C; Could / Release 3; Must)

6.5.2.2 Style Tools - Automated Composition

6.5.2.2.1 Style tools shall have the capability to automatically compose content. (Release 2; Could / Release 3; Must)

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)

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)

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)

6.5.2.2.2 Style tools shall allow users to modify automatically composed content. (Release 2; Could / Release 3; Must)

6.5.2.3 Style Tools - System Administration

6.5.2.3.1 The system shall accept content based on the access rights and privileges of the user submitting the content. (Release 1C; Could / Release 3; Must)

6.5.2.3.2 The system shall assign unique ID's to digital objects created by style tools. (Release 1C; Could / Release 3; Must)

6.5.2.3.3 The system shall provide storage for WIP style tools content. (Release 1C; Could / Release 3; Must)

6.5.2.3.3.1 The system shall allow management of WIP content based on access rights and privileges.

6.5.2.3.3.2 The system shall provide tracking of all WIP activities.

6.5.2.3.3.3 The system shall provide search and retrieval capabilities for WIP content.

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 1C; Could / Release 3; Must)

3.2.6.6 Content Originator Ordering

Content Originator ordering is a system interface to FDsys that allows Content Originators to submit content, order and re-order content, specify content delivery, and request other service options. It will provide the capability to create, capture, augment, and store agency processing requirements specific to ordering functions, preservation needs, version, and job specifications (e.g., SF1, 952, 2511, 3868). In addition, Content Originator ordering will allow users to discover the cost of job and fulfillment options, select fulfillment choices, and discover payment/billing status when applicable. Service Providers will use the interface to interact, deliver, and report upon order status. Service Specialists will use the interface to manage the ordering process. In addition, the system shall support the ability for Service Specialists or Content Originators to add additional copies (riders) to a request or order placed by the publishing agency or Congress. Content Originator ordering will pass content to pre-ingest processing, notify Content Evaluators when job are placed, and integrate with GPO's financial systems. Context specific help and support will be accessible through the interface.

3.2.6.6.1 Current Situation

GPO's Customer Services department is responsible for coordinating the contracting and procurement process for Federal agencies and Congress. They handle the entire process including determining which procurement vehicle to utilize, writing specifications, obtaining bids from Service Providers, selecting the contractor, contract administration, and quality assurance. The department uses numerous legacy systems to manage this process. Additionally, GPO accepts any file types from Content Originators for production. The most common formats are Adobe InDesign, Quark XPress, Microsoft Word, and Adobe Acrobat Portable Document Format (PDF).

Job tracking is generally limited to manually tracking phone call and email correspondence between Service Providers and Content Originator. Data is manually entered by Service Specialists into GPO's mainframe Procurement Information Control System (PICS). PICSWEB, a web-based interface to PICS, allows Content Originator's to review information on the cost and status of their job. PICS can only be managed and viewed by GPO personnel and Content Originator's have limited read-only access to the system through PICSWEB.

3.2.6.6.2 Content Originator Ordering Requirements

6.6.2.1 Content Originator Ordering Core Capabilities

6.6.2.1.1 The system shall provide a user interface for Content Originator ordering. (Release 1C; Must)

6.6.2.1.2 The system shall have the capability to process jobs prior to content being approved for publication prior to ingest. (Release 1C: Must)

6.6.2.1.3 The system shall have the capability to process jobs prior to content being received. (Release 1C; Must)

6.6.2.1.4 The system shall have the capability to track jobs using the unique ID requirements. (Release 1C; Must)

6.6.2.1.5 The system shall have the capability to support a Content Originator specific tracking number and link to a unique ID. (Release 1C; Could / Release 2; Must)

6.6.2.1.6 The system shall have the capability to be interoperable with external Content Originator ordering systems (e.g., Treasury Integrated Print Procurement System). (Release 1C; Could)

6.6.2.1.7 The system shall adhere to policies set forth in *GPO Publication 305.3.* (Release 1C; Must)

6.6.2.2 Content Originator Ordering - Job Management

6.6.2.2.1 The system shall provide the capability to create, acquire, edit and store BPI data specific to ordering functions, preservation needs, version, and job specifications (e.g., SF1, 952, 2511, 3868, etc.). (Release 1C; Must)

6.6.2.2.2 The system shall allow users to generate and submit jobs electronically. (Release 1C; Must)

6.6.2.2.2.1 The system shall ensure users are authorized to submit jobs (e.g., are authorized to spend funds) based upon business rules.

6.6.2.2.2.2 The system shall allow authorized users to approve content for publication.

6.6.2.2.2.3 The system shall support credential technologies (e.g. PKI) per the FDsys security requirements.

6.6.2.2.3 The system shall allow users to view and search similar job specifications. (Release 1C; Should / Release 2; Must)

6.6.2.2.4 The system shall have the capability to identify similar jobs and specifications (e.g., strapping jobs) based upon business rules. (Release 1C; Should / Release 2; Must)

6.6.2.2.4.1 The system shall notify Service Specialists of similar jobs and job specifications.

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 1C; Must)

6.6.2.2.6 The system shall provide the capability for Content Evaluators and Content Originators to ride jobs as defined by GPO business rules. (Release 1C; Must)

6.6.2.2.7 The system shall provide the capability to notify Content Evaluators and Content Originators that riders have been placed. (Release 1C; Should / Release 2; Must)

6.6.2.2.8 The system shall provide the capability to alert Content Evaluators and Content Originators that GPO is accepting riders for content as defined by GPO business rules. (Release 1C; Must)

6.6.2.2.9 The system shall have the capability to determine contract types (e.g., one-time bids, SPA, term contract) based upon specification and business rules. (Release 1C; Could).

6.6.2.2.10 The system shall allow users to request a contract type. (Release 1C; Should / Release 2; Must)

6.6.2.2.11 The system shall allow users to view a history of all previous jobs based on user rights. (Release 1C; Should / Release 2; Must)

6.6.2.2.12 The system shall provide estimated costs to authorized users for jobs based upon job specifications. (Release 1C; Could / Release 2; Must)

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 solicitation release. (Release 1C; Must)

6.6.2.2.14 The system shall have the capability to inform authorized users that a job specification has been edited. (Release 1C; Should / Release 2; Must).

6.6.2.2.15 The system shall provide the capability for Content Originators to specify Content Delivery options (hard copy, electronic presentation, digital media) based upon the content submitted. (Release 1C; Must)

6.6.2.2.16 The system shall allow users to select fulfillment options for content delivery. (Release 1C; Must)

6.6.2.2.16.1 The system shall provide the capability to support multiple hard copy fulfillment options including, but not limited to: Customer pick-up, Ship, Deliver, Mail, Free on Board (FOB) Contractor City, Free on Board (FOB) Destination, and Government Bills of Lading. (Release 1C; Must)

6.6.2.2.16.2 The system shall provide the capability to enter multiple shipping and fulfillment destinations. (Release 1C; Must)

6.6.2.2.16.3 The system shall provide the capability for Content Originators to select ship, fulfillment, mail, or pickup dates. (Release 1C; Must)

6.6.2.2.16.4 The system shall provide the capability for Content Originators and Service Providers to select shipping providers (e.g., Fed-Ex, UPS, USPS). (Release 1C; Must)

6.6.2.2.16.5 The system shall have the capability to provide estimated fulfillment costs based upon job specifications. (Release 1C; Could)

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 1C; Must)

6.6.2.2.17 The system shall maintain Service Provider information. (Release 1C; Must)

6.6.2.2.17.1 Authorized users shall have the capability to access Service Provider information. (Release 1C; Must)

6.6.2.2.17.2 The system shall provide the capability for Service Providers and GPO users to manage Service Provider information. (Release 1C; Must)

6.6.2.2.17.2.1 Service Provider contact information shall include, but not be limited to: Name of company, Physical address, Mailing address (if different), Fulfillment address (if different), Names of contact personnel, Phone number, Cell phone number, E-mail, Fax, State & Contractor code.

6.6.2.2.17.2.2 The system shall provide the capability for multiple contact personnel for each Service Provider.

6.6.2.2.17.3 The Service Provider shall be able to select equipment categories from a predefined list. (Release 1C; Could / Release 2; Must)

6.6.2.2.17.3.1 Authorized GPO personnel shall be able to manage the predefined list of equipment categories.

6.6.2.2.17.4 The Service Provider shall be able to select capabilities from a predefined list. (Release 1C; Must)

6.6.2.2.17.4.1 Authorized GPO personnel shall be able to manage the predefined list of capabilities.

6.6.2.2.17.4.2 The service provider shall be able to input customized capabilities not included on the predefined list.

6.6.2.2.17.5 The Service Provider shall be able to manage preferences including, but not limited to: (Release 1C; Could / Release 2; Must)

- Preferred methods of fulfillment for job.
- Preferred methods of fulfillment based on the type of procurement (e.g., term contract, simplified purchase agreement order, small purchase order, one time bid order).

- Preferred method of fulfillment for request job.
- Preferred time of deliveries.

6.6.2.2.17.6 The system shall maintain Service Provider performance information. (Release 1C; Must)

6.6.2.2.17.6.1 The system shall allow GPO users to manage Service Provider performance data.

6.6.2.2.17.6.2 Quality levels shall be assigned by authorized GPO personnel in accordance with *GPO Publication 310.1*.

6.6.2.2.17.6.3 Quality history data shall include, but not be limited to:

- Number of jobs completed at given quality levels
- Number of jobs inspected at given quality level
- Number of jobs rejected at given quality levels

6.6.2.2.17.6.4 Compliance history shall include, but not be limited to:

- Number of jobs completed
- Number of jobs completed late
- Percentage of job completed late

6.6.2.2.17.6.5 Notices received shall include, but not be limited to:

- Number of cure notices
- Number of show-cause notices
- Number of shipped short letters
- Number of do not condone letters
- Number of terminations for default (program)
- Number of terminations for default (orders)
- Number of erroneous information letters
- Number of non-responsible quality history letters
- Number of non-responsible quality level letters
- Number of non-responsible performance letters
- Number of non-responsible other letters
- Number of exception clause letters

6.6.2.2.17.6.6 Notes

6.6.2.2.18 The system shall provide the capability to search for Service Providers based on job specifications and Service Providers capabilities, location, and equipment. (Release 1C; Must)

6.6.2.2.19 The system shall generate a list of Service Providers based upon job specifications and Service Providers capabilities, location, minimum acceptable quality level, and equipment. (Release 1C; Must)

6.6.2.2.19.1 The system shall provide the capability for Content Originator and Service Specialists to select from approved Service Providers based upon GPO business rules and GPO procurement regulations.

6.6.2.2.20 The system shall allow Service Specialists to generate and distribute solicitations (e.g., post online, send to specified Service Providers). (Release 1C; Must)

6.6.2.2.21 The system shall accept bids from Service Providers. (Release 1C; Must)

6.6.2.2.21.1 The system shall accept bids with multiple line items.

6.6.2.2.21.2 The system shall accept fixed bids with an indefinite quantity.

6.6.2.2.21.3 The system shall electronically stamp bids with time, date, and user data.

6.6.2.2.21.4 The system shall allow Service Specialists to announce bid results electronically.

6.6.2.2.22 The system shall allow Service Specialists and Content Originators to award jobs to Service Providers. (Release 1C; Must)

6.6.2.2.22.1 The system shall have the capability to send content and order information to Service Providers after award.

6.6.2.2.24 The system shall allow Service Providers to request contract modifications based upon business rules. (Release 1C; Should / Release 2; Must)

6.6.2.2.25 The system shall allow Service Specialists to request, authorize, and manage contract modifications based upon business rules. (Release 1C; Should / Release 2; Must)

6.6.2.2.26 The system shall allow Content Originators to request and authorize contract modifications based upon business rules. (Release 1C; Should / Release 2; Must)

6.6.2.2.27 The system shall provide the capability for users to request re-orders. (Release 1C; Must)

6.6.2.3 Content Originator Ordering - Job Tracking

6.6.2.3.1 The system shall have the capability to log activities and communications with Content Originators, Service Providers, and Service Specialists including but not limited to: . (Release 1C; Must)

- Job made available to Service Provider
- Job received by Service Provider
- Proofs sent to Content Originator
- Proofs received by Content Originator
- Proof approved
- Proof approved with author's alterations
- Proof approved with Service Provider's errors
- New proofs requested due to author's alterations
- New proofs requested due to Service Provider's errors
- Proofs sent to Service Provider
- Proofs received by Service Provider
- Changes made by Content Originator
- Changes made by Service Provider
- Signed proof approval receipt available
- Job complete
- Job delivered to each individual destination
- Job delivered to all destinations
- Job delivery receipts available
- Contact name(s)
- Contact organization(s)
- Contact information (e.g., phone number, e-mail address)
- Type of communication (e.g., telephone, meeting, e-mail)
- Digest
- Unique ID referenced (e.g., job number)
- Approved for publication

6.6.2.3.1.1 The system shall provide a means to add notes to each job.

6.6.2.3.2 The system shall provide the capability to contact Service Providers for job status (e.g., tracking of job). (Release 1C; Should / Release 2; Must)

6.6.2.3.2.1 The system shall automatically contact Service Providers.

6.6.2.3.2.2 The system shall have the capability for authorized users to request automated notifications for job activities.

6.6.2.3.3 The system shall allow Service Specialists to generate and distribute notification to Service Providers and Content Originator (e.g., show cause, cure notice, 907, specification amendments). (Release 1C; Should / Release 2; Must)

6.6.2.3.4 The system shall have the capability to provide notification of fulfillment to users. (Release 1C; Should / Release 2; Must)

6.6.2.3.4.1 Notification of fulfillment shall include, but not be limited to:

- Fulfillment tracking numbers from the Service Provider
- Signed fulfillment receipts
- Confirmation of fulfillment from agency recipients

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).

6.5.2.3.4.2.1 The system shall have the capability to provide authorized users with the ability to cancel a job.

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.

6.5.2.3.4.2.3 The system shall have the capability to provide notification of fulfillment based on the log of activities.

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).

6.5.2.3.4.2.5 The system shall have the capability for users to elect not to receive notification of fulfillment.

6.5.2.3.4.2.6 The system shall allow authorized users to manage fulfillment notification.

6.6.2.3.5 The system shall have the capability to provide users with confirmation of fulfillment. (Release 1C; Should / Release 2; Must)

6.6.2.3.5.1 The system shall have the capability to receive and store product fulfillment tracking numbers (e.g., Fed-Ex Tracking Number) from Service Providers.

6.5.2.3.5.1.1 The system shall have the capability to store multiple tracking numbers for each order.

6.5.2.3.5.1.2 The system shall provide a hyperlink to a fulfillment provider tracking website.

6.6.2.3.5.2 The system shall have the capability to receive confirmation of fulfillment from the agency or end user.

6.5.2.3.5.2.1 The system shall have the capability to receive multiple confirmations of fulfillment.

6.6.2.3.6 The system shall have the capability to support Job Definition Format (JDF). (Release 3; Could)

3.2.7 CONTENT ACCESS AND PROCESSING

Content access and processing provides the services and functions that allow users to determine the existence, description, location and availability of content, and request delivery of content and metadata. In addition, content access and processing allows for the management of Access Content Packages and user interaction with the system.

This section is an overarching specification for all content access functional requirements, and individual sections have been created for each functional area within access. Content access and processing includes information about the following:

- Search – Performing queries on content and metadata so that content can be retrieved from storage and delivered to users.
- Request - Processing no-fee and fee based content delivery requests.
- Cataloging - Creating descriptive metadata that conform to accepted standards and support access and delivery of standard bibliographic records.
- Reference tools - Creating lists and resources that assist users in locating and accessing content.
- User interface - Developing and managing user interactions with the system.
- User support - Providing answers to user inquiries and directing users to content and services.
- Accessibility – Providing content and system accessibility for persons with disabilities.

Under legal authority of Title 44, Chapters 17, 19, and 41 of the United States Code (U.S.C.), GPO's Office of Information Dissemination (Superintendent of Documents) administers various dissemination programs with the mission of providing permanent public access to official Federal Government information. These include the Federal Depository Library Program (FDLP), International Exchange Service, GPO Sales Program, By-Law programs, and the GPO Access public Web site. The FDLP distributes electronic and tangible publications to a network of over 1,250 Federal Depository libraries across the country. GPO is able to provide these publications to depository libraries for no-fee through a congressional appropriation. Select publications are also available for sale to the public via the GPO Sales Program, including through the U.S. Government Bookstore.

GPO Access, the primary vehicle for dissemination of electronic publications via the FDLP, provides no-fee public access to full-text databases of official Federal Government publications. As used in this document, GPO Access is an umbrella term for electronic Government information products that are in scope for the FDLP and made accessible to the public by or through GPO including access files and public databases available on the GPO Access public web site and other GPO servers; other remotely accessible electronic Government information products managed either by GPO or by other institutions with which GPO has established formal agreements; and remotely accessible electronic Government information products that GPO identifies, describes, and links to, but which remain under the control of the originating agencies.

Access to Federal Electronic Information

Public Law 103-40, the U.S. Government Printing Office Electronic Information Access Enhancement Act of 1993, as codified in Title 44 Sections 4101- 4104 of the United States Code, charged the Superintendent of Documents with developing mechanisms to enhance public access to a wide range of Federal electronic information products. Sections 4101 through 4104 are below.

§ 4101 - Electronic directory; online access to publications; electronic storage facility

(a) In General. — The Superintendent of Documents, under the direction of the Public Printer, shall —

(1) maintain an electronic directory of Federal electronic information;

(2) provide a system of online access to the Congressional Record, the Federal Register, and, as determined by the Superintendent of Documents, other appropriate publications distributed by the Superintendent of Documents; and

(3) operate an electronic storage facility for Federal electronic information to which online access is made available under paragraph (2).

(b) Departmental Requests. — To the extent practicable, the Superintendent of Documents shall accommodate any request by the head of a department or agency to include in the system of access referred to in subsection (a) (2) information that is under the control of the department or agency involved.

(c) Consultation. — In carrying out this section, the Superintendent of Documents shall consult —

(1) users of the directory and the system of access provided for under subsection (a); and

(2) other providers of similar information services. The purpose of such consultation shall be to assess the quality and value of the directory and the system, in light of user needs.

§ 4102 – Fees.

(a) In General. — The Superintendent of Documents, under the direction of the Public Printer, may charge reasonable fees for use of the directory and the system of access provided for under section 4101, except that use of the directory and the system shall be made available to depository libraries without charge. The fees received shall be treated in the same manner as moneys received from sale of documents under section 1702 of this title.

(b) Cost Recovery. — The fees charged under this section shall be set so as to recover the incremental cost of dissemination of the information involved, with the cost to be computed without regard to section 1708 of this title.

§ 4103 – Biennial Report.

Not later than December 31 of each odd-numbered year, the Public Printer shall submit to the Congress, with respect to the two preceding fiscal years, a report on the directory, the system of access, and the electronic storage facility referred to in section 4101 (a). The report shall include a description of the functions involved, including a statement of cost savings in comparison with traditional forms of information distribution.

§ 4104 – Definition.

As used in this chapter, the term "Federal electronic information" means Federal public information stored electronically.

Comprehensive Index of Public Documents

GPO has a legal mandate under 44 U.S.C. 1710-11 to prepare and publish a "comprehensive index of public documents," including "every document issued or published…not confidential in character." Cataloging provides a structured means to identify and locate content of interest.

3.2.7.1 Current Situation

GPO currently operates three major web portals for the purpose of disseminating information to End Users and managing bibliographic records.

GPO Access disseminates information from all three branches of the Federal Government to Congress, Federal agencies, library partners, and the general public. User support is provided through a Customer Relationship Management (CRM) tool with a Web interface. GPO Access also includes legislative, executive and judicial agency Web sites that are hosted by GPO. Available at http://www.gpoaccess.gov/.

The FDLP Desktop, Integrated Library System (ILS), and Online Public Access Catalog (OPAC) provide cataloging and reference tools for the Federal information resources disturbed through the FDLP. The ILS contains bibliographic records for both tangible and electronic publications. Electronic publications may be located on servers that are within and outside of GPO's control (e.g. Agency web sites), and bibliographic records often include links to publications that are available electronically. Available at http://www.access.gpo.gov/su_docs/fdlp/index.html and http://catalog.gpo.gov.

The U.S. Government Bookstore allows users to purchase tangible publications online. Available at http://bookstore.gpo.gov/.

Release 0

Prior to FDsys Release 1A, GPO is actively engaging in "Release 0" activities. The goal of Release 0 is to generate GPO Access Packages from compliant Submission Information Packages (SIP). GPO Access Packages will contain converted content that has been derived from tangible U.S. Government publications that are within scope of the FDLP. GPO Access Packages will be created according to the GPO Access Package specification.

Current Metrics

GPO tracks the number of retrievals, or content retrieved from Wide Area Information Server (WAIS) databases on GPO Access. GPO Access averages approximately 37 million document retrievals per month. Since its inception in 1994, GPO Access retrievals have exceeded 2.4 billion. The total number of retrievals from GPO Access in FY 2005 was 4.3 million or 1.1 million per day. June 2005 was the busiest month ever, with more than 39 million retrievals. Through November 2005, more than 52 million documents have been retrieved in FY 2006. Please refer to the FDsys System Sizing document for additional information.

3.2.7.2 Requirements for Access Content Processing

7.2.1 Access Core Capabilities

7.2.1.1 The system must provide open and interoperable access to content. (Release 1B; Must)

7.2.1.2 The system must provide open and interoperable access to metadata. (Release 1B; Must)

7.2.1.3 The system must provide access to content at the minimum level of granularity that is specified in the FDsys unique ID requirements. (Release 1B; Must)

7.2.1.4 The system shall provide the capability for End Users to use persistent names to access content. (Release 1B; Must)

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 1B; Must)

7.2.1.6 The system must provide the capability for users to access information about relationships between content packages, between digital objects, and between digital objects and content packages. (Release 1B; Must)

7.2.1.7 The system must provide the capability to use GPO's ILS to access metadata repositories not resident within the system. (Release 1B; Must)

7.2.1.8 The system must provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including the following. (Release 1B; Must)

- A partnership between GPO, the University Library of Case Western Reserve University, and the Census Bureau, establishing a Web site specifically for depository library access to Census 2000 data issued by the Census Bureau in comma- delimited ASCII format.
- 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.
- A partnership between GPO and the University of North Texas Libraries

to provide permanent online access to electronic publications of selected Federal Government agencies which have ceased operation (Cybercemetery).

- A partnership with the U.S. Department of State, the Richard J. Daley Library, University of Illinois at Chicago, and GPO to provide access to the Department of State Foreign Affairs Network (DOSFAN).
- A partnership between GPO and the Federal Reserve Bank of St. Louis for public access to content in the Federal Reserve Archival System for Economic Research (FRASER) service.
- A partnership between GPO and the U.S. General Accounting Office (GAO), making GAO publications permanently available online through GPO Access.
- In cooperation with GPO, the National Library of Medicine will provide permanent public access to the information in the following NLM publications:
    - MEDLINE
    - Medical Subject Headings
    - NLM LocatorPlus
- A partnership between GPO, Wichita State University, and the National Institute for Aviation Research making Documents Data Miner (DDM) available. DDM is a collection management tool for Federal depository libraries.
- A partnership between GPO and the Department of Energy's Office of Scientific and Technical Information making DOE GrayLIT available to the public through GPO Access. DOE GrayLIT provides a portal to more than 100,000 full-text technical reports located at DOE, the Department of Defense, the Environmental Protection Agency, and the National Aeronautics and Space Administration.
- A partnership between GPO and the Department of Energy's Office of Scientific and Technical Information making DOE Federal R&D Project Summaries available to the public through GPO Access. DOE Federal R&D Project Summaries includes more than 240,000 research summaries and awards by three of the major sponsors of research in the Federal Government.
- A partnership between GPO and the Department of Energy's Office of Scientific and Technical Information making DOE Information Bridge available to the public through GPO Access. DOE Information Bridge provides access to full-text documents and bibliographic citations of Department of Energy (DOE) research report literature.
- A partnership between GPO and the Oklahoma State University, Edmon Low Library providing access to Browse Topics. Browse Topics, developed by volunteer government information librarians, provides

topical pathfinders to U.S. Government information. The list of topics is derived from the Guide to U.S. Government Information (Subject Bibliography Index) published by GPO.

- A partnership between GPO and Louisiana State University Libraries providing access to a list of Federal Agency Internet Sites.

7.2.2 Access to Content Packages

7.2.2.1 The system must provide the capability for GPO to manage access to content packages according to GPO business rules. (Release 1A; Must)

7.2.2.2 The system must accept access rules for content packages. (Release 1A; Must)

7.2.2.3 The system must provide the capability to limit access to content with re-dissemination restrictions as specified by the Content Originator. (Release 1B; Must)

7.2.2.4 The system must provide the capability to limit access to content with limited distribution as specified by the Content Originator. (Release 1B; Must)

7.2.2.5 The system must provide the capability to limit access to classified content as specified by the Content Originator. (Release 1B; Must)

7.2.2.6 The system must provide the capability to limit access to copyrighted content as specified by the Content Originator. (Release 1B; Must)

7.2.2.7 The system must provide the capability to limit access to content that is out of scope for GPO’s dissemination programs. (Release 1B; Must)

7.2.2.8 The system must provide the capability to limit access to content that has not been approved by the Content Originator for public release. (Release 1B; Must)

7.2.2.9 The system must provide the capability to limit access to embargoed content until the appropriate release data and time as specified by the Content Originator. (Release 1B; Must)

7.2.2.10 The system must provide the capability to limit access to content based on criteria specified by the Content Originator. (Release 1B; Must)

7.2.2.11 The system must provide access to content currently available on GPO Access. (Release 1B; Must)

7.2.2.12 The system must provide the capability to notify users of limitations on access to content. (Release 1B; Must)

7.2.2.13 The system shall provide the capability to provide customized access to content packages. (Release 1C; Should / Release 2; Must)

7.2.2.14 The system shall provide the capability to provide personalized access to content packages. (Release 1C; Could / Release 2; Must)

7.2.2.15 The system must provide the capability for users to access in scope final published versions of ACPs. (Release 1B; Must)

7.2.2.16 The system must provide the capability for authorized users to access final approved versions of ACPs that are not in scope for GPO's dissemination programs. (Release 1B; Must)

7.2.3 Access to the System

7.2.3.1 The system must have the capability to provide access to system functions by user class. (Release 1A; Must)

7.2.3.2 The system must provide access to public End Users that does not require them to log-in or register with the system. (Release 1B; Must)

7.2.3.3 The system must provide the capability for authorized Content Originators, Service Providers, Service Specialists, and Content Evaluators to access WIP storage. (Release 1A; Must)

7.2.3.3.1 The system shall have the capability to allow Content Originators to authorize access to content in WIP. (Release 1A; Must)

7.2.3.3.2 The system must provide "check in and check out" capabilities for content in WIP. (Release 1C; Could / Release 2; Must)

7.2.3.4 The system shall provide the capability to provide customized access to the system. (Release 1C; Should / Release 2; Must)

7.2.3.5 The system shall provide the capability to provide personalized access to the system. (Release 1C; Could / Release 2; Must)

7.2.4 Access - User Registration

7.2.4.1 The system must provide the capability for users to register with the system. (Release 1A; Must)

7.2.4.2 The system must provide the capability to establish a user account for each registered user. (Release 1A; Must)

7.2.4.3 The system must provide the capability to create user records for registered users. (Release 1A; Must)

7.2.4.4 The system must have capability to store and manage an unlimited number of user records. (Release 1A; Must)

7.2.4.5 The system must provide the capability for authorized users to access user records. (Release 1A; Must)

7.2.4.6 The system must provide the capability for GPO System Administrators to set required fields in user records. (Release 1A; Must)

7.2.4.7 The system must provide the capability to record information submitted by users during registration with system. (Release 1A; Must)

7.2.4.8 The system must provide the capability to for GPO to customize what information is collected during user registration. (Release 1A; Must)

7.2.4.8.1 The system must have the capability to collect name from the user during registration (e.g., honorific title, first name, last name, job title).

7.2.4.8.2 The system must 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).

7.2.4.8.3 The system shall provide the capability to collect security clearance information from the user during registration.

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).

7.2.4.8.4.1 Users may be members of multiple user classes simultaneously.

7.2.4.8.4.2 The system shall associate registered users with at least one user class.

7.2.4.8.5 The system shall provide the capability to collect role-based information from the user during registration.

7.2.4.8.6 The system shall provide the capability to collect proof of identity information from the user during registration.

7.2.4.8.7 The system shall provide the capability to collect authority to publish information from the user during registration.

7.2.4.9 The system shall provide the capability to perform records management functions on user records. (Release 1B; Must)

7.2.5 Access - User Preferences

7.2.5.1 The system must provide the capability for authorized users to manage user preferences including but not limited to the following: (Release 1C; Should / Release 2; Must)

- Preferred contact methods
- Delivery options
- User interfaces
- Alert services
- Help features
- Frequently accessed tools

7.2.5.2 The system must provide the capability for authorized users to manage other users' preferences. (Release 1C; Should / Release 2; Must)

7.2.5.3 The system must provide the capability for GPO to establish and manage default user preferences. (Release 1C; Should / Release 2; Must)

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)

7.2.5.5 The system shall provide the capability to provide customized user preferences. (Release 1C; Should / Release 2; Must)

7.2.5.6 The system shall provide the capability to provide personalized user preferences. (Release 1C; Could / Release 2; Must)

7.2.6 Access Processing

7.2.6.1 The system must provide the capability to process and manage ACPs. (Release 1B; Must)

7.2.6.1.1 The system must provide the capability to process and manage digital objects that are used for access.

7.2.6.1.2 The system must provide the capability to manage metadata that are used for access.

7.2.6.2 The system must provide the capability to create access derivatives. (Release 1B; Must)

7.2.6.3 The system must provide the capability to apply cataloging and reference tools processes. (Release 1B; Must)

7.2.6.4 The system must provide the capability to assign persistent names. (Release 1B; Must)

7.2.6.5 The system must provide the capability for access processing to request that an ACP be modified or created from an AIP. (Release 1B; Must)

7.2.6.6 The system shall provide the capability for access processing to provide content, metadata, business process information, and other metadata as necessary to delivery processing for the purpose of fulfilling an End User request or Content Originator order. (Release 1B; Must)

7.2.6.7 The system must provide the capability to perform records management functions on ACPs. (Release 1B; Must)

7.2.6.7.1 Records management functions must comply with GPO and Federal records management policies.

7.2.6.7.2 Records management functions must be performed according to records management schedules for content and metadata within the system.

7.2.6.8 The system must provide the capability to identify and manage relationships between digital objects, between content packages, and between digital objects and content packages, including, but not limited to the following: (Release 1A; Must)

- Changes in content that occur in the legislative process (e.g., the progression from a congressional bill to a public law to codification in the *United States Code*).
- Changes in content that occur between publications in Government processes (e.g., a notice in the *Federal Register* to the corresponding sections in the *Code of Federal Regulations).*
- Digital objects referenced within other digital objects (e.g., linked citations).
- Language translations
- Serials per the cataloging and reference tools requirements.

3.2.7.3 Accessibility

The accessibility requirements focus on FDsys content and system accessibility for persons with disabilities. The system shall provide the capability to create, assess, and validate content packages for compliance with Section 508 technical standards. In addition, FDsys components and technologies shall comply with Section 508 technical standards.

What is Section 508?

Section 508 refers to a statutory section in the Rehabilitation Act of 1973, which is codified in 29 U.S.C. 794d. In 1998, President Clinton signed the Workforce Investment Act of 1998 into law. The Act amended Section 508 of the Rehabilitation Act of 1973 to provide access to and use of Federal executive agencies' electronic and information technology (EIT) by individuals with disabilities.

Furthermore, Section 508 requires Federal executive departments and agencies that develop, procure, maintain, or use electronic and information technology to ensure that Federal employees and members of the public with disabilities have access to and use of information and data, comparable to that of the employees and members of the public without disabilities–unless it is an undue burden to do so.

Section 508 requirements are separate from, but complementary to, requirements in sections 501 and 504 (ADA) of the Rehabilitation Act that require, among other things, that agencies provide reasonable accommodations for employees with disabilities, provide program access to members of the public with disabilities, and take other actions necessary to prevent discrimination on the basis of disability in their programs.

Who is covered by Section 508?

Section 508 covers Federal executive departments and agencies including the U.S. Postal Service. In addition, contractors providing services or products to Federal executive agencies must provide Section 508 compliant deliverables. While GPO is not legally required to comply with Section 508, GPO is committed to setting an example for other Federal agencies by voluntarily complying with Section 508 accessibility standards.

In addition, the Department of Justice has encouraged GPO to comply with Section 508. An April 2000 Department of Justice report on Federal accessibility states that, because "[m]any smaller agencies rely on the Government Printing Office for their Web site design and maintenance,…the Government Printing Office should provide leadership to ensure that all Web pages it develops or maintains are accessible." The report is titled Information Technology and People with Disabilities: The current State of Federal Accessibility and was presented by then Attorney General Reno to then President Clinton.

What is covered by Section 508?

Section 508 covers electronic and information technology (EIT) procured, developed, maintained, or used by a Federal executive agency. EIT is information technology (IT), as defined at FAR 2.101, and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. In addition to IT, EIT includes telecommunication products, such as telephones, information kiosks, transaction machines, World Wide Web sites, multimedia (including videotapes), and office equipment, such as copiers and fax machines.

Section 508 Regulations

Access Board Standards

The first regulation implementing Section 508 was issued by the Architectural and Transportation Barriers Compliance Board (the "Access Board"), an independent Federal agency, whose primary mission is to promote accessibility for individuals with disabilities. This regulation is referred to as the Access Board's "standards." The standards, along with an explanatory preamble, were published in the Federal Register, as a final rule, on December 21, 2000. The standards are codified at 36 CFR Part 1194. The Access Board's standards became enforceable on June 21, 2001.

Section 508 standards are technical specifications and performance-based requirements which focus on the functional capabilities covered by technologies. The standards are organized into six sections:

- Software Applications and Operating Systems
- Web-based Intranet and Internet Information and Applications
- Telecommunications Products
- Video and Multimedia Products
- Self Contained, Closed Products

- Desktop and Portable Computers

FAR Rule

The second rule issued to implement Section 508 amends the Federal Acquisition Regulation (FAR) to ensure that agency acquisitions of EIT comply with the Access Board's standards. The entire FAR is codified at 48 CFR Chapter 1. The FAR change implementing Section 508 was published along with an explanatory preamble in the Federal Register on April 25, 2001, and was effective as of June 25, 2001.

GPO's Response to Section 508

In July 2000, GPO created a set of draft Web design guidelines for GPO Access. At the time, these guidelines applied strategies taken from the World Wide Web Consortium (W3C)'s Web Content Accessibility Guidelines, version 1.0 to ensure that GPO Access would be accessible under guidelines set forth under the Americans with Disabilities Act.

In response to the Section 508 legislation and standards, GPO performed an extensive review of GPO Access throughout 2001 in order to ensure compliance with Federal accessibility standards. The Biennial Report to Congress on the Status of GPO Access, which was published by GPO on December 31, 2001, states that GPO is committed to setting an example for other Federal agencies by ensuring that GPO Access pages and hosted sites meet the accessibility requirements for electronic and information technology set forth in Section 508 of the Rehabilitation Act.

To further its commitment to accessibility, the GPO Access Web site redesign of 2003 included a Section 508 compliant Web interface, Section 508 compliance was included in an internal instruction titled GPO Access Web Design, and GPO web sites contain information about GPO's ongoing commitment to accessibility.

World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Guidelines

While most Federal Government entities comply with Section 508, many private sector organizations tend to follow the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) guidelines listed below. WAI guidelines are based on the fundamental technical specifications of the Web, and are developed in coordination with other W3C technical specifications including but not limited to HTML, XML, CSS, SVG, and SMIL.

Authoring Tool Accessibility Guidelines (ATAG)

The Authoring Tool Accessibility Guidelines (ATAG) documents explain how to make authoring tools accessible to people with disabilities. Authoring tools are software that people use to produce Web pages and Web content. A primary focus of ATAG is defining how tools help Web developers produce Web content that conforms to Web Content Accessibility Guidelines. http://www.w3.org/WAI/intro/atag.php.

Web Content Accessibility Guidelines (WCAG)

The Web Content Accessibility Guidelines (WCAG) documents explain how to make Web content accessible to people with disabilities. Web "content" generally refers to the information in a Web page or Web application, including text, images, forms, sounds, and such. (More specific definitions are available in the WCAG documents.) http://www.w3.org/WAI/intro/wcag.

User Agent Accessibility Guidelines (UAAG)

The User Agent Accessibility Guidelines (UAAG) documents explain how to make user agents accessible to people with disabilities, particularly to increase accessibility to Web content. User agents include Web browsers, media players, and assistive technologies, which are software that some people with disabilities use in interacting with computers. http://www.w3.org/WAI/intro/uaag.php.

3.2.7.3.1 Current Situation

GPO is currently working to ensure that existing content and Web pages on GPO Access and agency hosted sites are Section 508 compliant, and that future pages are created specifically with these accessibility standards in mind. GPO follows established Government and industry best practices for complying with Section 508 technical standards. When requested by agencies, GPO incorporates language into its contracts requiring that contractors guarantee that files comply with Section 508 of the Rehabilitation Act, but it does not specify how compliance is implemented or validated.

3.2.7.3.2 Requirements for Accessibility

7.3.2.1 Accessibility Core Capabilities

7.3.2.1.1 The system must provide the capability to assess content for compliance with Section 508 technical standards. (Release 1B; Must)

7.3.2.1.2 The system must provide the capability to create content that is compliant with Section 508 technical standards. (Release 1B; Must)

7.3.2.1.3 The system must provide the capability to validate content for compliance with Section 508 technical standards. (Release 1B; Must)

7.3.2.1.4 The system must accept accessibility requirements and implementation guidance from Content Originators. (Release 1A; Must)

7.3.2.1.5 The system must provide Section 508 compliant access to the system. (Release 1A; Must)

7.3.2.1.6 In order to achieve compliance with Section 508 technical standards, established best practices should be followed. (Release 1B; Could)

7.3.2.1.7 The system must create content that contain well formed code which conforms to World Wide Web Consortium (W3C) Guidelines. (Release 1B; Must)

7.3.2.2 Accessibility - Section 508 Technical Standards

7.3.2.2.1 FDsys software applications and operating systems shall be Section 508 compliant according to 36 CFR Part 1194.21 to the extent possible. (Release 1A; Should)

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.

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.

7.3.2.2.1.3 A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.

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 must also be available in text.

7.3.2.2.1.5 When bitmap 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.

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.

7.3.2.2.1.7 Applications shall not override user selected contrast and color selections and other individual display attributes.

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.

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.

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.

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.

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.

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 to the extent possible. (Release 1A; Should)

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).

7.3.2.2.2.2 Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.

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.

7.3.2.2.2.4 Documents shall be organized so they are readable without requiring an associated style sheet.

7.3.2.2.2.5 Redundant text links shall be provided for each active region of a server-side image map.

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.

7.3.2.2.2.7 Row and column headers shall be identified for data tables.

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.

7.3.2.2.2.9 Frames shall be titled with text that facilitates frame identification and navigation.

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.

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

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.

7.3.2.2.2.13 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) through (l).

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.

7.3.2.2.2.15 A method shall be provided that permits users to skip repetitive navigation links.

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.

7.3.2.2.3 FDsys telecommunications products shall be Section 508 compliant according to 36 CFR Part 1194.23 to the extent possible. (Release 1A; Should)

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.

7.3.2.2.3.2 Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.

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.

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.

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.

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.

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.

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.

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.

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.

7.3.2.2.3.11 Products which have mechanically operated controls or keys, shall comply with the following:

(a) Controls and keys shall be tactilely discernible without activating the controls or keys.

(b) 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.

(c) 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.

(d) The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.

7.3.2.2.4 FDsys video and multimedia products shall be Section 508 compliant according to 36 CFR Part 1194.24 to the extent possible. (Release 1A; Should)

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 stand-alone 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.

7.3.2.2.4.2 Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.

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.

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.

7.3.2.2.4.5 Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.

7.3.2.2.5 FDsys self contained, closed products shall be Section 508 compliant according to 36 CFR Part 1194.25 to the extent possible. (Release 1A; Should)

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.

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.

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).

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.

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.

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.

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.

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.

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.

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:

(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.

(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.

(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.

(4) Operable controls shall not be more than 24 inches behind the reference plane.

7.3.2.2.6 FDsys desktop and portable computer products shall be Section 508 compliant according to 36 CFR Part 1194.26 to the extent possible. (Release 1A; Should)

7.3.2.2.6.1 All mechanically operated controls and keys shall comply with §1194.23 (k) (1) through (4).

7.3.2.2.6.2 If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).

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.

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.

3.2.7.4 Search

Search executes queries on content and metadata so that content can be retrieved from storage, processes, and delivered to users. FDsys search tools should meet or exceed industry standards for search and retrieval technology. As necessary, more than one search tool may be used to meet the needs of all user classes who will be searching the system. The FDsys search tools must handle user searches of content and metadata both simultaneously and separately across multiple internal repositories. Search must have the ability to search multiple media, file formats, and levels of granularity. Search should produce a highly relevant, organized, usable, and detailed results list that provides the location and description of content. Search tools should provide innovative methods for users to access information related to their query. Search must include accessible and customizable graphical user interfaces that allow all users to submit and refine queries, filter results, and export results sets.

3.2.7.4.1 Current Situation

GPO's online system, GPO Access, was launched on June 8, 1994. At the time of launch, the system provided fee-based access to three databases. The system became available to the public free of charge on December 1, 1995. Traditionally, the vast majority of information made available via GPO Access has been derived from databases used in the printing of Government publications. The databases are delivered by a distributed text searching system called Wide Area Information Servers (WAIS).

While this text searching system was cutting-edge at the time, the creator of WAIS, Thinking Machines, went bankrupt in 1995. Since then, WAIS has been supported entirely by GPO's IT staff. The system has since been customized to meet the needs of GPO. Over ten years later, WAIS is still the primary search engine deployed by GPO. Files are posted online directly following the receipt of the information from the publishing agency or Congress, and they are generally by-products of printed products. While GPO has been experimenting with providing dynamic content as demanded by today's user, WAIS cannot support dynamic content delivery. In addition, GPO's Web design and hosting customers as well as internal customers have demanded search capabilities that go beyond the abilities of WAIS, such as PDF indexing and search. This situation has led to the use of two other search platforms—OpenText and Microsoft.

While all of GPO's Web services utilize search functionality, five major entities have unique search demands:

- GPO Access <http:.//www.gpoaccess.gov> disseminates information from all three branches of the Federal Government for Federal agency, library partner, and general public use. With the exception of one beta application (eCFR), GPO Access allows users to perform full-text searches via the WAIS platform.
- The Catalog of U.S. Government Publications <http://catalog.gpo.gov> functions as GPO's Online Public Access Catalog (OPAC) and allows users to search bibliographic records of publications that are part of GPO's National Bibliography of U.S. Government Publications.

- The U.S. Government Bookstore <http://bookstore.gpo.gov> allows users to search a catalog of publications that are available for sale and purchase tangible publications online. The search functionality of the Bookstore is implemented in Lucene on an Apache server.
- GPO's Web hosting and design services offer a mixture of WAIS and Microsoft search platforms. More recently, sites hosted by GPO <http://www.gpo.gov/webteam/sites.htm> (such as the U.S. Supreme Court Web site) have been utilizing the Microsoft platform. Previously, Web sites (such as the Export Administration Regulations Web site) were utilizing the WAIS platform.
- Customer Services is in constant communication with Federal agencies and vendors to disseminate information products. Currently, Customer Services provides an online system called PICSWEB <http://govprint.access.gpo.gov/> that allows customers to track, estimate, and obtain information on any of their printing jobs.

In addition, GPO is currently implementing a data and search disaster recovery program for selected Web services. In the event that GPO's WAIS engine becomes unavailable, a backup search will kick in until service is restored. While this system has not yet been fully developed, initial discussions indicate that the search will run on the FAST platform.

GPO tracks the number of retrievals, or content retrieved from a WAIS database on GPO Access. GPO Access averages approximately 37 million document retrievals per month. Since its inception in 1994, GPO Access retrievals have exceeded 2.4 billion. The total number of retrievals from GPO Access in FY 2005 was 4.3 million or 1.1 million per day. June 2005 was the busiest month ever, with more than 39 million retrievals. Through November 2005, more than 52 million documents have been retrieved in FY 2006.

3.2.7.4.2 Requirements for Search

7.4.2.1 Search Core Capabilities

7.4.2.1.1 The system must provide the capability to search for and retrieve content from the system. (Release 1B; Must)

7.4.2.1.2 The system must provide the capability to search for and retrieve metadata from the system. (Release 1B; Must)

7.4.2.1.3 The system must provide the capability to search across multiple internal content and metadata repositories simultaneously and separately. (Release 1B; Must)

7.4.2.1.4 The system must provide the capability to search content that is currently available on the GPO Access public Web site. (Release 1B; Must)

7.4.2.1.5 The system must provide the capability to search cataloging records in order to provide access to select external repositories with which GPO has formal partnership agreements. (Release 1B; Must)

7.4.2.1.6 The system must provide the capability to search and retrieve unstructured content (e.g., text). (Release 1B; Must)

7.4.2.1.7 The system must provide the capability to match character strings (e.g., search exact phrases). (Release 1B; Must)

7.4.2.1.8 The system must provide the capability to search and retrieve semi-structured content (e.g., inline markup). (Release 1B; Must)

7.4.2.1.9 The system must provide the capability to search and retrieve structured content (e.g., fielded). (Release 1B; Must)

7.4.2.1.10 The system must provide the capability to search for content by means of querying metadata. (Release 1B; Must)

7.4.2.1.11 The system must provide the capability for users to search collections based on user class, user role, and access rights. (Release 1B; Must)

7.4.2.1.12 The system must provide the capability to search in Access Content Storage and Work in Progress storage both simultaneously and separately. (Release 1B; Must)

7.4.2.2 Search - Query

7.4.2.2.1 The system must provide the capability for users to select content collections to search. (Release 1B; Must)

7.4.2.2.2 The system must 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)

7.4.2.2.3 The system must provide the capability for users to select search complexity levels (e.g., simple search, advanced/fielded search). (Release 1B; Must)

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.

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.

7.4.2.2.4 The system shall allow users to limit searches by available qualifiers, options, or limits as defined by GPO business rules. (Release 1B; Must)

7.4.2.2.5 The system must provide the capability for GPO Business Managers to customize search qualifiers, options, or limits including but not limited to the following: (Release 1B; Must)

- Content and metadata (e.g., full-text, bibliographic records, descriptive metadata).
- Storage or repository (e.g., ACS, WIP, repository of bibliographic records)
- Locally defined collections or catalogs (e.g., National bibliography, Congressional, Congressional serial set, periodical, serial, regulatory).

- GPO Access application (e.g., Public and Private Laws, Congressional Reports, Congressional Documents, Congressional Bills, Federal Register, History of Bills, Congressional Record, Congressional Record Index, United States Code, Code of Federal Regulations, List of CFR Sections Affected (LSA), Congressional Hearings (including House and Senate Appropriations Hearings), Congressional Committee Prints, Congressional Calendars (including House, Senate, and Committee), Weekly Compilation of Presidential Documents, Budget of the United States Government, Congressional Record (Bound), House Journal, Semiannual Regulatory Agenda (Unified Agenda), U.S. Constitution: Analysis and Interpretation, Economic Indicators, Economic Report of the President, Congressional Directory, U.S. Government Manual, Public Papers of the President of the United States, House Ways and Means Committee Prints (Green Book), GAO Comptroller General Decisions, GAO Reports, House Practice, Senate Manual, House Rules and Manual, Privacy Act Issuances, Department of Interior IG Reports, U.S. Government Printing Office Style Manual, Cannon’s Precedents of the House of Representatives, Deschler’s Precedents of the U.S. House of Representatives, Hinds’ Precedents of the House of Representatives, Independent Counsel’s Referral to Congress, Government Information Locator Service Records (GILS), Supreme Court Decisions 1937-75, Davis-Bacon Wage Determinations, Commerce Business Daily, Congressional Publications, Statutes at Large).
- Bibliographic and FDLP information (e.g., keyword, title, serials/periodical, author, all subjects, LC subject, geographic subject, MeSH subject, NASA subject, publisher, publication place, SuDoc class number, shipping list number, item number, ISBN number, ISSN number, OCLC number, technical report number, contract number, stock number, series number, notes, contents, URL/PURL, LC class number, depository library number).
- Date (e.g., date published, date, date range).
- Content Originator format (e.g., books, maps, CD, DVD, floppy, VHS, visual material, mixed material, microfiche, online).
- Citation (e.g., h.r. 123, s. 345, 24 CRF 12).
- Content type (e.g., harvested, converted, deposited).
- Rights limitation (e.g., embargoed, copyrighted).

7.4.2.2.6 The system must allow users to perform a search for conceptually related terms (e.g., search for "World Series" returns articles on the Red Sox). (Release 1B; Must)

7.4.2.2.6.1 The system shall allow GPO administrators to add, modify, and delete concept relationships.

7.4.2.2.6.2 The system shall process content, metadata, and BPI to create and update existing concept relationships.

7.4.2.2.6.3 The system shall process user input (e.g. search terms) to help define concept relationships.

7.4.2.2.7 The system must support standard Boolean search language. (Release 1B; Must)

7.4.2.2.7.1 The system shall support full Boolean operators, including but not limited to: AND, OR, NOT, BEFORE, NEAR, and ADJACENT.

7.4.2.2.7.2 The system shall support implied Boolean operators, including but not limited to "+" and "-".

7.4.2.2.7.3 The system shall support the nesting of Boolean operators via parentheses.

7.4.2.2.7.4 Boolean operators must not be case-sensitive.

7.4.2.2.8 The system must allow users to perform a natural language search that does not require connectors or a specific syntax. (Release 1B; Must)

7.4.2.2.9 The system must support a customizable list of stop words. (Release 1B; Must)

7.4.2.2.10 The system must allow for right and left truncation. (Release 1B; Must)

7.4.2.2.11 The system must allow users to use wildcard characters to replace characters within words. (Release 1B; Must)

7.4.2.2.12 The system must support proximity searching. (Release 1B; Must)

7.4.2.2.13 The system must support synonyms searching. (Release 1B; Must)

7.4.2.2.14 The system may provide the capability for contextual searching (Release 1B; Could)

7.4.2.2.15 The system must conform to ISO 239.50 or other international standards for search interoperability. (Release 1B; Must)

7.4.2.2.16 The system must provide the capability to perform searches across internal repositories including legacy repositories. (Release 1B; Must)

7.4.2.2.17 The system must have a documented interface (e.g., API) to allow search by non-GPO systems. (Release 1B; Must)

7.4.2.2.18 The system must have the capability to comply with OAI-PHM. (Release 1B; Must)

7.4.2.2.19 The system must allow users to select specified search functionality. (Release 1B; Must)

7.4.2.2.20 The system must support queries of variable lengths. (Release 1B; Must)

7.4.2.2.21 The systems must have the ability to limit search query length. (Release 1B; Must)

7.4.2.2.22 The system must provide the capability to weight search terms (e.g., term must appear, term must not appear, term is part of an exact phrase). (Release 1B; Must)

7.4.2.3 Search - Refine

7.4.2.3.1 The system must provide the capability for users to modify previous search queries to enable execution of subsequent searches. (Release 1B; Must)

7.4.2.3.1.1 The system shall provide the capability to direct subsequent queries against different content collections.

7.4.2.3.1.2 The system shall provide the capability for users to retain selected targets while modifying queries.

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 1B; Must)

7.4.2.3.2.1 The system shall provide users with the ability to directly execute a search from conceptually related terms.

7.4.2.3.3 The system must recognize alternate spellings of terms and provide suggestions for alternative terms. (Release 1B; Must)

7.4.2.3.3.1 The system shall suggest corrected spellings of terms.

7.4.2.4 Search - Results

7.4.2.4.1 The system must provide search results to users. (Release 1B; Must)

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)

7.4.2.4.3 The system must provide the capability to sort results lists. (Release 1B; Must)

7.4.2.4.4 The system must provide the capability to categorize results. (Release 1B; Must)

7.4.2.4.5 The system must provide the capability to cluster results. (Release 1B; Could)

7.4.2.4.6 The system may provide the capability to analyze results lists. (Release 1B; Could)

7.4.2.4.7 The system shall provide the capability to display results graphically. (Release 1B; Could)

7.4.2.4.8 The system must provide the capability to apply one or multiple taxonomies. (Release 1B; Could)

7.4.2.4.9 The system must provide the capability for users to limit the number of results displayed. (Release 1B; Must)

7.4.2.4.10 The system must provide the capability to display the total number of results in the result set returned by the search. (Release 1B; Must)

7.4.2.4.11 The system must provide the capability to configure the elements in a result.

(Release 1B; Must)

7.4.2.4.11.1 The system must display, at a minimum, title, file size, version, content collection (source), and an identifier (link).

7.4.2.4.11.2 The system shall have the capability to display other elements in a result (e.g., relevance rank, description of content) when available.

7.4.2.4.12 The system shall provide the capability to highlight query terms in the results list. (Release 1B; Could)

7.4.2.4.13 The system must provide the ability to generate error messages for failed searches. (Release 1B; Must)

7.4.2.4.14 The system must provide the capability to display inline image thumbnails of content in a results list. (Release 1B; Must)

7.4.2.4.15 The system must allow users to save search results individually or as a batch (e.g., without selecting each result individually) for export. (Release 1B; Should / Release 2; Must)

7.4.2.4.16 The system must provide the capability to deliver search results at the finest level of granularity supported by the target content package and as required in the FDsys Unique ID requirements. (Release 1B; Must)

7.4.2.4.17 The system shall provide the capability to modify relevancy ranking factors based on business rules. (Release 1B; Should / Release 2; Must)

7.4.2.5 Saved Searches

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 1B; Should / Release 2; Must)

7.4.2.5.2 The system shall provide the capability to automatically execute saved searches on a schedule defined by the user. (Release 1B; Should / Release 2; Must)

7.4.2.5.3 The system shall provide the capability to notify users when automatically executed searches return results. (Release 1B; Should / Release 2; Must)

7.4.2.6 Search - User Interface

7.4.2.6.1 The system must provide a search interface that allows users to submit queries to the system and receive results. (Release 1B; Must)

7.4.2.6.2 The system must provide the capability to have multiple search interfaces based on search skill level and user class. (Release 1B; Must)

7.4.2.6.3 The system must provide the capability to have customizable search interfaces based on user preferences and requirements. (Release 1C; Should / Release 2; Must)

7.4.2.6.4 The system must provide the capability to have navigational elements to allow users to navigate through results. (Release 1B; Must)

7.4.2.6.5 The system must have the capability to store and access user search preferences (e.g., preferred layout, preferred search method, frequently used content collections). (Release 1C; Should / Release 2; Must)

7.4.2.7 Search - Administration

7.4.2.7.1 The system must provide the capability to manage user search interfaces. (Release 1B; Must)

7.4.2.7.2 The system must provide a Web-based administrator graphical user interface (GUI). (Release 1B; Must)

7.4.2.7.3 The system must provide the capability to configure an unlimited number of search portals. (Release 1B; Must)

7.4.2.7.4 The system must provide for the control of search run times, including the ability to preempt runtimes by an administrator-defined limit. (Release 1B; Must)

7.4.2.7.5 The system must provide the capability to support user search while other system functions are being performed (e.g., re-indexing databases, updating content). (Release 1B; Must)

7.4.2.7.6 The system must provide the capability to log search activities. (Release 1B; Must)

3.2.7.5 Request

Request will allow users to request delivery of content and metadata from FDsys. Request must have the capability to handle no-fee and fee-based delivery requests. An example of a no-fee request for delivery is a Public End User downloading a PDF document that is within scope of the Federal Depository Library Program. An example of a fee-based request for delivery is a Public End User using a shopping cart function to order publications from an e-commerce Web site. For fee-based content, request must provide the capability for End Users discover the cost of delivery, choose delivery options, and submit payment for delivery. In addition, request must provide the capability for GPO and external Service Providers to request delivery of content packages for the purpose of content processing and delivery. Request must ensure that customer transactions can be conducted in a secure environment. Request must have the ability to interact with GPO systems or other Authorized Representatives for a variety of services, including but not limited to financial and inventory control systems. Request must provide the capability for End Users to manage and securely store information in user accounts such as order histories, user preferences for delivery options, and preferred payment methods.

3.2.7.5.1 Current Situation

Federal Depository Library Program

GPO works in partnership with over 1,250 libraries participating in the Federal Depository Library Program (FDLP) to provide the public with no-fee access to U.S. Government publications. GPO is able to disseminate these publications to depository libraries for no-fee through a congressional appropriation. Depository libraries receive publications based their depository library type. There are two types of libraries in the FDLP, regional and selective libraries. Regional libraries are required to receive all publications that are distributed, and selective libraries have greater flexibility in choosing publications for their collections. Selective depositories select from over 7,000 item numbers published in the List of Classes of United States Government Publications Available for Selection by Depository Libraries to customize their collection for the particular patron group they serve, such as the academic or legal communities. Item numbers may represent one serial title or a group of miscellaneous publications. Additions to selections are made twice during the annual selection update cycle. Deletions to a library's selection list may be done at any time. These selections make up a depository library's unique profile that is used to distribute FDLP items.

GPO provides public End Users with no-fee online access to full-text documents in ASCII text, HTML, and screen optimized PDF for printing and downloading through GPO Access. In addition, GPO provides access to content and metadata through the Catalog of U.S. Government Publications, GPO's Online Public Access Catalog (OPAC). As used in this document GPO Access is an umbrella term for electronic Government information products that are in scope for the FDLP and made accessible to the public by or through GPO including access files and public databases available on the GPO Access public Web site and other GPO servers; other remotely accessible electronic Government information products managed either by either GPO or by other institutions with which GPO has established formal agreements; and remotely accessible electronic Government information products that GPO identifies, describes, and links to, but which remain under the control of the originating agencies.

Publication and Information Sales Program

Under the authority of Title 44 of the United States Code, GPO's Sales Program provides the public an opportunity to purchase tangible government information products. GPO is recognized by the public as the primary central source for selling official and authentic versions of documents from all three branches of the Federal Government. Customers can place orders for publications and subscriptions by telephone, fax, or mail through the GPO Contact Center. In addition, GPO's U.S. Government Bookstore, http://bookstore.gpo.gov, allows users to purchase tangible publications online. GPO accepts payment in the form of cash, check, major credit cards (Visa, MasterCard, Discover/NOVUS, and American Express), Government purchase orders, and deposit accounts. All payments, except credit card payments, require some manual processing before being certified as paid.

Publication and Information Sales Program RFP

In October 2005, GPO released a Request for Proposal (RFP) for GPO's Publication and Information Sales Program. The RFP was developed by GPO for information and planning purposed for GPO. In the Publication and Information Sales Program RFP, GPO announced that it was seeking innovative relationships with the private sector to create new business models. The agency's goal is to build new private sector relationships that will expand our business and improve service to customers. GPO is also hoping to capitalize on industry experience to offer services to publishing agencies that will assist them with reaching their specific audiences as well as the general public.

GPO is seeking an Authorized Representative to operate the Publication and Information Sales Program and be the primary distributor for official government content on a revenue sharing basis. The selected Authorized Representative would operate under mutually beneficial performance-based revenue sharing models and fee-based service offerings. This is a service-based model, pertaining to elements such as inventory acquisition and management, sales, marketing, order processing and fulfillment, customer support, storage, and distribution.

The Publication and Information Sales Program is expected to manage transactions from End Users who wish to purchase Government content from GPO, regardless of the form in which that content is delivered. GPO views the development of the FDsys as being largely complementary to the service-based relationship it is planning to establish with the Publication and Information Sales Program RFP, and the FDsys is expected to interface with future Publication and Information Sales Program activities. The FDsys digital repository will provide the source of digital content to support all of GPO's dissemination activities. In the case of tangible products, whether hard copy or digital media, the Authorized Representative is expected to fulfill the customer's tangible product order. For customers who purchase content delivered online, the Authorized Representative would again manage the transaction but the product content will be delivered from the FDsys.

3.2.7.5.2 Requirements for Request

7.5.2.1 Request Core Capabilities

7.5.2.1.1 The system shall provide the capability for users to request delivery of content. (Release 1B; Must)

7.5.2.1.2 The system shall provide the capability for users to request delivery of metadata. (Release 1B; Must)

7.5.2.1.3 The system must comply with GPO and Federal privacy, security, and records management policies. (Release 1B; Must)

7.5.2.2 No Fee Requests

7.5.2.2.1 The system must provide the capability for End Users to request no-fee content delivery as defined by GPO business units. (Release 1B; Must)

7.5.2.2.1.1 The system must not restrict or otherwise diminish access to items that are currently available through GPO Access.

7.5.2.2.1.2 The system must provide the capability for users to print and download information currently available through GPO Access.

7.5.2.2.2 The system must provide the capability for Federal Depository Library End Users to select and request content and metadata for delivery to their library based on their unique profile and preferences. (Release 1B; Must)

7.5.2.2.3 The system shall comply with GPO policies related to selection of tangible and electronic titles by Federal Depository Library End Users. (Release 1B; Must)

7.5.2.2.4 The system shall provide the capability to interface with “Authorized Representatives” as designated by GPO’s Library Services and Content Management business unit for processing of no-fee delivery requests. (Release 1B; Must)

7.5.2.2.5 The system must provide the capability to interface with GPO’s Integrated Library System and other legacy systems as defined by GPO business units for processing of no-fee requests. (Release 1B; Must)

7.5.2.2.6 The system must provide the capability to process no-fee requests for delivery of content with access restrictions. (Release 1B; Must)

7.5.2.2.7 The system must support the delivery of serials and periodicals. (Release 1B; Must)

7.5.2.2.8 The system must provide the capability for users to cancel full or partial requests prior to fulfillment. (Release 1B; Must)

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)

7.5.2.2.9.1 The system shall provide the capability for users to opt-out of personalized offers.

7.5.2.2.10 The system must provide the capability to provide authorized users with a detailed transaction summary according to GPO business rules. (Release 1B; Should / Release 2; Must)

7.5.2.2.11 The system shall provide the capability for GPO to configure transaction summaries to include but not be limited to the following: (Release 1B; Should / Release 2; Must)

- Title(s) requested.
- Order number.
- Date of request.
- SuDoc class number.

- Item number.
- Shipping list number.

7.5.2.2.12 The system must provide the capability to generate reports for no-fee transactions. (Release 1B; Must)

7.5.2.3 Fee-based Requests

7.5.2.3.1 The system must provide the capability for users to request fee-based content delivery as defined by GPO business rules. (Release 1C; Must)

7.5.2.3.2 The system must 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 1C; Must)

7.5.2.3.3 The system must provide the capability to interface with GPO's financial and inventory systems for processing of fee-based requests. (Release 1C; Must)

7.5.2.3.4 The system must ensure that user transactions are conducted in a secure environment at the industry standard level of integrity. (Release 1C; Must)

7.5.2.3.5 The system must have the capability to generate price information for the delivery of content. (Release 1C; Must)

7.5.2.3.6 The system must have the capability to adjust price information for fee-based content delivery. (Release 1C; Must)

7.5.2.3.6.1 Pricing structures must comply with GPO's legislative mandates under Title 44 of the *United States Code* and GPO's Sales Program policies.

7.5.2.3.6.2 The system must provide the capability to manually adjust the price.

7.5.2.3.6.3 The system must provide the capability to dynamically adjust the price.

7.5.2.3.6.4 The system must provide the capability to apply price schedules.

7.5.2.3.7 The system must adhere to industry best practices for performance of a Web-accessible e-commerce system. (Release 1C; Must)

7.5.2.3.8 The system must include an online bookstore web interface that complies with the FDsys user interface requirements and includes but is not limited to the following features: (Release 1C; Could)

- Shopping cart.
- Order tracking.
- Backorder capabilities.
- Third party ordering.

- Thumbnail cover images.
- Fully browsable and searchable catalog of items available for purchase that is updated at least daily.

7.5.2.3.9 The system must provide the capability to process international and domestic requests for publications, subscriptions, and standing orders according to GPO business rules. (Release 1C, Must)

7.5.2.3.10 The system must provide the capability to process fee-based requests for the delivery of content with access restrictions. (Release 1C; Must)

7.5.2.3.11 The system must support methods of payment as defined by GPO business rules. The system must provide the capability to accept the following payment methods: (Release 1C; Must)

- Check/electronic transfer.
- Major credit cards including Visa, MasterCard, Discover/NOVUS, and American Express.
- Debit cards.
- Purchase orders.
- Requests for invoicing.
- Deposit accounts.

7.5.2.3.12 The system must provide the capability to automatically verify and validate payment information submitted by users prior to delivery fulfillment. (Release 1C; Must)

7.5.2.3.13 The system must 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)

7.5.2.3.14 The system must 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)

7.5.2.3.15 The system must 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 1C; Must)

7.5.2.3.15.1 The system shall provide the capability to manage, secure, and maintain End User information associated with subscriptions. (Release 1C; Must)

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)

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)

7.5.2.3.16.1 The system shall provide the capability for users to opt-out of personalized offers.

7.5.2.3.17 The system must provide the capability for users to cancel full or partial requests prior to fulfillment. (Release 1C; Must)

7.5.2.3.18 The system must provide the capability to provide authorized users with a detailed transaction summary according to GPO business rules. (Release 1C; Must)

7.5.2.3.19 The system shall provide the capability for GPO to configure transaction summaries to include but not be limited to the following: (Release 1C; Should / Release 2; Must)

- Title(s) requested.
- Quantities.
- Price of each publication.
- Order number.
- Payment method.
- Cost that will be billed to the user.
- Date of request.

7.5.2.3.20 The system must provide the capability to manage transaction records according to GPO and Federal policies. (Release 1C; Must)

7.5.2.3.20.1 The system shall securely maintain electronic copies of orders, shipments, and financial records for at least seven years.

7.5.2.3.21 The system must provide the capability to generate reports for fee-based transactions (e.g., order histories, sales transactions, inventory data). (Release 1C; Must)

7.5.2.4 Request - Delivery Options

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 1B; Must)

7.5.2.4.2 The system must provide the capability for users to request delivery of content or metadata from available options as defined by GPO business units. (Release 1B; Must)

7.5.2.4.3 The system must 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 1B; Must)

7.5.2.4.4 The system must provide the capability for users to select file type from available options (e.g., DOC, MP3, PDF). (Release 1B; Must)

7.5.2.4.5 The system must provide the capability for users to select resolution (e.g., images, video) from available options. (Release 1B; Could / Release 2; Must)

7.5.2.4.6 The system must provide the capability for users to select color space from available options (e.g. RGB, CMYK). (Release 1B; Could / Release 2; Must)

7.5.2.4.7 The system must provide the capability for users to select compression and size from available options. (Release 1B; Could / Release 2; Must)

7.5.2.4.8 The system must provide the capability for users to select transfer rate from available options. (Release 1B; Could / Release 2; Must)

7.5.2.4.9 The system must provide the capability for users to select platform from available options. (Release 1B; Must)

7.5.2.4.10 The system must provide the capability for users to select the version of content from available options. (Release 1B; Must)

7.5.2.4.11 The system must provide the capability for users to select delivery of related content from available options. (Release 1B; Could / Release 2; Must)

7.5.2.4.12 The system must 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 1B; Must)

7.5.2.4.13 The system must provide the capability for users to select quantity of items requested for delivery (e.g., one, five, batch). (Release 1B; Must)

7.5.2.4.14 The system must provide the capability for users to select output type from available options (e.g., hard copy, electronic presentation, digital media). (Release 1B; Must)

7.5.2.4.15 The system must provide the capability for users to select data storage device from available options (e.g., CD, DVD, server). (Release 1B; Must)

7.5.2.4.16 The system must provide the capability for users to select level of granularity from available options (e.g., title, part, section, paragraph, graphic, page). (Release 1B; Must)

7.5.2.4.17 The system must provide the capability for users to select electronic delivery method from available options (e.g., FTP, RSS, email, download, broadcast). (Release 1B; Must)

7.5.2.4.18 The system must provide the capability for users to schedule delivery from the system. (Release 1B; Should)

7.5.2.4.19 The system must provide the capability for users to select tangible delivery method from available options (e.g., air transportation, ground transportation, pickup, overnight, priority, freight). (Release 1C; Must)

7.5.2.4.20 The system must provide the capability for GPO to offer users separate “bill to” and “ship to” options for delivery or shipment of tangible content. (Release 1C; Must)

7.5.2.4.21 The system must provide the capability for users to submit multiple address options for delivery or shipment of tangible content. (Release 1C; Must)

7.5.2.4.22 The system must provide the capability to preview requested content. (Release 2; Should / Release 3; Must)

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)

7.5.2.5 Request - User Accounts

7.5.2.5.1 The system must provide the capability to create a secure user account with the system. (Release 1B; Must)

7.5.2.5.2 The system shall provide the capability for End Users and Service Providers to manage their accounts which includes but is not limited to the following: (Release 1B; Should / Release 1C; Must)

- Update profile.
- Manage content delivery preferences.
- Select, request, and schedule items for delivery.
- View request and delivery histories.

7.5.2.6 Order Numbers and Request Status

7.5.2.6.1 The system must provide the capability to create and assign an alphanumeric order number for requests. (Release 1B; Must)

7.5.2.6.2 The system must not repeat an order number. (Release 1B; Must)

7.5.2.6.3 The system must record order numbers in metadata. (Release 1B; Must)

7.5.2.6.4 The system must have the capability to provide order numbers to users. (Release 1B; Must)

7.5.2.6.5 The system must provide the capability for users to track the status of their requests. (Release 1B; Must)

3.2.7.6 Cataloging and Reference Tools

Cataloging

In the GPO context, cataloging and indexing refers to the legally-required activities that result in the Catalog of U.S. Government Publications. GPO has a legal mandate under 44 U.S.C. 1710-11 to prepare and publish a “comprehensive index of public documents,” including “every document issued or published…not confidential in character.” GPO’s library customers expect that this mandate will be fulfilled through the creation of descriptive (access) metadata, i.e., cataloging or bibliographic records, that conform to accepted national library standards and practices. In FDsys cataloging tools create descriptive metadata that conform to accepted standards, and support access to and delivery of standard bibliographic records.

Content in the scope for cataloging are official U.S. Government publications. Not all FDsys content will be cataloged. For example, an agency print order for envelopes will result in metadata in the system, but the envelopes will not meet the scope criteria to qualify for cataloging.

The cataloging process uses applicable descriptive metadata elements, including metadata that is harvested along with the digital object to which it is related. GPO will also acquire bibliographic metadata from external Content Originators and Service Providers (e.g., library and agency partners, OCLC).

GPO provides metadata records to various users (e.g., individual libraries, value-added resellers, the Library of Congress, etc.) in a variety of standard formats (e.g., MARC or ONIX).

Reference Tools

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

Reference tools will include lists and resources that assist users in locating and accessing content. Reference tools will have the ability to create, acquire and store metadata (e.g. MARC), references to metadata (e.g. Subject Bibliographies), and references to content (e.g. Federal Agency Internet Sites, Browse Topics, etc.).

Lists, in the context of reference tools, may be static pages produced from report generation capabilities, or dynamic results lists from searches. These searches may be pre-configured (“canned”) or individually created for one-time use.

3.2.7.6.1 Current Situation

GPO’s cataloging mission is required by law, and considerable funds have already been expended on the Integrated Library System (ILS) prior to conceptualization of the FDsys.

GPO has acquired Ex Libris’ Aleph version 16.2, which serves as the platform for descriptive metadata management. FDsys must be integrated to be fully functional with the ILS. The ILS package also includes federated searching and reference linking tools, MetaLib and SFX.

The FDsys must interface with the ILS and the Online Computer Library Center, Inc. (OCLC) system for creating bibliographic metadata and storage capabilities for structured data is required. Bibliographic metadata includes links to content maintained on various sites managed by or completely external to GPO, e.g. the OCLC Digital Archive, on various agency and library sites, etc.

This integration should enable data exchange to facilitate the creation of cataloging and reference tools. Cataloging will draw upon metadata acquired and stored by FDsys, and will transform or organize that data into meaningful structures (e.g. MARC, Dublin Core, ONIX).

The ILS stores records in MARC format. In order to accommodate, accept, or output other metadata formats, crosswalks will need to be developed and provided by FDsys.

3.2.7.6.2 Requirements for Cataloging and Reference Tools

7.6.2.1 Cataloging and Reference Tools - Metadata Management

7.6.2.1.1 The system shall provide for the creation of metadata for content. (Release 1A; Must)

7.6.2.1.2 The system shall support creation of metadata according to specified cataloging rules. (Release 1A; Must)

7.6.2.1.3 The system will apply authority control to provide cross-referencing of terms. (e.g., a user enters any form of a name, title, or subject in a search and all database items associated with that form must be retrieved). (Release 1B; Must)

7.6.2.1.4 The system shall support the creation of metadata meeting book industry requirements (e.g., ONIX). (Release 1C; Must)

7.6.2.1.5 The system shall support the creation of library standard bibliographic records (e.g., MARC). (Release 1A; Must)

7.6.2.1.6 The system shall support the creation of metadata by the system (e.g., automatically create). (Release 1A; Must)

7.6.2.1.7 The system shall provide for the creation of metadata by authorized users (e.g., manually create). (Release 1A; Must)

7.6.2.1.8 The system shall provide for the creation of new metadata records based on existing metadata records. (Release 1A; Must)

7.6.2.1.9 The system shall provide the capability to acquire and integrate metadata from external sources. (Release 1A; Must)

7.6.2.1.10 The system shall relate descriptive metadata with the content described. (Release 1A; Must)

7.6.2.1.11 The system shall provide capability for authorized users to manage metadata. (Release 1A; Must)

7.6.2.1.12 The system shall support versioning of metadata. (Release 1A; Must)

7.6.2.1.13 The system shall have the ability to provide access to metadata throughout the lifecycle of the content. (Release 1A; Must)

7.6.2.1.14 The system must provide the capability to add metadata specifically for GPO sales purposes (e.g., book jacket art, reviews, summaries). (Release 1C; Could)

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 1A; Must)

7.6.2.2 Cataloging and Reference Tools - Metadata Delivery

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 1B; Must)

7.6.2.2.2 The system will provide for display and output of brief citations. (Release 1B; Must)

7.6.2.2.3 The system will provide for display and output of basic bibliographic citations. (Release 1B; Must)

7.6.2.2.4 The system will provide for display and output of full records. (Release 1B; Must)

7.6.2.2.5 The system will provide for display and output of MARC records. (Release 1B; Must)

7.6.2.2.6 The system will provide for the delivery of output in a variety user-specified methods or formats, including but not limited to electronic mail or Web pages. (Release 1B; Must)

7.6.2.2.7 The system shall output metadata in formats specified by the user, including but not limited to MARC, ONIX, ASCII text, or comma delimited text. (Release 1B; Must)

7.6.2.3 Reference Tools

7.6.2.3.1 The system shall have the ability to generate lists based on any indexed metadata field. (Release 1B; Must)

7.6.2.3.2 The system should have the capability to generate lists based on user defined criteria (e.g., that match a library's item selection profile). (Release 1B; Must)

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 1B; Must)

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 1B; Must)

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 1B; Should)

7.6.2.3.6 The system shall have the capability to link to external content and metadata. (Release 1B; Must)

7.6.2.3.7 The system shall be interoperable with third party reference tools (e.g., search catalogs of other libraries). (Release 2; Should)

7.6.2.3.8 The system shall have the capability to dynamically generate reference tools. (Release 2; Could)

7.6.2.3.9 The system will allow GPO to manage reference tools. (Release 1B; Must)

7.6.2.3.10 The system must be able to generate lists based on user preferences. (Release 1C Should / Release 2; Must)

7.6.2.3.11 The system shall provide the capability for users to customize reference tools. (Release 1C; Should / Release 2; Must)

7.6.2.3.12 The system shall support interactive processes so users can create reference tools. (Release 2; Should)

7.6.2.4 Cataloging and Reference Tools - Interoperability and Standards

7.6.2.4.1 The system shall interface with, and allow full functionality of, the GPO Integrated Library System. (Release 1A; Must)

7.6.2.4.2 The system must be compliant with the following NISO and ISO standards: Z39.2 - Information Interchange Format, Z39.9 - International Standard Serial Numbering-ISSN, Z39.29 – 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 1A; Must)

7.6.2.4.3 The system must 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 1A; Must)

7.6.2.4.4 The system shall support the creation of ONIX records. (Release 1C; Must)

7.6.2.4.5 The system shall provide the capability to support search of GPO local data elements that identify unique attributes of the FDLP (e.g., GPO Superintendent of Documents (SuDocs) classification number, Item number, Depository Library number). (Release 1A; Must)

3.2.7.7 User Interface

The user interface functional element will allow for the management of user interactions with the system. Graphical User Interfaces (GUIs) and workbenches (sets of available tools) are key components of this functional area. A workbench will be created for each user class and GUIs will be created for each functional element as required in accordance with the release schedule. Workbenches for internal and external user classes must allow users to access toolsets and perform authorized functions. The system must have the capability to provide default workbenches that do not require users to log-in or register with the system. Users who opt to register with the system will gain the ability to customize GUIs and workbenches, and receive personalized services. The default public End User workbench must provide the capability for users to access official Federal Government information without registering with the system.

3.2.7.7.1 Current Situation

GPO currently operates numerous of services for the purpose of providing user interfaces to current systems. Some of the major services are listed below.

- Content Originator user interfaces include but are not limited to the Procurement Integrated Control System Web (PICSWEB), MicroComp, GPO.gov, and File Transfer Protocol (FTP).
- The Content Evaluator user interface includes but is not limited to the Integrated Library System (ILS) Acquisitions Module.
- Service Specialist user interfaces include but are not limited to the GPO Intranet; ILS Cataloging Module; GPO mainframe including ABLS, Printing Cost Calculating System (PCCS), MPCF, MPCF, Work In Progress (WIP), Production Estimating Planning System (PEPS), STAIRS, PRF, ROPS, and Procurement Integrated Control System (PICS); Wide Area Information Server (WAIS) / OpenText; Online Computer Library Center (OCLC) Digital Archive; Akamai; WebTrends; Customer Relations Management (CRM) system; Public Key Infrastructure (PKI) Systems; onBase; Contractor Connect; GPO Procurement or (GPOPROC); Microsoft Access; and FTP.
- Service Provider user interfaces include are not limited to GPO mainframe, Contractor Connect, Quick Quote, GPO.gov, and the GPO printing system.
- End User interfaces include but are not limited to GPO Access (HTML / WAIS / OpenText), CRM, Legislative, Executive, and Judicial agency Web sites that are hosted by GPO, Federal Depository Library (FDLP) Desktop, Online Public Access Catalog (OPAC), U.S. Government Bookstore, and GPO.gov.

3.2.7.7.2 Requirements for User Interface

7.7.2.1 User Interface Core Capabilities

7.7.2.1.1 The system must provide a default Graphical User Interface (GUI) for each functional element as required in accordance with the system release schedule. (Release 1A; Must)

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.

7.7.2.1.2.1 The system must provide the capability to provide default workbenches that do not require users to register with the system. (Release 1A; Must)

7.7.2.1.2.2 The system must provide the capability for GPO to create workbenches for subsets of user classes. (Release 1A; Must)

7.7.2.1.2.3 The system must provide the capability for GPO to manage the toolsets that are available on default workbenches. (Release 1A; Must)

7.7.2.1.2.4 The system must provide a default public End User workbench that allows users to access official Federal Government information without registering with the system. (Release 1B; Must)

7.7.2.1.2.5 The default public End User workbench must be Section 508 compliant. (Release 1B; Must)

7.7.2.1.2.6 The system must provide a default Service Specialist workbench that provides the capability for Service Specialists to handle exception processing. (Release 1A; Must)

7.7.2.1.2.7 The system must 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 1A; Must)

7.7.2.1.3 The system must provide the capability to maintain a consistent look and feel throughout workbenches and GUIs to the extent possible. (Release 1A; Should)

7.7.2.1.3.1 GUIs must conform to GPO design guidelines and GPO business rules.

7.7.2.1.4 The system must support web-based GUIs. (Release 1A; Must)

7.7.2.1.5 The system must support non web-based GUIs, as necessary. (Release 1A; Should)

7.7.2.1.6 The system must provide GUIs capable of displaying supported types of electronic files (e.g., electronic presentation). (Release 1A; Must)

7.7.2.1.7 The system shall provide for non-English language extensibility such that GUIs could contain non-English language text. (Release 1A; Could / Release 2; Must)

7.7.2.1.8 The system must provide GUIs that accept input of information by users. (Release 1A; Must)

7.7.2.1.9 The system must provide GUIs that accept submission of content by users. (Release 1A; Must)

7.7.2.1.10 The system must provide GUIs that allow users to input and submit registration information and login to the system. (Release 1A; Must)

7.7.2.1.11 The system must display the appropriate default GUIs and workbenches based on a user's access rights, user role, user class, or registration information. (Release 1A; Must)

7.7.2.1.12 The system must provide the capability to integrate search, cataloging and reference tools, request, and user support seamlessly into an End User workbench. (Release 1B; Must)

7.7.2.1.13 The system must provide GUIs that can be displayed on Macintosh, Unix, and Windows environments. (Release 1A; Must)

7.7.2.1.14 The system must provide GUIs that are capable of providing feedback, alerts, or notices to users. (Release 1A; Must)

7.7.2.1.15 The system must provide GUIs that are capable of providing context specific help and user support. (Release 1A; Must)

7.7.2.2 User Interface Standards and Best Practices

7.7.2.2.1 The system shall comply with best practices and guidelines regarding usability for graphical user interface design. (Release 1A; Should)

7.7.2.2.1.1 GUIs should be developed in accordance with guidance issued by the Research-Based Web Design & Usability Guidelines function as best practices for Federal Agencies.

7.7.2.2.1.2 Web GUIs should be developed in accordance with the *Web Style Guide*, 2nd edition.

7.7.2.2.2 The system must conform to current World Wide Web Consortium (W3C) guidelines for interoperable technologies including but not limited to the following. (Release 1A; Must)

7.7.2.2.2.1 The system must conform to Extensible Markup Language (XML).

7.7.2.2.2.2 The system must conform to Extensible Style sheet Language (XSL).

7.7.2.2.2.3 The system must conform to Document Type Definition (DTD) and schema.

7.7.2.2.2.4 The system must conform to XSL Transformations (XSLT).

7.7.2.2.2.5 The system must conform to XML Path Language (XPath).

7.7.2.2.2.6 The system must conform to Extensible HyperText Markup Language (XHTML).

7.7.2.2.2.7 The system must conform to Cascading Style Sheets (CSS).

7.7.2.2.2.8 The system must conform to Document Object Model (DOM).

7.7.2.2.2.9 The system must conform to Hypertext Transfer Protocol (HTTP).

7.7.2.3 User Interface Customization and Personalization

7.7.2.3.1 The system must provide the capability for authorized users who have registered with the system to customize default GUIs and workbenches. (Release 1C; Should / Release 2; Must)

7.7.2.3.1.1 The system must provide the capability to add tools.

7.7.2.3.1.2 The system must provide the capability to remove tools.

7.7.2.3.1.3 The system must provide the capability to hide tools.

7.7.2.3.1.4 The system shall provide the capability to modify the placement of tools.

7.7.2.3.1.5 The system shall provide the capability to modify the size of tools.

7.7.2.3.1.6 The system shall provide the capability to select text size from available options.

7.7.2.3.1.7 The system shall provide the capability to select color scheme from available options.

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)

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)

7.7.2.3.4 The system must provide the capability for users to revert to their original default GUIs and workbenches. (Release 1C; Should / Release 2; Must)

7.7.2.3.5 The system must provide the capability to maintain interface configurations across user sessions. (Release 1C; Should / Release 2; Must)

7.7.2.4 User Interface Default Workbenches

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 1A; Must)

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. (Release 1A; Must)

- 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.
- Deposited content GUI shall enable users to
  - Submit content to pre-ingest WIP.

  - Input metadata.
- 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.
- Search GUI shall enable users to
  - Search and retrieve content and metadata stored in ACS and WIP.
- User support GUI shall enable users to
  - Submit inquires and receive responses.
  - Search knowledge base.
- Data mining GUI shall enable users to
  - Create, schedule, and view reports.

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. (Release 1A; Must)

- 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.
- Data mining GUI shall enable users to
  - Create, schedule, and view reports.

7.7.2.4.4 The system must provide a default user interface for GPO Service Specialists that includes but is not limited to the following tools. (Release 1A; Must)

- 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.
- Search shall enable users to
  - Search and retrieve content and metadata stored in ACS and WIP.
- 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.
- Deposited content GUI shall enable users to
  - Submit content to pre-ingest WIP.
  - Input metadata.
- 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.
- Preservation GUI shall enable users to
  - Manage preservation processes including assessments.
- Version control GUI shall enable users to
  - Input, view, and manage version information.
- 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.

- Reference tools GUI shall enable users to
    - Create, manage, and access reference tools.
- User support GUI shall enable users to
    - Communicate with users.
    - Manage user support tools.
    - Search and manage knowledgebase.
- Request GUI shall enable users to
    - Input, select, and manage delivery options.
    - Schedule delivery.
- Data mining GUI shall enable users to
    - Input supplemental data.
    - Input parameters for data normalization.
    - Extract data for analysis.
    - Create, schedule, and view reports.

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. (Release 1B; Must)

- 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.
- Deposited content GUI shall enable users to
    - Submit content to pre-ingest WIP.
    - Input metadata and BPI.
- Harvested content GUI shall enable users to
    - Manage harvesting processes.
    - Submit content to pre-ingest WIP.
    - Input metadata and BPI.
- Converted content GUI shall enable users to
    - Manage converted content.

  - Submit content to pre-ingest WIP.
  - Input metadata and BPI.
- Content Originator ordering GUI shall enable users to
  - Input and view BPI.
  - View jobs status.
- Search shall enable users to
  - Search and retrieve content and metadata stored in ACS and WIP.
- Request GUI shall enable users to
  - Select content delivery options.
  - Schedule content delivery.
- Content delivery GUI shall enable users to
  - Pull content packages from the system.
- Data mining GUI shall enable users to
  - Create, schedule, and view reports.
- User support GUI shall enable users to
  - Submit inquires and receive responses.
  - Search knowledge base.

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. (Release 1B; Must)

- Search GUI shall enable users to
  - Submit queries against content and metadata including bibliographic records.
  - View, sort, and categorize results.
- 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.

- Access GUI shall enable users to
    - View relationships between content packages, between digital objects, and between content packages and digital objects.
- Cataloging GUI shall enable users to
    - View and export metadata.
- Reference tools GUI shall enable users to
    - Access reference tools.
- User support GUI shall enable users to
    - Search knowledge base.
    - Subscribe and unsubscribe to alert services.
    - Access training materials.
    - Submit inquires and receive responses.
- Content delivery GUI shall enable users to
    - Pull content packages from the system.
    - View content rendered for electronic presentation.
- Data mining GUI shall enable users to
    - Create, schedule, and view reports.

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. (Release 1B; Could / Release 2; Must)

- Data Mining GUI shall enable users to
    - Create, schedule, and view reports.

7.7.2.4.8 The system must provide a default user interface for authorized Systems Administrators / Operations Managers that includes but is not limited to the following tools. (Release 1A; Must)

- Security GUI shall enable users to
    - 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.

- Content processing GUI shall enable users to
    - Manage content packages.
    - Manage content processes.
    - Transfer content from the system.
    - Perform records management functions.
- Authentication GUI shall enable users to
    - Manage authentication processes including content certification and integrity marks.
    - Monitor content integrity and receive notification of changes to content.
- Search GUI shall enable users to
    - Manage and configure search tools.
- Storage GUI shall enable users to
    - Manage storage.
    - Monitor storage.
- Workflow GUI shall enable users to
    - Manage workflows, activities, and work lists.
    - Monitor all workflows.
    - Send notifications.
- ESB GUI shall enable users to
    - Configure all ESB processes.
    - Manage business processes.
    - Perform administrative tasks.
    - Monitor all processes.
- Data mining GUI shall enable users to
    - Manage default report templates.
    - Input supplemental data.
    - Input parameters for data normalization.
    - Extract data for analysis.
    - Create, schedule, and view reports.

3.2.7.8 User Support

GPO has a strong commitment to provide superior customer service and user support. This commitment spans from assisting Content Originators at the stage of content creation to providing services that assist users in using GPO's diverse array of tangible and electronic products. User support will provide answers to user questions and direct them to content and services. User support services include a helpdesk and knowledge base, interactive training, real-time alert services, and services that provide the capability for users to receive personalized support based on their stored preferences. User support will also be provided in conjunction with the public End User interface and will provide the capability for users to submit personal information to the system. End Users will not be required to submit personal information, however it may be needed to provide some user support features. User support will provide the capability to submit personal information to the system for all user classes. User support will be provided to all users that interact with the system. This may include answering inquiries and resolving customer complaints as well as providing any technical assistance needed for the online bookstore.

3.2.7.8.1 Current Situation

GPO has a strong commitment to provide superior customer service and user support. This commitment spans from assisting Content Originators at the stage of content creation to providing services that assist users in using GPO's diverse array of tangible and electronic products. Numerous GPO departments have established various user support systems and procedures.

Information Dissemination utilizes a Customer Relations Management (CRM) application from RightNow Technologies and associated knowledge base to assist GPO Access users. The knowledge base that has been populated with answers to frequently asked questions related to the following services: GPO Access, the U.S. Government Online Bookstore, and the Federal Depository Library Program. Users can currently search or browse the knowledge base as a whole or by category / subcategory. Questions that cannot be answered by the knowledge base can be sent to GPO using the "Ask a Question" tab, and questions will be routed to the appropriate subject specialists within GPO. The knowledge base is constantly being updated and expanded based on user inquiries. The application also has reporting, chat, and other support capabilities. The GPO Contact Center uses an Automatic Call Distribution (ACD) System from Avaya to manage and route incoming calls. GPO also uses Symon Enterprise Server and Vista Software to monitor and provide real-time stats on the helpdesk.

The Institute for Federal Printing and Electronic Publishing (IPFEP) and ePUB are other examples of current GPO user support mechanisms for federal agencies. These services not only assist users but also add substantial value to customer and user experiences with GPO.

Customer Service currently provides the majority of its support through telephone, facsimile, and e-mail correspondence. The majority of user support in the form of contract administration is handled over the phone and manually documented on a GPO Form 714 - Record of visit, conference, telephone call. This form is physically stored in the job jacket with all other contracting materials. Contract administration and other customer service communications are not logged, stored or organized in an electronic system. Logging communications between GPO, contractors, and agencies is limited within the Procurement Information Control System (PICS) and is done manually.

3.2.7.8.2 Requirements for User Support

7.8.2.1 User Support Core Capabilities

7.8.2.1.1 The system shall provide multiple methods of contact for user assistance. (Multiple Releases)

7.8.2.1.1.1 The system shall provide multiple methods for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance. (Multiple Releases)

7.8.2.1.1.1.1 Web form (Release 1A; Should / Release 1B; Must)

7.8.2.1.1.1.2 Phone (Release 1A; Could)

7.8.2.1.1.1.3 E-Mail (Release 1A; Must)

7.8.2.1.1.1.4 Mail (Release 1A; Could)

7.8.2.1.1.1.5 Real-time text chat (Release 1A; Could)

7.8.2.1.1.1.6 Facsimile (Release 1A; Could)

7.8.2.1.1.1.7 Desktop Facsimile (Release 1A; Could)

7.8.2.1.1.2 The system shall provide multiple methods for GPO Service Specialists to contact End Users, Service Providers and Content Originators for user assistance. (Multiple Releases)

7.8.2.1.1.2.1 Phone (Release 1A; Could)

7.8.2.1.1.2.2 E Mail (Release 1A; Must)

7.8.2.1.1.2.3 Real-time text chat (Release 1A; Could)

7.8.2.1.1.2.4 Facsimile (Release 1A; Could)

7.8.2.1.1.2.5 Desktop Facsimile (Release 1A; Could)

7.8.2.1.2 The system shall provide users with the ability to opt-out of user support features. (Release 1B; Could)

7.8.2.1.2.1 The system shall provide users with the ability to turn on each user support feature individually.

7.8.2.1.2.2 The system shall provide users with the ability to turn off each user support feature individually.

7.8.2.2 User Support - Context Specific Help

7.8.2.2.1 The system shall provide context-specific help on user interfaces. (Release 1B; Could / Release 1C; Must)

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 1B; Could / Release 1C; Must)

7.8.2.2.1.2 Content of context specific help shall be specific to user class. (Release 1B; Could / Release 1C; Must)

7.8.2.2.1.3 Context specific help shall consist of help menus. (Release 1B; Could / Release 1C; Must)

7.8.2.2.1.3.1 Help menus shall contain user support information related to what is on the current user interface.

7.8.2.2.1.3.2 Help menus shall provide access to all available user support information for the entire system.

7.8.2.2.1.3.3 Authorized Service Specialists shall have the ability to manage information (text, images, audio, video, multimedia) in the help menu.

7.8.2.2.1.3.4 All users shall have the ability to search the help menu.

7.8.2.2.1.3.5 The system shall return search results to the user.

7.8.2.2.1.3.6 All users shall have the ability to navigate the help menu using an index.

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)

7.8.2.2.1.4.1 GPO Service Specialists shall have the ability to manage customizable descriptive text.

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)

7.8.2.2.1.5.1 All users shall have the ability to click on help icons or text.

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.

7.8.2.2.1.5.3 Authorized GPO Service Specialists shall have the ability to manage information (text, images, audio, video, multimedia) displayed as a result of clicking on help icons or text.

7.8.2.2.1.5.4 Authorized GPO Service Specialists shall have the ability to place help icons or text where needed on the user interface.

7.8.2.2.1.5.5 All users shall have the ability to view information displayed by clickable help icons.

7.8.2.3 User Support - Helpdesk

7.8.2.3.1 The system shall have the capability to support a helpdesk to route, track, prioritize, and resolve user inquiries to GPO Service Specialists. (Release 1B; Must)

7.8.2.3.2 Information collected and maintained by the helpdesk must comply with GPO and Federal privacy policies. (Release 1B; Must)

7.8.2.3.2.1 Information collected and maintained by the helpdesk must comply with “Records maintained on individuals” Title 5 *U.S. Code* Sec. 552a, 2000 edition.

7.8.2.3.2.2 Information collected and maintained by the helpdesk must comply with H.R. 2458, E-Government Act of 2002.

7.8.2.3.3 The system shall have the capability to receive inquiries from registered and non-registered users. (Release 1B; Must)

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.

7.8.2.3.4 Users shall have the capability to select from lists of categories when submitting inquiries. (Release 1B; Could / Release 1C; Must)

7.8.2.3.4.1 Users shall have the capability to select from subgroups of categories when submitting inquiries.

7.8.2.3.4.2 Authorized users shall have the capability to manage categories and subcategories.

7.8.2.3.5 Content Originators and End Users shall have the capability to attach files when submitting inquiries. (Release 1B; Could / Release 1C; Must)

7.8.2.3.6 The system shall have the capability to notify users that their inquiry has been received. (Release 1B; Could / Release 1C; Must)

7.8.2.3.7 The system shall have the capability to time and date stamp all inquiries and responses. (Release 1B; Could / Release 1C; Must)

7.8.2.3.8 The system shall have the capability to notify designated Service Specialists that they have been assigned an inquiry. (Release 1B; Could / Release 1C; Must)

7.8.2.3.9 The system shall have the capability to route, track, and prioritize inquiries and responses received. (Release 1B; Must)

7.8.2.3.10 The system shall allow a Service Specialist to manually create a new inquiry in order to accommodate inquiries that do not enter the system electronically. (Release 1B; Must)

7.8.2.3.11 The system shall provide the capability to queue inquiries. (Release 1B; Could / Release 1C; Must)

7.8.2.3.12 The system shall support priority processing. (Release 1B; Could / Release 1C; Must)

7.8.2.3.13 The system shall allow authorized users to manage the status categories for inquires. (Release 1B; Could / Release 1C; Must)

7.8.2.3.14 The system shall provide the capability for authorized users to restrict access to inquiry tracking. (Release 1B; Must)

7.8.2.3.15 The system shall provide automated routing of inquiries to the departments/individuals according to workflow guidelines, including but not limited to. (Release 1B; Could / Release 2; Must)

7.8.2.3.15.1 Automated inquiry routing shall be based on selections made by the user when an inquiry is made.

7.8.2.3.15.2 Automated inquiry routing shall be based on keywords in the inquiry sent by the user.

7.8.2.3.15.3 Automated inquiry routing shall be based on the user class of the inquirer.

7.8.2.3.15.4 The system shall allow authorized users to set routing preferences based on selections made, keywords and user class.

7.8.2.3.16 GPO Service Specialists shall have the capability to route inquiries to other Service Specialists based on the needs of the End User or Content Originator. (Release 1B; Could / Release 1C; Must)

7.8.2.3.16.1 GPO Service Specialists shall have the ability to route an inquiry to a selected individual.

7.8.2.3.16.2 GPO Service Specialists shall have the ability to route an inquiry to a selected department.

7.8.2.3.16.3 GPO Service Specialists shall have the ability to route inquiries to users who do not have access to the system using e-mail.

7.8.2.3.17 The system shall allow the user to determine the departments or individuals they wish to request answers from. (Release 1B; Could / Release 1C; Must)

7.8.2.3.18 The system shall provide the capability to request user feedback regarding quality of response given. (Release 1B; Could / Release 1C; Must)

7.8.2.3.19 The system shall provide users with access to history of their inquiries and responses. (Release 1B; Could / Release 1C; Must)

7.8.2.3.20 The system shall store inquiries and responses. (Release 1B; Must)

7.8.2.3.21 The system shall have the capability to allow authorized users to amend inquiries and responses. (Release 1B; Could / Release 1C; Must)

7.8.2.3.22 The system shall have the capability for users to search inquiries and responses. (Release 1B; Must)

7.8.2.3.23 The system shall allow authorized users to search by user-specific fields, including but not limited to job number, order number, agency, status, and inquiry number. (Release 1B; Must)

7.8.2.3.24 The system shall support the capability to monitor the quality of responses given by helpdesk staff. (Release 1B; Could; / Release 2; Must)

7.8.2.3.25 The system shall have the capability to provide users with access to questions and answers from other users related to their queries. (Release 1B; Could / Release 1C; Must)

7.8.2.3.25.1 The system shall allow for search of questions and answers from other users.

7.8.2.3.25.2 The system shall provide the capability to assign user access rights to individual questions and answers.

7.8.2.3.26 The system shall provide the capability to identify GPO users responding to user inquiries. (Release 1B; Must)

7.8.2.3.27 The system shall provide the capability to log information exchanges. (Release 1B; Must)

7.8.2.3.27.1 Information exchange logs shall store metadata relating to what is being discussed.

- Type of exchange (e.g., e-mail, phone, fax)
- Exchange sent by
- Exchange sent to
- Content of exchange
- Job Unique ID, when available
- Package Unique ID, when available
- Other fields customizable by GPO

7.8.2.3.28 The system shall provide the capability to spell-check inquiries and responses before submission. (Release 1B; Could)

7.8.2.4 User Support - Knowledge Base

7.8.2.4.1 The system shall allow GPO Service Specialists, GPO Business Managers, and other users as authorized to add information to a knowledge base. (Release 1B; Must)

7.8.2.4.2 The system shall provide the ability for GPO Service Specialists, GPO Business Managers, and other users as authorized to add electronic files to the knowledge base as attachments. (Release 1B; Must)

7.8.2.4.3 The system shall provide the capability to create customized templates for knowledge base entries. (Release 1B; Could)

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.

7.8.2.4.4 The system shall have the capability to time and date stamp all knowledge base entries. (Release 1B; Must)

7.8.2.4.5 The system shall provide the ability for authorized users to manage information in the knowledge base. (Release 1B; Must)

7.8.2.4.6 The system shall provide the capability to add inquiries and answers from the helpdesk to the knowledge base. (Release 1B; Must)

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.

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.

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 1B; Must)

7.8.2.4.8 The system shall provide the capability to store standard responses for use by specific user groups or subgroups. (Release 1B; Could / Release 1C; Must)

7.8.2.4.9 The system shall allow for information stored in the knowledge base to have role-based access restrictions. (Release 1B; Must)

7.8.2.4.9.1 The system shall allow for access restrictions to be applied to complete categories.

7.8.2.4.9.2 The system shall allow for access restrictions to be applied to individual knowledge base entries.

7.8.2.4.10 The system shall provide the capability for all users to search the knowledge base. (Release 1B, Must)

7.8.2.4.10.1 The system shall provide the capability for all users to perform a full-text search the knowledge base.

7.8.2.4.10.2 The system shall provide the capability for all users to search the knowledge base by phrase.

7.8.2.4.10.3 The system shall provide the capability for all users to search the knowledge base by identification number.

7.8.2.4.11 The system shall provide the capability to sort results of knowledge base searches. (Release 1B, Must)

7.8.2.4.11.1 The system shall provide the capability to sort search results by category.

7.8.2.4.11.2 The system shall provide the capability to sort search results by subject.

7.8.2.4.11.3 The system shall provide the capability to sort search results by a default sort.

7.8.2.4.12 The system shall provide the capability for all users to receive e-mail updates when the content of information stored in a knowledge base entry is updated. (Release 1B; Could / Release 2; Must)

7.8.2.4.13 The system shall provide the capability to perform records management functions on knowledge base data. (Release 2; Must)

7.8.2.4.14 The system shall provide the capability to spell-check knowledge base entries before submission. (Release 1B, Could)

7.8.2.5 User Support - Alerts

7.8.2.5.1 The system shall have the capability to provide alert services.

7.8.2.5.1.1 The system shall allow all users to subscribe and unsubscribe to alert services. (Release 1C; Could / Release 2; Must)

7.8.2.5.1.2 Alert services shall be provided in the following formats: (Release 1C, Could / Release 2: Must)

- E-mail messages
- RSS Feeds conforming to the RSS 2.0 Specification.
- Messages while logged into FDsys

7.8.2.5.1.3 The system shall allow users to customize alert services. (Release 1C; Could / Release 2; Must)

7.8.2.5.1.4 The system shall provide alerts based on user profiles and history. (Release 1C; Could / Release 2; Must)

7.8.2.5.1.5 The system shall have the capability to automatically send alerts based on system events. (Release 1C; Could / Release 2; Must)

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 1C; Could / Release 2; Must)

7.8.2.5.1.7 The system shall have the capability to automatically send alerts based on job processing events. (e.g., order submitted, proofs returned, order shipped) (Release 1C; Must)

7.8.2.5.1.8 Authorized users shall be able to create new alert categories where new alerts are manually generated. (Release 1C; Could / Release 2; Must)

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)

7.8.2.5.1.10 The system shall have the capability for GPO users to recommend alerts for addition to the knowledge base. (Release 1C; Could / Release 2; Must)

7.8.2.6 User Support - Training and Events

7.8.2.6.1 The system shall provide users access to training materials and training history. (Release 1C; Could)

7.8.2.6.1.1 The system shall provide access to training materials supplied as digital video.

7.8.2.6.1.2 The system shall provide access to training materials supplied as digital documents.

7.8.2.6.1.3 The system shall provide access to training materials supplied as digital audio.

7.8.2.6.1.4 The system shall provide access to training materials supplied as digital multimedia.

7.8.2.6.1.5 The system shall provide access to training materials supplied in other formats.

7.8.2.6.2 The system shall allow authorized users as determined by GPO Operations Managers to manage training materials and training history. (Release 1C; Could)

7.8.2.6.3 The system shall have the capability for authorized users as determined by GPO Operations Managers to restrict access to training material and training history. (Release 1C; Could)

7.8.2.6.3.1 Access restrictions to training materials shall be based on user class.

7.8.2.6.3.2 Access restrictions to training materials shall be based on individual users.

7.8.2.6.4 The system shall allow users to enroll in training and events. (Release 1C; Could)

7.8.2.6.5 The system shall allow authorized users as determined by GPO Operations Managers to manage training and events. (Release 1C; Could)

7.8.2.6.6 The system shall provide interactive training. (Release 2; Could)

7.8.2.6.6.1 The system shall provide interactive self-paced training.

7.8.2.6.6.2 The system shall provide interactive instructor-led training.

7.8.2.6.7 The system shall provide users verification of enrollment in training and events. (Release 2; Could)

7.8.2.6.8 The system shall provide the capability for users to measure their progress and performance. (Release 3; Could)

7.8.2.6.9 The system shall provide the capability for users to provide feedback on training. (Release 3; Could)

7.8.2.6.10 The system shall provide online tutorials. (Release 2; Could)

3.2.8 CONTENT DELIVERY AND PROCESSING

Content delivery encompasses the delivery of pre-ingest bundles (PIBs) and Dissemination Information Packages (DIPs). PIBs contain digital objects, business process information and metadata required for service providers to output proofs and produce end products or services. DIPs contain digital objects, business process information and metadata based to facilitate user requests.

Transformation and assembly processes will take place in delivery processing. Access Content Packages (ACP) will be transformed into DIPs and PIBs will be assembled. Archival Information Packages (AIPs) will be transformed into DIPs as necessary for preservation by other organizations. Digital objects may be adjusted based on user requests to support the delivery of hard copy, electronic presentation and digital media.

3.2.8.1 Current Situation

Under legal authority of Title 44, Chapters 17, 19, and 41 of the United States Code, GPO's Office of Information Dissemination (Superintendent of Documents) administers various dissemination programs with the mission of providing permanent public access to official Federal Government information. These include the Federal Depository Library Program (FDLP), GPO Sales Program, and GPO Access public Web site. The FDLP distributes electronic and tangible publications to a network of Federal Depository libraries across the country. Electronic versions of many, but not all, publications are delivered to the public via GPO Access in PDF, ASCII text, and HTML file formats. These formats are manually converted from the files supplied to GPO for printing.

Using GPO Access, end users can subscribe to RSS feeds for "FDLP News and Updates" and "GPO Access: What's New." These RSS feeds can be read using a news reader or a news aggregator, which must be downloaded from a third party and installed on the end user's computer.

Agencies currently submit their files to GPO' in the form of removable digital media, camera copy or film and there is not a system in place for GPO to electronically deliver this content to service providers. Occasionally, files may be e-mailed to service providers; however file size limitations and occasional file corruption of fonts prevent this from being an acceptable means to deliver content to service providers.

3.2.8.2 Requirements for Content Delivery and Processing

8.2.1 Content Delivery Core Capabilities

8.2.1.1 The system shall have the capability to retrieve ACPs from Access Content Storage based on user request. (Release 1B; Must)

8.2.1.2 The system shall have the capability to create DIPs from ACPs in delivery processing based upon a user request. (Release 1B; Must)

8.2.1.3 The system shall have the capability to create PIBs in delivery processing. (Release 1B; Must)

8.2.1.4 The system shall have the capability to deliver DIPs and PIBs based on requests. (Release 1B; Must)

8.2.1.5 The system shall have the capability to push DIPs and PIBs to users. (Release 1B; Must)

8.2.1.6 Users shall have the ability to pull DIPs and PIBs from the system. (Release 1B; Must)

8.2.1.7 The system shall have the capability to restrict Service Providers' access to DIPs and PIBs for jobs that they have not been awarded. (Release 1B, Must)

8.2.1.8 The system shall have the capability to determine if delivery is possible. (Release 1C; Must)

8.2.1.8.1 The system shall have the capability to determine if delivery is possible based upon business rules.

8.2.1.8.2 The system shall have the capability to determine if delivery is possible based upon limitations of delivery mechanisms.

8.2.1.8.3 The system shall have the capability to determine if delivery is possible based upon limitations of content formats.

8.2.1.8.4 The system shall have the capability to inform users that delivery is not possible.

8.2.1.8.5 The system shall have the capability to inform users why delivery is not possible.

8.2.1.9 The system shall have the capability to provide users with estimated transfer time for delivery. (Release 1B; Could)

8.2.1.10 The system shall have the capability to provide notification of fulfillment to users. (Release 1C; Must)

8.2.1.10.1 The system shall have the capability to provide notification based on user preferences. (Release 1C; Should / Release 2; Must)

8.2.1.10.2 The system shall have the capability to provide notification based on information gathered at time of request. (Release 1C; Must)

8.2.2 Content Delivery Processing

8.2.2.1 The system shall have the capability to package DIPs containing the digital object, metadata, and BPI. (Release 1B; Must)

8.2.2.2 The system shall have the capability to assemble PIBs containing digital objects, business process information and metadata required for service providers to output proofs and produce end product or service. (Release 1B; Must)

8.2.2.3 The system shall have capability to transform digital objects to different formats. (Release 1B; Must)

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)

8.2.2.4.1 The system shall have the capability to adjust the resolution of digital objects.

8.2.2.4.2 The system shall have the capability to resize digital objects.

8.2.2.4.3 The system shall have the capability to adjust the compression off digital objects.

8.2.2.4.4 The system shall have the capability to adjust the color space of digital objects. (e.g., CMYK to RGB)

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)

8.2.2.4.6 The system shall have the capability to rasterize digital objects.

8.2.2.5 The system shall have the capability to process DIPs based on user request. (Release 1B; Must)

8.2.2.6 The system shall have the capability to repurpose content from multiple packages into a single DIP. (Release 2; Must)

8.2.3 Content Delivery Mechanisms

8.2.3.1 The system shall have the capability to push DIPs and PIBs to users using various delivery mechanisms, including, but not limited to the following: (Release 1B; Must)

- RSS feeds conforming to the RSS 2.0 Specification.
- E-mail
- Transfer Control Protocol/Internet Protocol, including but not limited to File Transfer Protocol.
- Other mechanisms as needed to support delivery to digital media devices.

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 Hard Copy Output

Hard copy output is tangible printed content (e.g., ink on paper) produced from digital files. Hard copy output may be requested as an Access request or through the Content Originator ordering user interface. Content Originator’s will include information on the desired output such as color attributes, trim sizes, binding preferences. For Content Originator ordering, hard copy output will be generated from PIBs. DIPs will be used to generate hard copy output based upon request and Content Originator re-orders.

3.2.8.3.1 Current Situation

The functional areas for hard copy production are the Federal agency, Congress, GPO Plant Operations, GPO Customer Services, and external contractors.

GPO's Customer Services department is responsible for coordinating the contracting and procurement process for Federal agencies and Congress. They handle the entire process including determining which procurement vehicle to utilize, writing specifications, obtaining bids from Service Providers, selecting the contractor, contract administration, and quality assurance. The department uses numerous legacy systems to manage this process. Additionally, GPO accepts any file types from Content Originators for production. The most common formats are Adobe InDesign, Quark XPress, Microsoft Word, and Adobe Acrobat Portable Document Format (PDF).

GPO's Plant Operations department primarily responsible for production of Government publications including United States Passports, the Federal Register, and the United States Code of Federal Regulations. The department also prints select Federal agency work traditionally procured by Customer Services.

3.2.8.3.2 Requirements for Hard Copy Output

8.3.2.1 Hard Copy Output Core Capabilities

8.3.2.1.1 The system shall have the capability to deliver DIPs and PIBs to users from which hard copy output can be created. (Release 1B; Must)

8.3.2.1.1.1 The system shall have the capability to provide DIPs and PIBs that support the production of hard copy on any required hard copy output technology (e.g., offset press, digital printing).

8.3.2.1.2 The system shall have the capability to deliver DIPs and PIBs that support static text and images. (Release 1B; Must)

8.3.2.1.3 The system shall have the capability to support hard copy output for variable data printing processes. (Release 1C; Could)

8.3.2.1.4 The system shall have the capability to add the GPO Imprint line to DIPs and PIBs per the GPO Publication 310.2 and the New Imprint Line Announcement. (Release 1B; Could)

8.3.2.1.4.1 The system shall allow users to manually add the Imprint line.

8.3.2.1.4.2 The system shall automatically add the Imprint Line.

8.3.2.1.4.3 The system shall allow users to manually adjust the location of the Imprint line.

8.3.2.1.5 DIPs and PIBs for hard copy output shall be delivered in file formats that conform to industry best practices. (Release 1B; Must)

8.3.2.1.5.1 The system shall have the capability to deliver files in their native application file format.

8.3.2.1.5.1.1 The system shall have the capability to convert native files to PDF.

8.3.2.1.5.2 The system shall have the capability to deliver optimized (print, press) PDFs.

8.3.2.1.5.2.1 Optimized PDFs shall have fonts and images embedded.

8.3.2.1.5.2.2 Image resolution of PDF's shall conform to industry best practices as defined in GPO's press optimized PDF settings.

8.3.2.1.5.3 The system shall have the capability to deliver page layout files containing images, fonts, and linked text files, including but not limited to:

- Adobe InDesign
- QuarkXPress
- Adobe Framemaker
- Adobe Pagemaker

8.3.2.1.5.4 The system shall have the capability to deliver vector graphics.

8.3.2.1.5.5 The system shall have the capability to deliver raster images.

8.3.2.1.5.6 The system shall have the capability to deliver Microsoft Office Suite application files, including but not limited to:

- Word
- PowerPoint
- Excel
- Visio

8.3.2.1.5.7 The system shall have the capability to deliver XML.

8.3.2.1.5.7.1 The system shall support cascading style sheets.

8.3.2.1.5.7.2 The system shall support document type definition/schema.

8.3.2.1.5.8 The system shall have the capability to deliver text files, including but not limited to:

- Rich Text (RTF)
- ASCII text
- Unicode
- Universal Multi-Octet Coded Character Set - ISO/IEC 10646

8.3.2.1.5.9 The system shall have the capability to deliver OASIS Open Document Format for Office Applications (OpenDocument) v1.0.

8.3.2.1.5.10 The system shall have the capability to deliver postscript files.

8.3.2.1.6 The system shall have the capability to generate DIPs and PIBs that contain Job Definition Format (JDF) data. (Release 3; Could)

3.2.8.4 Electronic Presentation

Electronic presentation output is the dynamic and temporary representation of content in digital format on End User devices, including computers and non-desktop electronic devices. Electronic presentation encompasses presenting images, text, video, audio and multimedia in electronic form.

3.2.8.4.1 Current Situation

The FDLP distributes electronic and tangible publications to a network of Federal Depository libraries across the country. GPO Access, the primary vehicle for the dissemination of electronic publications via the FDLP, provides public access to full-text databases of official Federal publications at no fee.

Many agency customers are also requesting from GPO, and GPO's affiliated contractors, repurposed digital files that they can place on line for viewing and/or download. Agencies requiring repurposed digital files may go through Production or Printing Procurement. Once the printed product is completed the files are repurposed for screen usage. Few files are currently created for strictly digital output.

Once a repurposed digital file has been created from the scanned hard copy or the digital input, additional features such as bookmarks, links, and indexing may be added to certain digital file types (PDF, etc.). A choice of file formats including PDF, JPG, ASCII, etc., may be provided back to the customer, with PDF being the most commonly requested format. Fillable PDF files for online use may be created from both hard copy and existing digital files.

When a repurposed digital file is requested in addition to the printed product, the file type and media to be returned to the customer are identified on the order form, along with any additional requirements. Once the printed publication is completed, the specified digital file should be created from the production files and should be an exact representation of the printed product (format, structure, etc.). The file will be supplied to the agency in the format and on the media requested on the order form. This process should be followed by GPO's in-house production facilities and outside contractors.

Many customers also request Web page capabilities in the form of digital files, typically HTML. Printing Procurement can request digital files such as HTML from outside vendors. Various areas of Production can also produce digital files and, in addition, can create and/or maintain Web sites for agency customers.

Agencies requiring digital file creation may submit an order form to Printing Procurement for bidding by contractors. The written specifications include information on the hard copy or file type and media submitted to the contractor, as well as the file type and media to be returned to the customer. Additional requirements for repurposed deliverables include searching capabilities, metadata creation, etc. Additional requirements for repurposed digital files with Web page capabilities (such as HTML) include coding, version compatibility, etc. Repurposed Deliverables Specification Language is available for inclusion into specifications. This language includes specific requirements for PDF and HTML deliverables. Once specifications are complete, bids are solicited and accepted in the same way they would be for a hard copy job described above.

In addition to customer agencies, GPO's ID section also utilizes digital files for soft copy display. Files submitted to Information Dissemination (from both In Plant Production and outside contractors) are evaluated to determine if they fall within the scope of ID programs. When a file is determined to be within scope, it is further processed for display on GPO Access. Additional derivatives may be created for different purposes from the existing digital file. Examples of processing options include WAIS database indexing and optimizing for placement on a web server. Additional requirements such as OCR scanning, bookmarks, breaking large files into smaller more easily downloaded components, etc., are available to the ID department.

3.2.8.4.2 Requirements for Electronic Presentation

8.4.2.1 Electronic Presentation Core Capabilities

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 1B; Must)

8.4.2.1.2 The system shall have the capability to render content for presentation on end user devices. (Release 1B; Must)

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 1B; Must)

8.4.2.1.4 The system shall have the capability to render content for presentation on non-desktop electronic devices, including but not limited to: (Release 1B; Should / Release 1C; Must)

- Personal Digital Assistants (PDAs)
- Digital Audio Players
- Electronic Books (E-Books)
- Cell Phones

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 1B; Could)

8.4.2.1.6 The system shall provide the capability to deliver DIPs that support static and dynamic text in multiple formats, including, but not limited to: (Release 1B; Must)

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)

8.4.2.1.6.2 The system shall have the capability to deliver electronic content in HTML with linked files (e.g., JPEG, GIV, MPEG, MP3) referenced in the HTML code conforming to the HTML 4.0.1 Specification. (Release 1B; Must)

8.4.2.1.6.3 The system shall have the capability to deliver electronic content in XHTML with linked files (e.g., JPEG, GIV, MPEG, MP3) referenced in the XHTML code conforming to the XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition) specification. (Release 1B; Must)

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)

8.4.2.1.6.4.1 The system shall have the capability to convert images to descriptive ASCII text. (Release 1B; Must)

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)

8.4.2.1.6.5.1 The system shall have the capability to convert images to descriptive Unicode text. (Release 1B; Must)

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; Could)

8.4.2.1.6.7 The system shall have the capability to deliver electronic content in MS Office formats. (Release 1B; Must)

- Microsoft Excel (.xls)
- Microsoft Word Document File Format (.doc)
- Microsoft PowerPoint File Format (.ppt)
- Microsoft Publisher File Format (.pub)

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)

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 1B; Could)

8.4.2.1.7 The system shall provide the capability to deliver DIPs that support static and dynamic images in multiple formats, including, but not limited to: (Release 1B; Must)

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.

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.

8.4.2.1.7.3 The system shall have the capability to deliver electronic content in TIFF conforming to TIFF – Revision 6.0.

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.

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.

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.

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:

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 1B; Must)

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 1B; Could)

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 1B; Could)

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 1B, Must)

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 1C, Should / Release 2; Must)

8.4.2.1.10 The system shall have the capability to deliver electronic content that maintains desired user functionality. (Release 1B; Must)

8.4.2.1.10.1 The system shall deliver electronic content that maintains hyperlinks to the extent possible.

8.4.2.1.10.2 The system shall deliver electronic content that maintains interactive content.

3.2.8.5 Digital Media

Digital media is a content delivery mechanism consisting of data storage devices. The digital media component of FDsys includes the delivery of content for storage on the following:

- Removable data storage devices (e.g., CD, DVD)
- Multifunctional/handheld devices (e.g., PDA, MP3 players, e-books)
- Storage at user sites (e.g., servers, personal computer)

Duplication/replication of removable digital media will be available through internal and external Service Providers. The system will determine how to deliver content to support storage on digital media.

Content may be pushed to a user's multifunctional device, or requested and pulled from the system. The system will determine how to deliver content to the user's device and offer options for delivery to those devices, when options are available.

3.2.8.5.1 Current Situation

The primary digital media type currently used at GPO is the compact disk (CD). CDs may be formatted for both Macintosh and Windows computers. Virtually all computer systems are able to read CDs, making them the most widely accepted form of removable digital media available today. GPO' s Plant Production division accepts, outputs, duplicates, and replicates CDs. CDs are also duplicated and replicated by service providers for agency customers.

GPO is working on expanding its in-house Digital Video Disk (DVD) capabilities. Some areas of Production currently have the ability to read and/or write DVDs, while others do not. The section that replicates CDs has DVD equipment in place and is conducting testing on DVD replication. Until testing is completed, a contract with a service provider is in place to handle DVD replication work from customers.

Many outdated types of media, such as floppy disks, ZIP drives, etc., are no longer typical at GPO. However, customers with older media may be able to submit their digital files to GPO's Production section for hard copy output and in addition have the files returned to them on a CD.

Jobs that do not go through GPO's in-house facilities are submitted to Agency Publishing Services. Specifications can be written for any type of digital media provided by the agency customer and will be procured from an outside service provider. While the most common form of media accepted by contractors is the CD, many contractors have the capability of utilizing other media.

3.2.8.5.2 Requirements for Digital Media

8.5.2.1 Digital Media Core Capabilities

8.5.2.1.1 The system shall have the capability to deliver PIBs and DIPs for digital media containing electronic content for electronic presentation, hard copy output or data storage. (Release 1B, Must)

8.5.2.1.2 The system shall have the capability to deliver PIBs and DIPs that support the creation of removable digital media. (Multiple Releases)

8.5.2.1.2.1 The system shall have the capability to deliver PIBs and DIPs that support the creation of removable optical digital media, including, but not limited to: (Multiple Releases)

8.5.2.1.2.1.1 Compact Discs (CD) (Release 1B, Must)

8.5.2.1.2.1.2 Digital Versatile Discs (DVD) (Release 1B, Must)

8.5.2.1.2.1.3 Blu-ray Discs (BD) (Release 1B, Could)

8.5.2.1.2.2 The system shall have the capability to deliver PIBs and DIPs that support the creation of removable magnetic digital media, including but not limited to: (Release 1B, Must)

- Magnetic tapes
- Removable magnetic hard disks (e.g., hard drives)
- Magnetic Floppy Disks or Diskettes

8.5.2.1.2.3 The system shall have the capability to deliver PIBs and DIPs that support the creation of removable semiconductor digital media, including but not limited to: (Release 1B, Must)

- Universal Serial Bus (USB) Flash drives
- Flash memory cards

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)

8.5.2.1.2.4.1 The system shall have the capability to generate ISO image files.

8.5.2.1.2.4.2 The system shall have the capability to generate VCD image files.

8.5.2.1.2.4.3 The system shall have the capability to generate UDF image files.

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)

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.

8.5.2.1.3 The system shall have the capability to deliver DIPs and PIBs to digital media.

8.5.2.1.3.1 The system shall have the capability to deliver DIPs and PIBs to GPO storage devices. (e.g., GPO servers). (Release 1B, Must)

8.5.2.1.3.2 The system shall have the capability to deliver DIPs and PIBs to non-GPO storage devices. (e.g., customer servers, service provider servers) (Release 1B, Should / Release 1C; Must)

8.5.2.1.3.3 The system shall have the capability to deliver DIPs and PIBs to non-desktop electronic devices, including, but not limited to: (Release 1B; Should / Release 1C; Must)

- Personal digital assistants (PDAs)
- Digital audio players
- Electronic books (E-Books)
- Cell phones

Appendix A – Acronyms and Glossary

Acronyms

ACRONYM	DEFINITION
ABLS	Automated Bid List System
ACES	Access Certificates for Electronic Services
ACP	Access Content Package
ACSIS	Acquisition, Classification, and Shipment Information System
ACS	Access Content Storage
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
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
CD-ROM	Compact Disk Read Only Memory
CDN	Content Delivery Network
CE	Content Evaluator
CFR	Code of Federal Regulations
CGP	Catalog of U.S. Government Publications
CMS	Content Management System
CMYK	Cyan, Magenta, Yellow, Black
Content Originator	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
DO	Digital Objects
DNS	Domain Name System
DOI	Digital Object Identifier
DoS	Denial of Service
DPI	Dots Per Inch
DVD	Digital Versatile Disc
EAD	Encoded Archival Description
ePub	Electronic Publishing Section
FAQ	Frequently Asked Question

ACRONYM	DEFINITION
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
FOIA	Freedom of Information Act
FOB	Free on Board
FTP	File Transfer Protocol
GAO	General Accounting Office
GAP	GPO Access Package
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
IEEE	Institute of Electronics and Electrical Engineers
IETF	Internet Engineering Task Force
ILS	Integrated Library System
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISBN	International Standard Book Number
ISSN	International Standard Serial Number
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
JDF	Job Definition format
LDAP	Lightweight Directory Access Protocol
LOC	List of Classes
LPI	Lines Per Inch
MAC	Message Authentication Code
MARC	Machine Readable Cataloging
METS	Metadata Encoding and Transmission Standard
MMAR	Materials Management Procurement Regulation
MOCAT	Monthly Catalog of Government Publications
MODS	Metadata Object Descriptive Schema
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
OAIS	Open Archival Information Systems
OCLC	Online Computer Library Center
OCR	Optical Character Recognition

ACRONYM	DEFINITION
PCCS	Printing Cost Calculating System
PDA	Personal Data Assistant
PDF	Portable Data Format
PDI	Preservation Description Information
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
PREMIS	PREservation Metadata: Implementation Strategies
PRONOM	Practical Online Compendium of File Formats
PPR	Printing Procurement Regulation
PURL	Persistent URL
RAID	Redundant Array of Inexpensive Disks
RFC	Request for Comments
RGB	Red, Green, Blue
RI	Representation Information
ROI	Return on Investment
RPPO	Regional Printing Procurement Office
RSA	Rivest, Shamir, Adleman
SAML	Security Assertion Markup Language
Section 508	Section 508 of the Rehabilitation Act
SF	Standard Form
SHA	Secure Hash Algorithm
SIP	Submission Information Package
SGML	Markup Language
SMP	Storage Management Processor
SMS	Storage Management System
SPA	Simplified Purchase Agreement
SSL	Secure Socket Layer
SuDocs	Superintendent of Documents
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
URL	Uniform Resource Locator
U.S.C.	United States Code
USGPO	United States Government Printing Office
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAIS	Wide Area Information Servers
WAP	Wireless Application Protocol
WIP	Work in Process
WML	Wireless Markup Language
WMS	Workflow Management System
XML	eXtensible Markup Language
XMLENC	XML Encryption
XMLDSIG	XML Signature

Glossary

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

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

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

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

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

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

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

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

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

Archive management - See **Preservation**.

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

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

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

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

Batch: A batch is a set of data or jobs to be processed in a single program run or a quantity required for or produced as the result of one operation.

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. A born digital object will exist in an entirely digital lifecycle; relating to a document that was created and exists only in a digital format.

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

Business Manager (User Class): Develops business plans to meet Content Originator and End User expectations. Also works with GPO Sales Group to repurpose data in order to provide value added services.

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 information, non-content specific information that is used within the business process and package description (PD).

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

Certification: Proof of verification or authority. Process associated with ensuring that a digital object is authentically the content issued by the author or issuer.

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.

Compose: The ability to style/format content

Composition: Creating content using FDsys applications.

Content: Information presented for human understanding.

Content Analysis: Interpretation of intended context.

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

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

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

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

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

Converted content: Digital content created from a tangible publication.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

End User (User Class)**:** Uses the system to search for and access records, to submit data requests, request assistance via mediated searches, communicate with GPO, and invoke system services.

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

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

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

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

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

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

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

Format management -See **Preservation**.

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

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

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

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

Hard copy: Tangible printed content.

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

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

History: A record of all system activities.

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 (OAIS): The OAIS entity that contains the services and functions that accept SIPs from Producers, prepare Archival Information packages for storage, and ensure that information packages and their supporting descriptive information packages are established within OAIS.

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).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

OAIS: Open Archival Information System Reference Model (ISO 14721:2003) - A reference model for an archive, consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a designate community. The model defines functions, activities, responsibilities, and relationships within this archive, sets forth common terms and concepts, and defined component functions which serve as the basis for planning implementation.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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: (n) 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 recipient(s). 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.

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

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

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

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

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

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

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 (User Class)**:** delivers the expected services and products after receiving notifications. For example, the Service Provider accepts print orders.

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

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

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

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

Storage management - See **Preservation**.

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

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

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

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

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

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

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).

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

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

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

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

Validation: A process that ensures data 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.

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 beyond an agreed upon threshold or tolerance which constitute a new version.

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

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

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

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

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

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

Appendix B- Operational Specification for Converted Content (Version 3.3)

Digitization Specifications and Operating Procedures for Archiving Materials: Creation of Preservation Master Files

For the following content types – Textual, Graphic Illustrations / Artwork, Originals, and Photographs

United States Government Printing Office (GPO)

Final
Feb 10, 2006

FINAL

Document Change Control Sheet

Document Title: FDsys Operational Specification for Converted Content

Date	Filename/version #	Author	Revision Description
2/2/2005	*DigitizationSpecs-v.1.doc*	N. Doyle / R. Selvey	First Draft
2/18/2005	*DigitizationSpecs-v1.1.doc*	N. Doyle / R. Selvey	Additions, corrections and input from outside sources (LOC, etc.)
2/18/2005	*DigitizationSpecs-v2.0.doc*	N. Doyle / R. Selvey	Additions, corrections, visuals
3/3/2005	*DigitizationSpecs-v2.1.doc*	N. Doyle / R. Selvey	Revisions, narrowed down Standards list
4/12/2005	*DigitizationSpecs-v2.2.doc*	N. Doyle / R. Selvey	Revisions based on workflow
5/10/2005	*DigitizationSpecs-v2.3.doc*	N. Doyle / R. Selvey	All targets / standards have been established and updated.
5/31/2005	*DigitizationSpecs-v2.4.doc*	N.Doyle / R. Selvey	Sect III.C – Aimpoints have been revised / updated
6/1/2005	*DigitizationSpecs-v2.5.doc*	N.Doyle / R. Selvey	Update submission level Metadata
6/24/2005	*DigitizationSpecs-v3.0.doc*	T. Priebe	Formatted into FDsys template
09/26/05	*DigitizationSpecs-v3.1.doc*	N Doyle	Updates based on digi. suggestions
12/01/05	*DigitizationSpecs-v3.2.doc*	N.Doyle	Changed compression scheme for bitonal to CCITT Group 4
02/10/06	*FDsys Operational Spec for Converted Content - v3.3.doc*	R. Selvey	Change CCP to SIP, update references, crosswalk to other specs, update after green team review, update qc, update ID, workflow, current situation, batch processing, update table of contents
02/16/06	*FDsys Operational Spec for Converted Content - v3.3.doc*	R. Selvey	Updates after PMO review

1.0 **Scope**

What is addressed in these requirements:

- Scanning and format requirements for text, photographs, and graphic materials
- Digitization Environment
- Digitization Standards
- Required hardware/software configurations
- Quality control

Types of scanning projects will include the following:

- Brittle books (serials and monographs)
- Pamphlets and unbound material
- Archival materials
- Bound materials
- Fold-outs, maps, posters, etc.
- Microform (includes microfilm, microfiche, and aperture cards)

This specification does not describe how to create a Submission Information Package (SIP). SIP functions are outlined in the FDsys SIP requirements.

1.1. Deliverable

The end product of the Conversion Process will be a GPO standard Submission Information Package (SIP).

1.2. Overview

This specification covers all the necessary conversion elements that are required for the creation of a SIP. The components of the conversion solution have been grouped into the following: 1) Conversion Processes; 2) Content Management; 3) Storage.

Converted content is one type of digital content that will be ingested by the Future Digital System. Converted content consists of electronic files created from tangible paper documents, which can be preserved as master files with associated metadata. GPO staff and external service providers "including contractors, library partners, and federal agencies" will provide converted content to the Future Digital System. The end product of conversion is a Submission Information Package (SIP). The SIP must be produced at a level of quality that is adequate to support preservation as well as future iterations of derivative products.

This document is an outline of our scanning specifications and will continue to evolve and improve as technological advancements occur in the digital imaging industry.

2.0 **Current Situation**

2.1. Background and objectives

The present objective internally within the GPO is to establish a prototype conversion activity to develop workflow processes and metrics to create all conversion elements that are required for the creation of a SIP.

The current system was designed to test and validate the viability of various technologies and planned processes. DCS is utilizing a pilot operation during its transition period to analyze, develop, and document reporting requirements for the future system. These requirements can then be incorporated into the evaluation criteria for components of the future system and used to evaluate the cost of implementation.

2.2. *Conversion*

Scanning is the only element of the conversion solution that has been benchmarked. Other elements, such as audio and video, need definition.

2.2.1. Scanning

A conversion solution does not currently exist within GPO. Digital Conversion Services (DCS) is currently a prototype operation that is producing scanned images only.

2.2.1.1. Operational situation

Current GPO equipment:

Sixteen workstations utilizing flatbed scanners. Scanning capability is 60 pages per hour per workstation/scanner.

Two workstations utilizing Auto-Document Feed (ADF) scanners. Scanning capability is 1000 pages per hour per workstation/scanner.

Equipment Guidelines:

Flatbed Scanner

Capabilities

- Allows the operator to place a single sheet or de-bound materials face down on the scan bed.
- Suitable for reflective media (e.g. paper, other substrates).
- Suitable for transmissive media such as negatives and film.

Limitations

- Size limitations based on scanner bed imaging area.
- Productivity dependant on operator performance.
- Fragile and brittle looseleaf books

Overhead Scanner/Digital Camera: Auto-page turning

Capabilities

- Suitable for bound or non-destructible material.
- Automated features rely less on speed of the operator.
- Scans pages while unattended or multi-tasking.

Limitations

- Not suitable for fragile or brittle material.
- Not suitable for looseleaf or de-bound material.
- Size limitations based on camera/scanner imaging area.

Overhead Scanner/Digital Camera: Manual-page turning

Capabilities

- Suitable for fragile and brittle material.

Limitations

- Productivity dependant on operator performance.
- Size limitations based on camera/scanner imaging area.

Auto-document Feed scanner

Capabilities

- High volume automated processing.
- Suitable for de-bound or destructible material.

Limitations

- Scans a limited volume of pages at a time based on the tray size.
- Occasionally introduces distortions due to moving or rotation of pages within the feeder.
- Size limitations based on scanner imaging area.
- Not suitable for rare, valuable, or brittle material.

Film Scanner

Capabilities

- Achieves higher resolution necessary for the type/size of media.
- Higher quality and dynamic range.
- Used for all types of transmissive media (e.g. *microfiche, microform, negatives, aperture cards, and E-6 slides*).

Limitations

- Some film scanners are limited to certain types of media sizes (i.e. 35 mm, medium format, etc), therefore more than one type may be necessary.

2.2.1.2. Metrics

Current GPO Capabilities

Scanning capability for flatbed workflow given existing resources is 60 pages per hour per workstation/scanner.

Environment

A variety of factors will affect the appearance of images, whether displayed or printed on reflective, transmissive or emissive devices or media. Those factors that can be quantified must be controlled to assure proper representation of an image by its environment.

ISO 3664: Viewing Conditions for Graphic Technology & Photography

***Monitors** (refer to NARA Technical Guidelines – pp. 23)*

- The monitor should be set to 24-bits (millions of colors) or greater, and calibrated to a gamma of 1.8 (Mac) or 2.2 (PC).
- Monitor color temperature set to 5000 Kelvin degrees with a desktop background of a neutral gray (avoid images, patterns, and/or strong colors).
- Monitor luminance level must be at least 85 cd/m2 and should be 120 cd/m2 or higher.

- CRT/LCD monitors designed for the graphic arts and multimedia are recommended for a digitization environment.
- Using a target such as the NARA Monitor Adjustment Target or a Kodak Grayscale can be used to adjust the monitor aimpoints of brightness / contrast for calibration *(refer to NARA Technical Guidelines – pp. 24)*

Room

- Ambient room lighting should be kept at or below 5000 Kelvin color temperature and should be dispersed/diffused throughout the room, not directly overhead causing glare problems. *(refer to NARA Technical Guidelines – pp. 23)*
- The room should be relatively dust free by use of a air filter and commitment to keeping all scanning systems free of dust and other particles.

Quantifying Scanner/Digital Camera Performance

Digitization Standards

Tests should be performed on all image capture equipment prior to purchase and throughout the life cycle of the equipment to ensure quality standards and verification of optimal performance. The following standards should be looked at as benchmarking tools to assess all equipment by either requesting test results from the vendor/manufacturer of imaging equipment or performing an evaluation with the use of a test target for performance metrics. These standards can be purchased from ISO at http://www.iso.ch or from IHS Global at http://global.ihs.com or other affiliated standards organizations such as ANSI at http://www.ansi.org/ or AIIM at http://www.aiim.org.

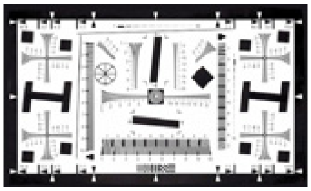
Subject	Document Number
Terminology	
Photography -- Electronic still-picture imaging – Terminology	ISO/FDIS 12231.2. July 2004 or 2005
Data Dictionary - Technical Metadata for Digital Still Images (Draft standard for trial use.)	NISO Z39.87-2002 AIIM 20-2002
Opto-Electronic Conversion Function	
Photography -- Electronic still-picture cameras -- Methods for measuring opto- electronic conversion functions (OECFs)	ISO 14524:1999
Resolution	
Photography -- Electronic still-picture cameras – Resolution measurements.	ISO 12233:2000
Photography -- Electronic scanners for photographic images -- Spatial resolution measurements -- Part 1: Scanners for reflective media	ISO 16067-1:2003
Photography -- Electronic scanners for photographic images -- Spatial resolution measurements -- Part 2: Film scanners	ISO16067-2 Sept. 2004
Photographic & Electronic Imaging (Resolution definition and application for evaluation of photographic and electronic systems.)	ANSI/AIIM TR26-1993
Noise	
Photography -- Electronic still picture imaging – Noise measurements	ISO 15739:2003
Dynamic Range	
Photography -- Electronic scanners for photographic images -- Dynamic range measurements	ISO 21550 Sept. 2004
Viewing Conditions	

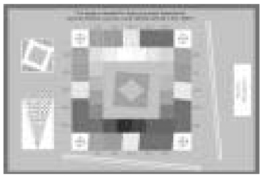
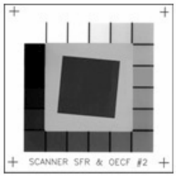
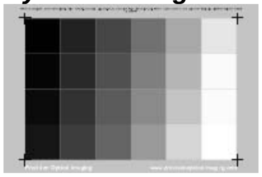
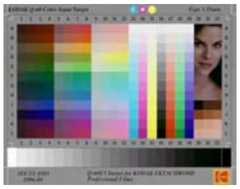
Viewing Conditions—Graphic technology and photography	ISO 3664:2000
Viewing Conditions—Graphic Technology – Displays for color proofing	ISO 12646
Color	
Photography and graphic technology – Extended color encodings for digital image storage, manipulation and interchange – Part 1: Architecture and requirements	ISO 22028-1:2004
Graphic technology -- Prepress digital data exchange -- Colour targets for input scanner calibration	ISO 12641:1997
Quality Control	
Recommended Practice for Quality Control of Image Scanners. Provides procedures for ongoing quality control of image scanners, including incorporation of targets.	ANSI/AIIM MS44-1988 (R1993)
Sampling Procedures and Tables for Inspection by Attributes. Includes tightened, normal and reduced plans. (American Society for Quality)	ANSI/ASQ Z1.4-2003
Sampling Procedures and Tables for Inspection by Variables for Percent Nonconforming (American Society for Quality)	ANSI/ASQ Z1.9-2003
Sampling Procedures for Inspection by Attributes of Images in Electronic Image Management (EIM) & Micrographics Systems. Provides guidance in selecting a sampling procedure	ANSI/AIIM TR34-1996

Test Targets

Before the purchasing of new digitization equipment and after the purchase, an initial performance capability evaluation should be conducted with each digitization device. This may involve using test targets to make benchmark assessments in image quality to predict the integrity of such devices and how effective they will be. Tests are also performed to optimize the performance of an image capture device based on operational settings. These test results should be cumulated into a database to track the performance and/or any variability.

Targets used for Benchmark Testing Digital Image Capture Devices

Digital Reproduction Elements	**Purpose**
ISO 12233:2000 ***ISO Resolution Chart for Electronic Still Cameras*** 	Targets: ISO 12233 Resolution Chart *(1X- 35.6cm x 20cm- Chrome on Photopaper)* Link to Purchase Designed to check resolution and spatial frequency response of electronic still imaging cameras, this chart comes in a variety of sizes and has testing software available upon request.

ISO 16067-1: 2003 **ISO 16067-2: Sept. 2004** **ISO 14524:1999** ***ISO Scanner Test Chart for Reflective/Transmissive Scanners***  **Slant Edge Target** 	Targets: QA-61 Link to Purchase Determines reflective light resolution and imaging characteristics of digital scanning systems. Targets: QA-62 Link to Purchase Designed for evaluation of the slant edge target and used for MTF analysis of the digital scanning system's spatial frequency response (true resolution).
Grayscale (Q-13) KODAK Gray Scale C Y M Kodak KODAK Color Control Patches Kodak	Target: Q-13 (small) (*comes with Kodak Color Control Patches)* Link to Purchase This target can be used to verify if the tonal curves are within a defined range of densities for highlight, midpoint, and shadow. The additional color patches can be used to monitor the calibration (ΔE) of the imaging capture device and it applies to both monochrome and color electronic still picture cameras and digital scanners.
ISO 21550 ***Dynamic Range Chart*** 	Target: Link to Purchase This International Standard defines methods for measuring the ability of scanning devices to capture tones focusing on the dark areas of the source image. This standard uses digital analysis techniques for measuring Dynamic Range for film and reflective media.
ISO 12641:1997 ***Color Reproduction Target for Calibration*** 	Target: ANSI IT8.7/1-1993 (Kodak Q-60E3) Link to Purchase Transmissive Target for scanner calibration Target: ANSI IT8.7/2-1993 (Kodak Q-60R1)

	Link to Purchase Reflection Target for scanner calibration

2.2.1.3. Inspection

In the prototype environment, all scanned images are manually inspected.

Document Inspection prior to scanning

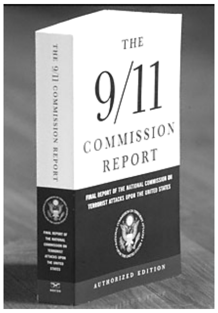
- Determine that all pages are in each publication.
- Determine if there is any damage to publications:
- Torn pages
- Damaged spine
- Stains
- Smudges
- Wrinkles

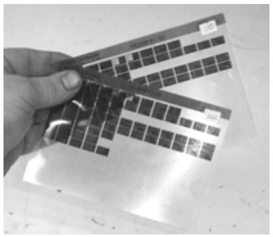
3.0 Current operational situation

Eight workstations are dedicated to inspection. Inspection is a manual examination of the page as compared to the image.

3.1. Document Characterization

Categories of Material	Handling	Types of Scanners

Type A*:* **Rare, valuable, & brittle** 	1.0 Must be specially handled with white, static-free gloves and treated with care. 2.0 Pages turned carefully and book must not be mishandled or dropped. 3.0 All areas kept free of extraneous paper dust and dirt through careful measures such as, compressed air or by lightly dusting over the imageable surface. 4.0 Some documents may require a translucent protective sleeve prior to digitization.	5.0 Overhead Scanner/Digital Camera – Manual-Page Turning **ONLY** 6.0 Flatbed Scanner
Type B: ***Pamphlets, unbound*** 	7.0 Can be separated and run through an automated feed process. 8.0 Can be unfolded and placed flat on an imageable surface. 9.0 Some may require removal of binding materials (*ie. staples, stitches, spiral, comb-binding, tape, etc*.)	10.0 Auto-document Feed scanner 11.0 Flatbed Scanner
***Type C*: Bound** 	12.0 Publications scanned while intact and in its original bound form. 13.0 Can be opened and placed flat on an imageable surface.	14.0 Overhead Scanner/Digital Camera – Auto/Manual-Page Turning

Type D: ***Fold-outs, maps, posters*** 	15.0 Can be separated and run through an automated feed process. 16.0 Can be unfolded and placed flat on an imageable surface. 17.0 Some are larger formats and may require a larger scanner/camera imaging device to capture the whole area.	18.0 Flatbed Scanner 19.0 Wide Format Cameras/Scanners
Type E: ***Microform*** 	20.0 Many different formats/sizes that may require specific equipment or handling, therefore more than one type of scanner may be necessary.	21.0 Film scanner (*various types*) 22.0 Flatbed Scanner

3.2. *Image Capture Classification*

Determine the type of image capture mode performed on each page

- **RGB** (Color halftones, solid images, photographs, charts, or any type of continuous-tone image)
- **Grayscale** (Non-color halftones, solid images, photographs, charts, or any other type of continuous-tone image)
- **Bitonal** (Black and white only – text matter or line-art matter)

3.3. *Content Management*

3.3.1. Image Workflow

Currently DCS utilizes a manual process for file workflow tracking and management.

The product set selected by DCS will support document/data capture and production/ad-hoc scanning in a single application. The application will also have a strong Application Programming Interface (API) to expand functionality when needed within the functionality of the Content OriginatorTS product selected. Most structured and unstructured documents can be scanned in batches, and the system should have the capability to automatically recognize each document in a batch and process them based on characteristics that have been predefined. The product's workflow should be integrated and manage documents allowing a high level of control over how the diverse types of documents that GPO will manage are processed. The product must provide the capability to define and modify workflows.

The selected product set should combine both document and data capture and allow remote Internet-based capture for future use. Capture stations should be designed with simplistic configuration procedures in place. Capture stations should be located at GPO's HQ site and at possible remote sites—across geographic regions or in the same building—and should be able to synchronize with a central capture site via the Internet. It is important that the product selected have an open architecture that makes it easy to extend the basic application to handle complex, high-volume document processing. The product should also be able to predefine "batch definitions or classes" to allow all classes and types of documents to be captured.

3.4. Storage

Storage of scanned images is on a network server, with standard IT back-up processing in place.

4.0 Desired Situation

4.1. Background Changes

Create a scanning environment that incorporates automated workflow software, with combinations of scanning equipment and efficient user interfaces to support each area within the workflow.

4.1.1. Specific Component

A Scanning module should be available to create batches, scan and import documents, and edit the contents of batches. A batch is a set of data or jobs to be processed in a single program run or a quantity required for or produced as the result of one operation. In most cases within a digitization environment, a single batch will be an entire publication or group of publications from a single customer/source. After the batches are created, they should be able to be entered into temporary storage in the system, making them available for processing by subsequent modules.

- **Batch creation:** The operator creates the batch by selecting the type of batch to create (the batch class) and then scanning or importing documents and pages. The document images are stored in a temporary folder for further processing by the system.
- **Batch editing:** Once the batch is created, the operator can visually check documents or pages, and edit them as necessary. Editing functions include replacing, reordering, or rejecting documents and pages. Entire documents or individual pages can be rotated and saved in the rotated state.

4.1.1.1. Objectives

To design a system that constructs as many "mini" conversion pipelines that can stand on their own should a failure occur. Each of these mini pipelines or "clusters" contain workflow, scanning, recognition, key-from image, key from paper, QA, storage functionality and the people to staff its stations. All of the clusters are then managed by a site-level workflow manager which normally manages workflow for all of the clusters, provides administrative functions and communicates with sites and services outside of the confines of the current site.

The system will be broken down into as many "independent clusters" as required to help guarantee reliability. Workflow and administrative functions at the site level will also be organized in a way to make sure that backups and administrative tasks are built to make a cluster as independent as possible.

4.1.1.2. Metrics

Metrics of workflow will follow previously mentioned ANSI and ISO standards.

4.1.1.3. Priorities among changes

1) Workflow Software
2) Batch Processing for Digitization of Documents
3) Quality Control Process
4) Process for Metadata Capture

5.0 Benchmarks

Image Capture Benchmarks for Preservation Masters *(refer to NARA Technical Guidelines – pp. 32-36)*

Scanner Setup (refer to DLF – pp. 3, NARA-pp.52)

Image Types	Bit Depth	Color Mode	Resolution (ppi/spi)	Scale	File Format	Compression
Reflective						
B&W Text Only	1-bit	B&W (bitonal)	600 ppi/spi	100% (1:1)	TIFF	CCITT Group 4
B& W Text with Illustrations (charts, artwork, graphs, photos)	8-bit	Grayscale	400 ppi/spi *		TIFF	None
Color Photos & Illustrations with Text	24-bit	RGB	400 ppi/spi *		TIFF	None
Transmissive						
16mm	36-48 / 16 bit	Color / Grayscale	5000 ppi/spi	1600 % (16:1)	TIFF	None
35mm	36-48 / 16 bit	Color / Grayscale	3400 ppi/spi	850% (8.5:1)		
2-1/4"	36-48 / 16 bit	Color / Grayscale	1800 ppi/spi	450% (4.5:1)		
4" x 5"	24-48 / 8-16 bit	Color / Grayscale	800 ppi/spi	200% (2:1)		
8" x 10" +	24-48 / 8-16 bit	Color / Grayscale	400 ppi/spi	100% (1:1)		

* Scanning resolutions for images over 11 x 16" (300 ppi for 8-bit grayscale and 300 ppi for 24-bit RGB color)

1. Originals will be backed with bright white opaque paper for flatbed scanning.
2. **Scan Kodak Grayscale Target (Q-13 or Q-14)**, or an equivalent 14-step or 20-step grayscale, only on publications required to preserve color/grayscale data and to further evaluate of the tonal/dynamic range of the scanning device output.

3. **Choose best defined presets to digitally capture type of publication** – **Based on all these factors**:
   a) *Color Mode* – to best define the color of the original publication format.

   b) *Scaling* – to best define the digital capturing parameters according to *III.A Scanner Setup specifications.*

   c) *Size/Crop* – assuring that an area of at least 1/4" outside of the parameters of the open page(s) is captured.

   d) *Resolution* – using the correct amount of this is dependant on the type of media as well as the content itself according to *III.A Scanner Setup* specifications. (ie. *transmissive vs. reflective, color vs. grayscale vs. bitonal*)

   e) *Descreen* – to remove any printed halftones that cause the obtrusive moiré patterns when digitally capturing from printed material such as newsprint or magazine-type paper.

   f) *Paper/Print Mode* – to determine the optimal settings for the scanner/camera to capture the best rendering of the original (*ie. Some scanner API's have substrate mode [magazine/coated, newsprint, uncoated, photograph] to choose from for the purposes of descreening or other capture features*)

   g) For significant embossed seals / images, the flatbed scanner must be set use One Directional Light

   h) *Tonal Adjustments* – scanner hardware and software must be equipped and capable of capturing correct highlights/shadows without losing detail. Also, the software should use tools with more controls (Levels and curves) along with numeric feedback.

   i) *Color management* could be involved in any settings using proper calibration software for both monitors and image capture devices (Cameras and scanners).

NOTE: Presets will be programmed for each scanner based on these definitions.

Curvature Reduction

If available in the API (Application Programming Interface) of the scanning software, applying an in-process setup to reduce the curvature or rotation of pages during the scanning phase may be necessary.

Aimpoints for Grayscale Target (Tone Compression)

On the preservation master file, the original scan contains a grayscale target. Tone compression is a technique to make the digital reproduction to look like the original in terms of the exact tonal range.

NOTE: This theory should not be applied in all cases, due to each publication's variation in quality attributes due to aging, or the process used in the creation of the publication.

Scanning Aimpoints for Grayscale Target (Q-13) using 24-bit Color Mode

		Neutralized White Point	Neutralized MidPoint	Neutralized BlackPoint
Step or Density	Kodak Q-13/14	A	M	B
	Visual Density	0.05 – 0.10	0.75 – 0.85	1.65 – 1.75
Aimpoint	RGB Level	242-242-242	122-122-122	40-40-40
	% Black	4%	60%	90%
Acceptable Range	RGB Level	236 – 248	116-128	34-46
	% Black	2 – 6%	58 – 62%	88 – 92%

Aimpoint Variability

For the three aimpoint values described above, none should exceed a variability of ± 6 RGB increments per each individual channel: Red, Green, and Blue. You can verify this by using an image sampler in the scanner software tools or an eyedropper tool from image processing software (such as Adobe Photoshop or equivalent) and set to measure an average of either 3 x 3 or 5 x 5 pixels to sample on the grayscale.

Note: never use a point sample or single pixel sample to base your measurement on.

Verification and Save

Results of the scan - All converted images must be inspected to ensure the highest quality possible. Images shall not contain dust representation, digital artifacts, scratches, poor color contrast, poor saturation, incorrect cropping, noise, duplicates, missing images, or any unknown discrepancies not visible on the original tangible piece. Conversion equipment must be configured and maintained to meet the requirements for digitization. This includes but is not limited to profiles, calibration, and cleanliness. All quality discrepancies must be corrected prior to release.

Minimum (submission) level Metadata - Each publication scanned and digitized, must have a minimal level of metadata associated with each TIFF file for preservation purposes. The data elements will consist of bibliographic, technical, and administrative information necessary to track, manage, and preserve the associated files with each title for the future content management system. The TIFF data elements and values (e.g. presented in XML as fields with values associated with file header tags), represent metadata used to render and manage image data.

GPO submission level metadata will capture:

(1) Identity
  (a) Title or caption
  (b) Unique Identifier (persistent locators, filenames, ISNs, etc)

(2) Responsibility
  (a) Author / Creator
  (b) Publisher / Authority

(c) Rights Owner *

(3) Version / Fixity*
    (a) Version information
    (b) Relationship to other version or manifestations

(4) Representation / Technical / Structure*
    (a) Must incorporate NISO Z 39.87-2002 technical metadata for digital still images
    (b) Structure Information

*If readily available

File Naming Convention –The system identifier requires machine or human indexing for corresponding files that relate to each document. Through a standard naming convention, the process of ingest, storage, search, and retrieval of documents is simplified. Files derived from conversion processes shall be assigned a unique 9 digit alphanumeric identifier conforming to the Code 39 barcoding standard (ANSI: BC1-1995). The first digit is the fixed letter "a" which enables validation for a METS schema later assigned. Digits will include 0-9 and letters A-Z (minus i and o). Scanned Publications at the page level shall be assigned the publication unique ID followed by an underscore and a sequential 5 digit identifier.

Example: A12345678_00001

Submission Information Package (SIP) – The images may be in RGB, Grayscale, or Bitonal mode and should have a unique identifier and metadata associated with each file. The quality of the files derived from conversion shall conform to the FDsys Operational Specification for Converted Content.

6.0 Constraints

- Not incorporating automated workflow software will constrain throughput.
- Not upgrading scanning equipment capability will constrain document scanning options.
- Not automating Quality Control process will increase personnel required, and constrain throughput.

Appendix C - List of Requirements

Identification	Requirement	Release/ Criticality
3.2.1.2	**Requirements for System, General**	
1.2.1	The system shall provide for the use of internal and external open interfaces.	Release 1A; Must
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 1A; Must
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 1A; Must
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 1A; Must
1.2.4	The system shall accommodate changes in hardware, software, communication technology, processes, policy, personnel, locations, etc. without requiring major re-engineering or design changes.	Release 1A; Must
1.2.5	The system shall be capable of accommodating growth and managing differing sizes of repositories and ever increasing volumes of content.	Release 1A; Must
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 1A; Must
1.2.7	The system shall provide support for content management lifecycle processes for all types of content.	Release 1A; Must
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 1A; Must
1.2.9	The system shall have the ability to transform content and metadata into packages that are compliant with open standards, including but not limited to XML.	Release 1A; Must
1.2.10	The system shall be available for use at all GPO locations.	Release 1A; Must
1.2.11	The system shall have the capability to support 20,000 concurrent users.	Release 1A; Must
1.2.12	The system shall have the capability to support an overall sustained weekly average uptime greater than or equal to 99.0%.	Release 1A; Must
1.2.12.1	The system shall have the capability to support a sustained weekly average uptime for peak periods greater than or equal to 99.7%. Peak time periods include all times with the exception of midnight to 6 am Eastern Time on Saturday and midnight to 6 am on Sunday.	Release 1A; Must
1.2.12.2	The system shall have the capability to support uptime for off-peak time periods greater than or equal to 90%. Off-peak times may be changed as needed to provide Congress the appropriate level of service.	Release 1A; Must
1.2.13	The system shall have the capability to have a response time to deliver digital services on a sustained weekly average of less than 2 Seconds.	Release 1A; Must

3.2.2.2	**Requirements for Content Metadata**	
2.2.1	**Content Metadata Core Capabilities**	
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 1A; Must

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 1A; Must
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 1A; Must
2.2.1.4	The system shall employ interoperable programming interfaces which are compliant with open standards, including, but not limited to, Extensible Markup Language (XML).	Release 1A; Must
2.2.1.5	The system must provide the capability to link content metadata with system metadata.	Release 1A; Must
2.2.1.6	The system must provide the capability to link content metadata with business process information.	Release 1A; Must

2.2.2	**Content Metadata Types**	
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 1A; Must
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 1A; Must
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 1A; Must
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 1A; Must
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 1A; Must
2.2.2.3.2.1	Publication-specific metadata (e.g., Federal Register, Code of Federal Regulations, United States Code, U.S. Reports)	Release 1A; Must
2.2.2.3.2.2	Document-specific metadata (e.g., Congressional Bills, Congressional Reports, Congressional Documents, proposed rules, business cards, envelopes, agency strategic plans)	Release 1A; Must
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 1A; Must
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 1A; Must
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 1A; Must
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 1A; Must
2.2.2.5	The system shall employ metadata which relates the context of a digital object and relationship to other objects.	Release 1A; Must
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 1A; Must
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 1A; Must

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 1A; Must

2.2.3	**Content Metadata Schema**	
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 1A; Must
2.2.3.2	In general, GPO shall refer to metadata schema rather than embed data elements in the METS wrapper.	Release 1A; Must
2.2.3.3	Deleted in RD v2.1	
2.2.3.4	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including but not limited to:	multiple releases
2.2.3.4.1	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including but not limited to:Machine Readable Cataloging (MARC)	Release 1A; Must
2.2.3.4.2	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including Metadata Object Description Schema (MODS)	Release 1A; Must
2.2.3.4.3	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including Dublin Core	Release 1A; Must
2.2.3.4.4	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including Encoded Archival Description (EAD)	Release 1C; Could
2.2.3.4.5	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including Text Encoding Initiative (TEI)	Release 1A; Could
2.2.3.4.6	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including Data Document Initiative (DDI)	Release 1C; Could
2.2.3.4.7	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including Federal Geographic Data Committee (FGDC)	Release 1C; Could
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 1A; Must
2.2.3.4.9	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including MPEG 21	Release 1B; Should
2.2.3.4.10	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including JPEG 2000	Release 1B; Should
2.2.3.4.11	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including ONIX	Release 1B; Must
2.2.3.4.12	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible, including but not limited to:MIX (NISO Metadata for Images)	Release 1A; Must
2.2.3.5	The system shall employ a registry of extension schema and input standards in use.	Release 1A; Must

2.2.3.6	Authorized users shall have the capability to manage the registry of schema employed by the system.	Release 1A; Must
2.2.3.7	The system shall have the capability to employ new schema and add them to the registry.	Release 1A; Must
2.2.3.8	The system shall use the following criteria to determine what schema shall be included in the registry.	Release 1A; Must
2.2.3.8.1	The schema must interact with METS.	Release 1A; Must
2.2.3.8.2	The schema must map to specific function(s), content type, or content formats within the system.	Release 1A; Must
2.2.3.8.3	The schema must be a recognized standard managed by a trusted and recognized authority (e.g., Library of Congress, W3C).	Release 1A; Must
2.2.3.8.4	The schema must not conflict with other schema in use by the system.	Release 1A; Must
2.2.3.9	The system shall be capable of using extension schema developed by GPO.	Release 1B; Must
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 1A; Must

2.2.4	**Content Metadata Import and Export**	
2.2.4.1	The system shall have the capability to acquire existing metadata from sources external to the system.	Release 1A; Must
2.2.4.2	The system shall have the ability to export metadata with or without associated content, including but not limited to:	Release 1B; Must
2.2.4.2.1	The ability to export metadata one record at a time.	Release 1B; Must
2.2.4.2.2	The ability to export metadata in batches.	Release 1B; Must
2.2.4.3	The system shall have the ability to export metadata compliant with multiple standards including but not limited to:	Release 1B; Must

2.2.5	**Content Metadata Management**	
2.2.5.1	The system shall have the ability to manage metadata regardless of its source.	Release 1A; Must
2.2.5.2	The system shall have the ability to create metadata meeting the requirements of multiple schema.	Release 1A; Must
2.2.5.3	The system shall provide the capability for GPO to designate metadata elements as mandatory.	Release 1A; Must
2.2.5.4	The system must provide the capability for content metadata and system metadata to interact (e.g., a time and date stamp of a content authentication process).	Release 1A; Must
2.2.5.5	The system must provide the capability for content metadata and Business Process Information to interact.	Release 1A; Must
2.2.5.6	The system shall log all additions, deletions, and changes to content metadata within the system.	Release 1A; Must

3.2.3.1.2	**Requirements for SIP**	
3.1.2.1	**SIP - Deposited Content**	
3.1.2.1.1	The SIP Deposited Object shall consist of digital object(s) associated with a document or publication, including at least one of the following categories of files:	Release 1A; Must
3.1.2.1.2	The metadata for deposited content in the SIP shall consist of fundamental representation information, any necessary DTD's (or schema), style sheets, and submission level metadata.	Release 1A; Must

3.1.2.2	**SIP - Harvested Content**	
3.1.2.2.1	The SIP Harvested Object shall consist of digital object(s) as harvested, including at least one of the following categories of files:	Release 1A; Must
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.	Release 1A; Must

3.1.2.3	**SIP - Converted Content**	
3.1.2.3.1	The SIP Converted Object shall consist of digital object(s) as obtained by scanning or other method, including at least one of the following categories of files:	Release 1A; Must
3.1.2.3.2	The metadata for converted content in the SIP shall refer to full technical information on the conversion, using NISO Z 39.87-2002 as a guideline, in addition to submission level metadata.	Release 1A; Must

3.1.2.4	**Core SIP Requirements**	
3.1.2.4.1	A SIP shall contain one content unit (e.g., publication) that may consist of one or more digital objects.	Release 1A; Must
3.1.2.4.2	A SIP shall contain a binding METS file, named sip.xml, which describes the SIP as a whole and the relationships between digital objects and metadata.	Release 1A; Must
3.1.2.4.3	A SIP shall contain one or more metadata files associated with the content.	Release 1A; Must
3.1.2.4.4	All metadata files shall be encoded in XML and conform to schema that are adopted by FDsys, according to the FDsys metadata requirements.	Release 1A; Must
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 1A; Must

3.1.2.5	**Requirements for sip.xml File**	
3.1.2.5.1	The sip.xml file shall conform to the most current version of the METS schema.	Release 1A; Must
3.1.2.5.2	The sip.xml shall conform to the most current GPO profile for METS schema.	Release 1A; Must
3.1.2.5.3	In general, digital objects shall be referred to, but not directly embedded in, the sip.xml file.	Release 1A; Must
3.1.2.5.4	In general, metadata files shall be referred to, but not directly embedded in, the sip.xml file.	Release 1A; Must
3.1.2.5.5	A metadata file must be associated with one or more digital objects in the sip.xml file.	Release 1A; Must

3.1.2.6	**Structural Layout for SIPs**	
3.1.2.6.1	The SIP shall contain the sip.xml file and two directories at the top level of the structure layout. The two top directories should be named as content and metadata.	Release 1A; Must
3.1.2.6.2	All digital objects for the content of a SIP shall be placed in the content directory.	Release 1A; Must
3.1.2.6.2.1	The content directory shall contain one or more sub-directories that will reflect the category of content included in the SIP.	Release 1A; Must
3.1.2.6.3	All metadata files shall be placed in the metadata directory.	Release 1A; Must
3.1.2.6.3.1	The metadata directory shall contain one or more sub-directories that will reflect the metadata included in the SIP.	Release 1A; Must

3.1.2.6.4	Each content category file shall have one corresponding metadata file expressed in the Metadata Object Description Schema (MODS) that includes descriptive metadata about that content.	Release 1A; Must
3.1.2.6.5	Each content category file shall have one or more corresponding metadata files that comply with an extension schema and that include administrative metadata appropriate to the class of object. .	Release 1A; Must

3.1.2.7	Packaging of SIPs	
3.1.2.7.1	All file components of the SIP shall be assembled into a structured file system directory hierarchy and then aggregated into a single file or entity for transmission and ingest into the system.	Release 1A; Must

3.1.2.8	SIP Descriptive Metadata Requirements	
3.1.2.8.1	For descriptive metadata elements, GPO shall employ Metadata Object Description Schema (MODS) records external to the binding METS file (sip.xml).	Release 1A; Must
3.1.2.8.2	All MODS elements and sub-elements shall be considered valid in the SIP.	Release 1A; Must
3.1.2.8.3	The following MODS descriptive metadata elements shall be considered mandatory and shall be present and valid in order for a SIP to be eligible for ingest:	Release 1A; Must

3.1.2.9	SIP Administrative Metadata Requirements	
3.1.2.9.1	The SIP shall include administrative metadata as needed, expressed in extension schema appropriate to the class of object, including but not limited to:	Release 1A; Must

3.2.3.2.2	Requirements for AIP	
3.2.2.1	AIP Core Capabilities	
3.2.2.1.1	AIPs shall be capable of including the digital object(s) in its native format.	Release 1A; Must
3.2.2.1.2	AIPs shall be capable of including the digital object(s) and corresponding XML version(s) including associated DTD, style sheet(s), and schema.	Release 1A; Must
3.2.2.1.3	AIPs shall include the Representation Information for content.	Release 1A; Must
3.2.2.1.4	The system shall support the creation of AIPs which are independent of any particular hardware and software component.	Release 1A; Must
3.2.2.1.5	The system will provide the capability for authorized users to access AIPs for the purpose of executing preservation processes or dissemination of AIPs.	Release 1A; Must
3.2.2.1.6	The AIP shall be expressed using METS.	Release 1A; Must
3.2.2.1.7	The AIP shall contain a binding METS file, named aip.xml, which describes the AIP as a whole and the relationships between digital objects and metadata.	Release 1A; Must
3.2.2.1.8	The AIP shall contain one or more metadata files associated with the content.	Release 1A; Must

3.2.2.2	Requirements for aip.xml File	
3.2.2.2.1	The aip.xml file shall conform to the most current version of the METS schema.	Release 1A; Must
3.2.2.2.2	The aip.xml shall conform to the most current GPO profile for METS schema.	Release 1A; Must
3.2.2.2.3	In general, digital objects shall be referred to, but not directly embedded in, the aip.xml file.	Release 1A; Must

3.2.2.2.4	In general, metadata files shall be referred to, but not directly embedded in, the aip.xml file.	Release 1A; Must
3.2.2.2.5	A metadata file must be associated with one or more digital objects inside the aip.xml file.	Release 1A; Must

3.2.2.3	**Structural Layout for AIPs**	
3.2.2.3.1	The AIP shall contain the aip.xml file and two directories at the top level of the structure layout. The two top directories should be named as content and metadata.	Release 1A; Must
3.2.2.3.2	All digital objects for the content of an AIP shall be placed in the content directory.	Release 1A; Must
3.2.2.3.2.1	The content directory shall contain one or more sub-directories that will reflect the category of content included in the AIP.	Release 1A; Must
3.2.2.3.3	All metadata files shall be placed in the metadata directory.	Release 1A; Must
3.2.2.3.3.1	The metadata directory shall contain one or more sub-directories that will reflect the metadata included in the AIP.	Release 1A; Must
3.2.2.3.4	Each content category file shall have one corresponding metadata file expressed in the Metadata Object Description Schema (MODS) that includes descriptive metadata about that content.	Release 1A; Must
3.2.2.3.5	Each content category file shall have one corresponding metadata file that complies with an extension schema that includes administrative metadata about that content.	Release 1A; Must

3.2.2.4	**AIP Metadata**	
3.2.2.4.1	All metadata files shall be encoded in XML and conform to schema that are adopted by FDsys, according to the FDsys metadata requirements.	Release 1A; Must
3.2.2.4.2	The AIP shall include PDI that identifies the essential attributes of the content that is being preserved so it can be rendered usably and understandably.	Release 1A; Must
3.2.2.4.3	The AIP shall include preservation metadata to record preservation processes, from ingest into the repository through disposal.	Release 1A; Must
3.2.2.4.4	The AIP shall refer to extension schema for descriptive metadata, including, but not limited to, MODS and MARC.	Release 1A; Must
3.2.2.4.4.1	The AIP shall incorporate the mandatory descriptive metadata elements from the SIP.	Release 1A; Must
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 1A; Must
3.2.2.4.6	The AIP shall include administrative metadata as needed, expressed in extension schema appropriate to the class of object, including but not limited to:	Release 1A; Must

3.2.2.5	**AIP Unique ID**	
3.2.2.5.1	The AIP shall include the unique identification number assigned to the content in the SIP.	Release 1A; Must
3.2.2.5.1.1	The system shall have the capability to assign a unique identification number to any new AIP resulting from preservation processes.	Release 1A; Must

3.2.3.3.2	**Requirements for ACP**	
3.3.2.1	**ACP Core Capabilities**	
3.3.2.1.1	The ACP shall have the capability to include digital objects associated with a document or publication, from one or more of the following:	Release 1B; Must
3.3.2.1.2	The ACP shall have the capability to include the following:	Release 1B; Must

3.3.2.1.2.1	Ephemera (e.g., letterhead, envelopes, business cards).	Release 1B; Must
3.3.2.1.2.2	Derivatives not included in the AIP but created from the AIP.	Release 1B; Must
3.3.2.1.2.3	Derivatives created from access copies, native files, or optimized copies.	Release 1B; Must
3.3.2.1.2.4	Derivatives created from derivatives (e.g., thumbnail images).	Release 1B; Must
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 1B; Must
3.3.2.1.4	The ACP shall have the capability to include all digital objects included in its corresponding AIP.	Release 1B; Must
3.3.2.1.5	The ACP metadata shall have the capability to include descriptive, structural, technical, administrative, and packaging metadata for access, content transformation, content management, content processing, derivation, and delivery.	Release 1B; Must
3.3.2.1.6	The ACP shall have a structural layout that facilitates access and delivery.	Release 1B; Must
3.3.2.1.7	The ACP shall have the capability to replicate the structural layout of an AIP.	Release 1B; Could
3.3.2.1.8	The system shall have the capability to package ACPs in such a way to facilitate access and delivery.	Release 1B; Must
3.3.2.1.9	The ACP shall have the capability to refer to or embed one or more metadata files associated with the content.	Release 1B; Must
3.3.2.1.10	The ACP shall have the capability to refer to or embed one or more digital objects associated with metadata.	Release 1B; Must
3.3.2.1.11	The ACP shall have the capability to include all metadata files included in its corresponding AIP.	Release 1B; Must

3.3.2.2	**ACP Binding Metadata File**	
3.3.2.2.1	If required by the system, the ACP shall have the capability to employ a binding metadata file which describes the ACP as a whole and the relationships between digital objects and content metadata to support access and delivery.	Release 1B; Could
3.3.2.2.1.1	If required by the system, the binding metadata file shall conform at a minimum to the most current version of the METS schema to support access and delivery.	Release 1B; Could
3.3.2.2.1.2	The system must provide the capability to embed or refer to digital objects (e.g., XML, OCR-ed text) as required to support access and delivery.	Release 1B; Could
3.3.2.2.1.3	The system must provide the capability to embed or refer to metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support access and delivery.	Release 1B; Could
3.3.2.2.1.4	The system must provide the capability to associate metadata files with one or more digital objects in the ACP.	Release 1B; Could

3.3.2.3	**ACP Metadata**	
3.3.2.3.1	The system shall have the capability to encode metadata files in XML and conform to schema adopted by FDsys, according to FDsys Content Metadata requirements.	Release 1B; Must
3.3.2.3.2	The ACP shall have the capability to embed or refer to metadata for access and delivery.	Release 1B; Must
3.3.2.3.3	The system must provide the capability to add structural and descriptive metadata for digital objects at a level of granularity that facilitates access to content at speeds that are at or above current industry standards for search and retrieval.	Release 1B; Must

3.3.2.3.4	The system must provide the capability to add structural and descriptive content metadata for digital objects at the specified level of granularity.	Release 1B; Must
3.3.2.3.5	The ACP shall have the capability to use extension schema for descriptive metadata for access, including, but not limited to the following:	Release 1B; Must
3.3.2.3.6	The ACP shall have the capability to include mandatory descriptive metadata elements from the AIP and SIP.	Release 1B; Must
3.3.2.3.7	The ACP shall have the capability to embed or refer to extension schema for additional structural metadata as appropriate to the class of object and as necessary for access and delivery.	Release 1B; Must
3.3.2.3.8	The ACP shall have the capability to embed or refer to extension schema for administrative metadata as appropriate to the class of object and as necessary for access and delivery, including but not limited to the following:	Release 1B; Must
3.3.2.3.9	The ACP shall have the capability to embed or refer to extension schema for other metadata as appropriate to the class of object and as necessary for access and delivery, including but not limited to the following:	Release 1B; Must
3.3.2.3.10	The ACP must have the capability to include the unique ID assigned to the SIP and AIP in metadata.	Release 1B; Must

3.2.3.4.2	**Requirements for DIP**	
3.4.2.1	**DIP Core Capabilities**	
3.4.2.1.1	The DIP shall have the capability to include digital objects, associated content metadata, and business process information to fulfill End User requests and Content Originator orders.	Release 1B; Must
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
3.4.2.1.3	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
3.4.2.1.4	The DIP shall have the capability to refer to or embed one or more metadata files associated with the content.	Release 1B; Must
3.4.2.1.5	The DIP shall have the capability to refer to or embed one or more digital objects associated with metadata.	Release 1B; Must
3.4.2.1.6	The system must provide the capability to delivery DIPs that only include content metadata.	Release 1B; Must
3.4.2.1.7	The DIP shall have the capability to be an exact replica of the AIP.	Release 1B; Must
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
3.4.2.1.9	The DIP shall have a structural layout that facilitates delivery.	Release 1B; Must
3.4.2.1.10	The system shall have the capability to package DIPs in such a way to facilitate delivery.	Release 1B; Must

3.4.2.2	**DIP Binding Metadata File**	
3.4.2.2.1	If required by the system, the DIP shall have the capability to employ a binding metadata file which describes the DIP as a whole and the relationships between digital objects and content metadata to support delivery.	Release 1B; Could
3.4.2.2.1.1	If required by the system, the binding metadata file shall conform at a minimum to the most current version of the METS schema to support delivery.	Release 1B; Could

3.4.2.2.1.2	The system must provide the capability to embed or refer to digital objects (e.g., XML, OCR-ed text) as required to support delivery.	Release 1B; Could
3.4.2.2.1.3	The system must provide the capability to embed or refer to metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support delivery.	Release 1B; Could
3.4.2.2.1.4	The system must provide the capability to associate content metadata files with one or more digital objects in the DIP.	Release 1B; Could

3.4.2.3	**DIP Metadata**	
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
3.4.2.3.2	The DIP shall have the capability to embed or reference metadata for delivery.	Release 1B; Must
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
3.4.2.3.4	The DIP shall have the capability to use extension schema for descriptive metadata for delivery, including, but not limited to the following:	Release 1B; Must
3.4.2.3.5	The DIP shall have the capability to embed or refer to extension schema for additional structural metadata as appropriate to the class of object and as required for delivery.	Release 1B; Must
3.4.2.3.6	The DIP shall have the capability to embed or refer to extension schema for administrative metadata as appropriate to the class of object and as required for delivery, including but not limited to the following:	Release 1B; Must
3.4.2.3.7	The DIP shall have the capability to embed or refer to extension schema for other metadata as appropriate to the class of object and as required for delivery, including but not limited to the following:	Release 1B; Must
3.4.2.3.8	The system must provide the capability to include information generated as a result of Content Originator ordering.	Release 1C; Must
3.4.2.3.9	The system must provide the capability to include information generated as a result of an End User request.	Release 1B; Must
3.4.2.3.10	The DIP must have the capability to include the unique ID assigned to the SIP, ACP, and AIP in metadata.	Release 1B; Must
3.4.2.3.11	The system shall have the capability to support the Open Archives Initiative Protocol.	Release 1B; Must

3.2.4.1.1	**Requirements for Pre-ingest Processes**	
4.1.1.1	**Pre-ingest Processing**	
4.1.1.1.1	The system shall accept content from Content Originators.	Release 1A; Must
4.1.1.1.2	The system shall accept jobs from Content Originator ordering.	Release 1C; Must
4.1.1.1.3	The system shall accept deposited content without style tools.	Release 1A; Must
4.1.1.1.4	The system shall accept deposited content from style tools.	Release 1C; Could / Release 2; Must
4.1.1.1.5	The system shall accept converted content.	Release 1A; Must
4.1.1.1.6	The system shall accept harvested content.	Release 1A; Must
4.1.1.1.7	The system shall have the capability to apply version control.	Release 1A; Must
4.1.1.1.8	The system shall detect duplicate content in the system and notify authorized users.	Release 1A; Must
4.1.1.1.8.1	The system shall determine if the version of content is already in the system, using, at a minimum:	Release 1A; Must
4.1.1.1.8.2	The system shall have the capability to reject duplicate content.	Release 1A; Must

4.1.1.1.9	The system shall have the capability to store content in WIP before job order information is received.	Release 1A; Must
4.1.1.1.10	The system shall have the capability to assign a unique ID to content.	Release 1A; Must
4.1.1.1.11	The system shall have the capability to assign a unique ID to jobs.	Release 1A; Must
4.1.1.1.12	The system shall populate the Identifier field in the corresponding MODS record with the content unique ID.	Release 1A; Must
4.1.1.1.13	The system shall link related jobs, business process information (BPI), and content through the content unique ID.	Release 1A; Must
4.1.1.1.14	The system shall allow Content Evaluators to make scope determinations.	Release 1A; Must
4.1.1.1.15	The system shall have the capability to perform integrity checking.	Release 1A; Must
4.1.1.1.16	The system shall have the capability to apply a digital time stamp to content.	Release 1A; Must
4.1.1.1.17	The system shall have the capability to perform accessibility assessments.	Release 1A; Must
4.1.1.1.18	The system shall have the capability to support the creation of a pre-ingest bundle (PIB).	Release 1C; Must
4.1.1.1.19	The system shall have the capability to accept modified DIPs from the Service Provider after publisher approval.	Release 1B; Must
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
4.1.1.1.21	The system shall accept publisher approval information for SIP creation.	Release 1A; Must
4.1.1.1.22	The system shall have the capability to assemble content into SIPs.	Release 1A; Must
4.1.1.1.23	The system shall have the capability to create a log of all transactions and activities.	Release 1A; Must

3.2.4.2.1	**Requirements for Ingest Processing**	
4.2.1.1	**Ingest Processing Core Capabilities**	
4.2.1.1.1	Ingest processing performs the following functions:	multiple releases
4.2.1.1.1.1	Accept and validate SIPs	Release 1A; Must
4.2.1.1.1.2	Create AIPs from SIPs	Release 1A; Must
4.2.1.1.1.3	Create ACPs from SIPs	Release 1B; Must
4.2.1.1.1.4	Apply digital time stamping to content	Release 1A; Must

4.2.1.2	**Ingest Processing**	
4.2.1.2.1	The system shall allow Content Originators and Service Specialists to submit content to ingest once content has been approved for release by the publisher.	Release 1A; Must
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 1A; Should
4.2.1.2.2	The system shall validate that SIPs conform to the requirements for a system compliant SIP, including but not limited to:	Release 1A; Must
4.2.1.2.2.1	The system shall verify that the SIP includes all mandatory metadata elements.	Release 1A; Must
4.2.1.2.2.2	The system shall verify that the METS file is valid.	Release 1A; Must
4.2.1.2.2.3	The system shall verify that at least one digital object is present.	Release 1A; Must
4.2.1.2.2.4	The system shall verify that all digital objects are operational with its intended supporting application.	Release 1A; Must
4.2.1.2.3	The system shall provide the capability to reject non-conforming SIPs.	Release 1A; Must
4.2.1.2.3.1	The system shall direct exceptions to Service Specialists.	Release 1A; Must
4.2.1.2.4	The system shall provide the capability to notify users that a SIP is nonconforming.	Release 1A; Must

4.2.1.2.5	The system shall provide the capability to notify users of the reasons a SIP is nonconforming.	Release 1A; Must
4.2.1.2.6	The system shall allow the use of automatic file format verification against a format registry (e.g., the DROID software to check the PRONOM technical registry).	Release 1A; Must
4.2.1.2.7	The system shall have the capability to verify content integrity (e.g., checksum).	Release 1A; Must
4.2.1.2.8	The system shall pass the AIP to archival information storage after creation.	Release 1A; Must
4.2.1.2.9	The system shall pass the ACP to access content storage after creation.	Release 1B; Must
4.2.1.2.10	The system shall have the capability to create a log of all transactions and activities.	Release 1A; Must

3.2.4.3.2	Requirements for Preservation Processing	
4.3.2.1	**Preservation Processing Core Capabilities**	
4.3.2.1.1	The system shall have the ability to store AIPs in a preservation repository environment.	Release 1A; Must
4.3.2.1.1.1	AIPs must remain free from corruption and remain accessible as GPO undergoes changes in information technology and infrastructure.	Release 1A; Must
4.3.2.1.2	The system shall manage preservation processes.	Release 1C; Must
4.3.2.1.2.1	Preservation process management includes the scheduled assessments, and resulting actions based on the attributes of the digital objects, their essential behaviors, etc., and applies the appropriate processes.	Release 1C; Must
4.3.2.1.3	The system shall maintain the integrity of content throughout preservation processes.	Release 1C; Must
4.3.2.1.3.1	When compared to the original AIP, the content is fully intelligible and unchanged in meaning and representation.	Release 1C; Must
4.3.2.1.4	The system shall preserve all essential behaviors of digital content.	Release 1C; Must
4.3.2.1.4.1	The system shall maintain content functionality associated with content presentation.	Release 1C; Must
4.3.2.1.5	The system shall preserve all significant properties and attributes of digital content.	Release 1C; Must
4.3.2.1.5.1	The system shall maintain content context.	Release 1C; Must
4.3.2.1.5.2	The system shall maintain content structure.	Release 1C; Must
4.3.2.1.5.3	The system shall maintain hyperlinks to content within the target document.	Release 1C; Must
4.3.2.1.6	The system shall have the capability to produce DIPs which faithfully replicate AIPs.	Release 1B; Could / Release 1C; Must
4.3.2.1.6.1	The system shall have the capability to produce DIPs which are interoperable with other OAIS-based repositories.	Release 1B; Could / Release 1C; Must
4.3.2.1.7	The system shall be capable of scheduling or executing preservation processes on individual AIPs or on classes of archival content.	Release 1C; Must

4.3.2.2	**Preservation Processing**	
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 1C; Must
4.3.2.2.1.1	The system shall assure that the files resulting from migrations will be in a format free of proprietary restrictions.	Release 1C; Should / Release 2; Must
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 1C; Must
4.3.2.2.1.3	The system shall provide logs that record the results of migrations.	Release 1C; Must

4.3.2.2.1.4	The system shall have the ability to produce notification of incomplete or unsuccessful migrations.	Release 1C; Must
4.3.2.2.2	The system shall have the ability to preserve bitstreams in their native or received form by refreshment.	Release 1C; Must
4.3.2.2.2.1	The system shall have the ability to verify that the refreshed file retains specified attributes and behaviors, i.e. is authentic and faithful.	Release 1C; Must
4.3.2.2.2.2	The system shall provide logs that record the results of refreshment processes.	Release 1C; Must
4.3.2.2.2.3	The system shall have the ability to produce notification of incomplete or unsuccessful refreshments processes.	Release 1C; Must
4.3.2.2.3	The system shall have the ability to support emulation to preserve access to content.	Release 1C; Must
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 1C; Must
4.3.2.2.4	The system shall support the transformation of AIPs into ACPs.	Release 1B; Must
4.3.2.2.5	When a preservation process results in the creation of a modification of an AIP, the system shall be capable of retaining the original AIP as it was accepted into the repository.	Release 1C; Must

4.3.2.3	**Preservation Processing - Assessment**	
4.3.2.3.1	The system shall have the ability to assess ingested content and determine preservation processes based on the assessments.	Release 1C; Must
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 1C; Must
4.3.2.3.1.2	There shall be no limit set on the number or frequency of assessments.	Release 1C; Must
4.3.2.3.1.3	The system shall have the ability to re-assess content stored in the system.	Release 1C; Must
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 1C; Could

4.3.2.4	**Preservation Processing - Administration**	
4.3.2.4.1	The system shall support scheduling the automatic execution of preservation processes.	Release 1C; Must
4.3.2.4.2	The system shall support batch preservation processing of content.	Release 1C; Must
4.3.2.4.3	The system shall support preservation processing on an item-by-item basis.	Release 1C; Must
4.3.2.4.4	The system shall maintain an audit trail of preservation processes.	Release 1C; Must
4.3.2.4.5	The system shall support the ability for authorized users to request preservation processes.	Release 1C; Must

4.3.2.5	**Preservation Processing - Storage**	
4.3.2.5.1	The system shall provide a digital archival repository environment which is based on open-standards architecture.	Release 1A; Must
4.3.2.5.1.1	The repository environment shall keep AIPs separate from working or production copies.	Release 1A; Must
4.3.2.5.1.2	The system shall ensure that the content in a working or production copy is synchronized with the AIP.	Release 1A; Must
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 1A; Must

4.3.2.6	**Preservation Processing - Metadata**	

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 1A; Must
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 1A; Must
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 1A; Must

4.3.2.7	**Preservation Processing - Security**	
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 1A; Must

3.2.4.4.2	**Requirements for Unique Identifier**	
4.4.2.1	**Unique ID Core Capabilities**	
4.4.2.1.1	The system shall have the capability to organize file(s) into digital objects at a level of granularity appropriate to the content and as defined by GPO.	Release 1A; Must
4.4.2.1.1.1	The system shall have the capability to assign unique IDs to publications.	Release 1A; Must
4.4.2.1.1.2	The system shall have the capability to assign unique IDs to publications down to paragraph level.	Release 1C; Should / Release 2; Must
4.4.2.1.1.3	The system shall have the capability to assign unique IDs to individually provided graphical elements at the individual element level.	Release 1A; Must
4.4.2.1.1.4	The system shall have the capability to assign unique IDs to embedded graphical elements at the individual element level.	Release 1C; Should / Release 2; Must
4.4.2.1.1.5	The system shall have the capability to assign unique IDs to video content.	Release 1A; Must
4.4.2.1.1.6	The system shall have the capability to assign unique IDs to video content at a level of granularity as required by the system and GPO business units.	Release 3; Could
4.4.2.1.1.7	The system shall have the capability to assign unique IDs to audio content.	Release 1A; Must
4.4.2.1.1.8	The system shall have the capability to assign unique IDs to audio content at a level of granularity as required by the system and GPO business units.	Release 2; Could
4.4.2.1.2	The system must create and assign a 9 character alphanumeric identifier (ANI) for each unique digital object.	Release 1A; Must
4.4.2.1.2.1	Unique IDs must be non-intelligent.	Release 1A; Must
4.4.2.1.2.2	Unique ID characters must include numbers 0-9 and letters A – Z (minus I and O).	Release 1A; Must
4.4.2.1.2.3	Unique IDs must start with the character “A” (technical requirement).	Release 1A; Must
4.4.2.1.2.4	Unique IDs must not conflict with other identifiers within FDsys.	Release 1A; Must
4.4.2.1.2.5	The number of digital objects will be in accordance with the FDsys System Sizing document.	Release 1A; Must
4.4.2.1.3	The system shall have the ability to assign and accept a unique ID to a related or continuous piece of content in context.	Release 1A; Must
4.4.2.1.3.1	Scanned publications and submission level metadata	Release 1A; Must
4.4.2.1.3.2	Scanned publications at the page level	Release 1A; Must
4.4.2.1.4	Unique IDs must not conflict with other identifiers within FDsys.	Release 1A; Must
4.4.2.1.5	The system shall store unique IDs in metadata.	Release 1A; Must

4.4.2.2	**Job ID**	
4.4.2.2.1	The system must create and assign a unique ID for each job.	Release 1A; Must
4.4.2.2.2	The system must provide the capability to assign unique IDs to Content Originator orders of content jobs.	Release 1C; Must
4.4.2.2.3	The system must provide the capability to assign unique IDs to Content Originator orders of service jobs.	Release 1C; Must
4.4.2.2.4	The system must provide the capability to assign unique IDs to non-Content Originator order related jobs.	Release 1A; Must
4.4.2.2.5	The system must not re-use Job unique IDs.	Release 1A; Must

4.4.2.3	**Content Package ID**	
4.4.2.3.1	The system must create and assign a unique ID for each Content Package.	Multiple Releases
4.4.2.3.1.1	The system must create and assign a unique ID to each SIP	Release 1A; Must
4.4.2.3.1.2	The system must create and assign a unique ID to each AIP	Release 1A; Must
4.4.2.3.1.3	The system must create and assign a unique ID to each ACP	Release 1B; Must
4.4.2.3.1.4	The system must create and assign a unique ID to each DIP	Release 1B; Must
4.4.2.3.2	The system must not re-use Content Package unique IDs.	Release 1A; Must
4.4.2.3.3	The system must record package unique ID's in metadata.	Release 1A; Must

4.4.2.4	**Interface for Unique ID**	
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 1A; Must
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 1A; Must

3.2.4.5.2	**Requirements for Persistent Name**	
4.5.2.1	**Persistent Name Core Capabilities**	
4.5.2.1.1	The system shall assign persistent names to all in-scope published versions during access processing.	Release 1B; Must
4.5.2.1.1.1	Persistent name must not conflict with other identifiers within FDsys.	Release 1B; Must
4.5.2.1.2	The system shall comply with standards and best practices pertaining to persistent naming.	Release 1B; Must
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 1B; Should
4.5.2.1.4	The system shall accommodate OpenURL syntax to enable federated searching.	Release 1B; Must
4.5.2.1.5	The system shall arbitrate between Content Originator naming and global naming standards.	Release 1B; Must
4.5.2.1.5.1	The system shall defer to a persistent name assigned by GPO or by a GPO naming authority.	Release 1B; Must
4.5.2.1.6	The system shall assign persistent names that are location independent.	Release 1B; Must
4.5.2.1.7	The system shall assign persistent names that are protocol independent.	Release 1B; Must
4.5.2.1.8	The system must not reuse persistent names.	Release 1B; Must
4.5.2.1.9	The system shall have the capability to assign intelligent persistent names.	Release 1B; Must
4.5.2.1.10	The system shall have the capability to assign non-intelligent persistent names.	Release 1B; Could

4.5.2.1.11	The system shall have the capability to incorporate existing identifiers into the persistent naming string.	Release 1B; Could
4.5.2.1.12	The system shall have the capability to record the date and time of persistent name creation.	Release 1B; Must
4.5.2.1.13	The system shall have the capability to create reports about persistent name management.	Release 1C; Could
4.5.2.1.14	The system shall associate persistent names to existing legacy GPO naming schemes, including but not limited to GPO-assigned PURLs.	Release 1B; Must
4.5.2.1.15	The system shall be scalable in terms of persistent name assignment and resolvability.	Release 1B; Must

4.5.2.2	**Persistent Name Resolution**	
4.5.2.2.1	The system shall use a resolution system to locate and provide access to content with persistent names.	Release 1B; Must
4.5.2.2.1.1	The resolution process shall resolve an assigned name into a resource or the resource metadata.	Release 1B; Must
4.5.2.2.1.2	The resolution process must allow for persistent name recognition within standard browsers.	Release 1B; Must
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 1B; Must
4.5.2.2.3	The system shall support resolution of a single persistent name to multiple distributed locations.	Release 1B; Should
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 1B; Should
4.5.2.2.4	The system shall support resolution of a single persistent name to multiple content versions.	Release 1B; Should
4.5.2.2.4.1	The system shall determine the most appropriate version based attributes including, but not limited to, access privileges, format, location, date.	Release 1B; Should

4.5.2.3	**Persistent Name Metadata**	
4.5.2.3.1	The system shall record persistent names associated with content.	Release 1B; Must
4.5.2.3.2	The system shall record existing persistent names associated with content.	Release 1B; Must
4.5.2.3.3	The system shall provide the capability to associate metadata with the persistent name	Release 1B; Must

3.2.4.6.2	**Requirements for Authentication**	
4.6.2.1	**Authentication Core Capabilities**	
4.6.2.1.1	The system must provide the capability to verify content as authentic meaning that it is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator.	Release 1A; Must
4.6.2.1.2	The system must provide the capability to certify content as official meaning that the content has been approved by, contributed by, or harvested from an official source such as a Federal publishing agency, its business partner, or other trusted source.	Release 1A; Must
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 1A; Must
4.6.2.1.3	The system must provide the capability to certify content at levels of granularity defined in GPO.	Release 1A; Must

4.6.2.1.4	The system must provide the capability to convey certification by means of an integrity mark.	Release 1A; Must
4.6.2.1.5	The system shall provide the capability to use GPO's Public Key Infrastructure (PKI) wherever optimal.	Release 1A; Should
4.6.2.1.6	The system must comply with GPO and Federal privacy policies.	Release 1A; Must
4.6.2.1.7	The system must comply with GPO and Federal authentication policies.	Release 1A; Must
4.6.2.1.8	The system must use public key cryptography, digital certificates, encryption or other widely accepted information security mechanisms.	Release 1A; Must

4.6.2.2	**Authentication - Content Pre-ingest and Ingest**	
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 1A; Must
4.6.2.2.1.1	The system shall verify Content Originator identity and authority to publish for content that is deposited with the system.	Release 1A; Must
4.6.2.2.1.2	Valid proof of the Content Originator's identity shall be logged by the system.	Release 1A; Must
4.6.2.2.1.3	The source of the deposited content shall be recorded in metadata.	Release 1A; Must
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 Content Originator to the system, and information about content integrity should be recorded in metadata.	Release 1A; Must
4.6.2.2.1.5	The system shall verify that the sender (Content Originator) and the recipient (GPO) were, in fact, the parties who claimed to send or receive content, respectively, and this information should be recorded in metadata.	Release 1A; Must
4.6.2.2.1.6	The system shall have the capability to record intended use in metadata.	Release 1A; Must
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 1A; Must
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 1A; Must
4.6.2.2.2.1	The system shall examine harvested content for the purpose of verifying the source of the harvested content.	Release 1A; Must
4.6.2.2.2.2	The source of harvested content shall be recorded in metadata.	Release 1A; Must
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 1A; Must
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 1A; Must
4.6.2.2.3.1	The source of converted content shall be recorded in metadata.	Release 1A; Must
4.6.2.2.3.2	The source of tangible content that was used to create the converted content shall be recorded in metadata.	Release 1A; Must
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 Service Provider to the system, and information about content integrity should be recorded in metadata.	Release 1A; Must
4.6.2.2.3.4	The system shall verify that the sender (Service Provider) and the recipient (GPO) were, in fact, the parties who claimed to send or receive content, respectively and this information should be recorded in metadata.	Release 1A; Must
4.6.2.2.3.5	The system shall have the capability to record intended use in metadata.	Release 1A; Must

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 1A; Must
4.6.2.2.4	The system must provide the capability to recognize and validate integrity marks at pre-ingest.	Release 1A; Must
4.6.2.2.4.1	The system shall have the capability to retain integrity marks in accordance with GPO business rules.	Release 1A; Must
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 1A; Must
4.6.2.2.5	The system shall provide the capability to process encrypted files at pre-ingest.	Release 1A; Could / Release 2: Must
4.6.2.2.6	The system must verify chain of custody at pre-ingest.	Release 1A; Must
4.6.2.2.6.1	Chain of custody information shall be recorded in metadata.	Release 1A; Must
4.6.2.2.6.2	The system shall have the ability to gather relevant information from integrity marks (e.g., digital signatures, digital certificates) for use as part of the chain of custody.	Release 1A; Must
4.6.2.2.7	The system must provide the capability to perform redundancy checking (e.g., checksum) on content at ingest.	Release 1A; Must
4.6.2.2.7.1	The system must provide the capability to record checksum type and value in metadata.	Release 1A; Must
4.6.2.2.8	The system must provide the capability to apply a digital timestamp to content at ingest.	Release 1A; Must
4.6.2.2.9	The system must update chain of custody information in metadata at ingest.	Release 1A; Must

4.6.2.3	**Authentication - User Credentials**	
4.6.2.3.1	The system must provide the capability to verify the identity of the Content Originator.	Release 1A; Must
4.6.2.3.2	The system must provide the capability to verify the Content Originator's authority to publish.	Release 1A; Must

4.6.2.4	**Authentication - Content Integrity**	
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 1A; Must
4.6.2.4.2	The system must assure integrity of content within the system.	Release 1A; Must
4.6.2.4.2.1	The system shall have the capability to assure integrity of content within the system at a definable frequency.	Release 1A; Must
4.6.2.4.2.2	The system shall have the capability to assure integrity of content in a timeframe based on GPO business rules.	Release 1A; Must
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 1A; Must
4.6.2.4.2.4	The system shall have the capability to assure integrity of content during backup and other system processes.	Release 1A; Must
4.6.2.4.3	The system must assure integrity of pre-ingested and ingested content.	Release 1A; Must
4.6.2.4.3.1	Content integrity shall be maintained during transmission from the Content Originator to the system.	Release 1A; Must
4.6.2.4.3.2	The system shall have the capability to verify and 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 1A; Must

4.6.2.4.4	The system must have the capability to assure integrity of delivered content.	Release 1B; Must
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 1B; Must
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 1B; Must
4.6.2.4.5	The system must provide the capability to provide notification that a change has occurred to content within the system.	Release 1A; Must
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 1A; Must
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 1A; Must
4.6.2.4.5.3	The system shall provide the capability to notify designated users when changes were made to content.	Release 1A; Must
4.6.2.4.5.4	The system shall provide the capability to notify designated users where changes were made to content.	Release 1A; Must
4.6.2.4.5.5	The system shall provide the capability to notify designated users by whom changes were made to content.	Release 1A; Must
4.6.2.4.5.6	The system shall provide the capability to notify designated users what changes were made to content.	Release 1A; Must
4.6.2.4.5.7	The system shall log changes to content in metadata.	Release 1A; Must
4.6.2.4.6	The system must provide the capability of demonstrating continued integrity of content packages when authorized changes are made (such as to the metadata).	Release 1A; Must

4.6.2.5	**Authentication - Time Stamps**	
4.6.2.5.1	The system must support digital time stamping.	Release 1A; Must
4.6.2.5.2	The system must provide the capability to provide date and time verification.	Release 1A; Must
4.6.2.5.3	The system must 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 1A; Must

4.6.2.6	**Authentication - Integrity Marks**	
4.6.2.6.1	The system must support the use of integrity marks.	Release 1A; Must
4.6.2.6.2	Integrity marks must include certification information.	Release 1A; Must
4.6.2.6.3	Integrity marks must employ widely accepted information security mechanisms (e.g., public key cryptography, digital certificates, digital signatures, XML signatures, digital watermarks, or traditional watermarks).	Release 1A; Must
4.6.2.6.4	The system must support the capability to manually add integrity marks to content.	Release 1B; Could
4.6.2.6.5	The system must support the capability to automatically add integrity marks to content.	Release 1B; Must
4.6.2.6.6	The system must support the use of visible integrity marks.	Release 1B; Must
4.6.2.6.7	The system must support the use of invisible integrity marks.	Release 1B; Could / Release 2; Must
4.6.2.6.8	The system must provide flexibility regarding where the integrity mark is applied through automated and manual processes.	Release 1B; Must
4.6.2.6.9	The system must 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 1B; Must
4.6.2.6.10	The system must support the application of multiple integrity marks on the same content.	Release 1B; Must

4.6.2.6.11	The system must support the application of security policies, such that integrity marks can be applied to content in particular sequences depending on levels of authority.	Release 1B; Must

4.6.2.7	**Authentication - Content Delivery**	
4.6.2.7.1	The system must provide the capability for users to validate the authenticity, integrity, and official status of the content packages that are delivered from the system.	Release 1B; Must
4.6.2.7.2	The system must 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 1B; Must
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:	multiple releases
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 1B; Could
4.6.2.7.3.2	The integrity mark must include certification information including the following but not limited to the following:	Release 1B; Must
4.6.2.7.3.3	Wherever feasible, the values for the above fields shall be extracted from the digital certificate that was used to create the digital signature.	Release 1B; Must
4.6.2.7.3.4	The system shall provide the flexibility to add new fields.	Release 1B; Must
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 1B; Must
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 1B; Must
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 1B; Must
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 1B; Should / Release 2; Must
4.6.2.7.3.9	For electronic presentation, validation shall be done automatically without End User intervention.	Release 1B; Should / Release 2; Must

4.6.2.8	**Re-authentication of Content**	
4.6.2.8.1	The system must provide the capability to re-authenticate content that has already been authenticated (e.g., expired certificate).	Release 1A; Could
4.6.2.8.2	The system must provide the capability to notify GPO System Administrators when content needs to be re-authenticated.	Release 1A; Could
4.6.2.8.3	The system must provide the capability for GPO to change or revoke the authentication status of content.	Release 1A; Must

4.6.2.9	**Authentication Standards/Best Practices**	
4.6.2.9.1	The system must have the capability to support RSA Digital Signature in accordance with IETF RFC 3447.	Release 1A; Must
4.6.2.9.2	The system must have the capability to support PKCS #1 for RSA key pair for digital signatures.	Release 1A; Must

4.6.2.9.3	The system must have the capability to support IEFT Public Key Infrastructure (PKIX) X. 509 v. 3 standards for certificate compatibility.	Release 1A; Must
4.6.2.9.4	The system must have the capability to support PKCS #1, #7, #11, and #12.	Release 1A; Must
4.6.2.9.5	The system must have the capability to support ITU X.509 version 3 standard for certificate format.	Release 1A; Must
4.6.2.9.6	The system must have the capability to support up to 2048-bit RSA public/private key generation (asymmetric algorithm).	Release 1A; Must
4.6.2.9.7	The system must have the capability to support cryptographic standards in accordance with the FIPS 140 series.	Release 1A; Must
4.6.2.9.7.1	The system must have the capability to comply with HMS FIPS 140-2.	Release 1A; Must
4.6.2.9.8	The system must have the capability to support FIPS 180-2 for SHA-1, SHA-256, SHA-384, and SHA-512.	Release 1A; Must
4.6.2.9.9	The system must have the capability to support Redundancy Checking including Cyclic Redundancy Checking (CRC) and checksum.	Release 1A; Must
4.6.2.9.10	The system must have the capability to support XML Digital Signature standards RFC 3275 and XMLDSIG.	Release 1A; Must
4.6.2.9.11	The system must have the capability to support AES encryption standard FIPS 197.	Release 1A; Must
4.6.2.9.12	The system must have the capability to support XML Encryption standard XMLENC.	Release 1A; Must
4.6.2.9.13	The system must have the capability to support TDES ANSI X9.52.	Release 1A; Must
4.6.2.9.14	The system must have the capability to support SSL / TLS.	Release 1A; Must
4.6.2.9.15	The system must have the capability to support LDAP IETF RFC 2251.	Release 1A; Must
4.6.2.9.16	The system must have the capability to support ITU X.500.	Release 1A; Must
4.6.2.9.17	The system must have the capability to support SAML.	Release 1A; Must
4.6.2.9.18	The system must be based on open standards including ITU, ISO, PKCS, IETF, ANSI and other open standards.	Release 1A; Must
4.6.2.9.19	The system must accommodate updates to the above cryptographic standards.	Release 1A; Must
4.6.2.9.20	The system must have the capability to comply with current electronic signature guidance from the National Archives and Records Administration including "Records Management Guidance for Agencies Implementing Electronic Signature Technologies."	Release 1A; Must

4.6.2.10	**Authentication Records Management**	
4.6.2.10.1	The system must create administrative records of authentication processes.	Release 1A; Must
4.6.2.10.2	The system must create transaction records of administrative processes.	Release 1A; Must
4.6.2.10.3	The system must support an audit capability for content certification.	Release 1A; Must
4.6.2.10.4	The system must support an audit capability for content validation.	Release 1A; Must
4.6.2.10.5	The system must comply with GPO and Federal records management policies.	Release 1A; Must

4.6.2.11	**Authentication Metadata**	
4.6.2.11.1	The system must provide the capability to include authentication and certification information in metadata.	Release 1A; Must
4.6.2.11.1.1	Authenticity metadata shall have the capability to include the following:	Release 1A; Must
4.6.2.11.1.2	Integrity metadata shall have the capability to include the following:	Release 1A; Must

4.6.2.1.1.1	Non-repudiation metadata shall have the capability to include the following:	Release 1A; Must
4.6.2.1.1.2	Intended Use metadata shall have the capability to include the following:	Release 1A; Must

3.2.4.7.2	Requirements for Version Control	
4.7.2.1	**Version Control Core Capabilities**	
4.7.2.1.1	The system shall have the ability to assign unique version identifiers to content packages that do not already contain version identifiers.	Release 1A; Should / Release 1C; Must
4.7.2.1.1.1	Version identifiers will be created at the time the version detection mechanism has activated a version trigger and detected a new version.	Release 1A; Should / Release 1C; Must
4.7.2.1.2	The system shall record existing version identifiers.	Release 1A; Must
4.7.2.1.2.1	Recorded version identifiers will be human and machine readable.	Release 1A; Must
4.7.2.1.3	The system must allow authorized users to input, view, and manage version information.	Release 1A; Must
4.7.2.1.4	The system shall have the capability to alert a Service Specialist and Content Originators when duplicate content is rejected.	Release 1A; Should / Release 1B; Must
4.7.2.1.5	The system shall log all version history.	Release 1A; Must
4.7.2.1.5.1	The version history log shall be incorporated into the package's metadata.	Release 1A; Must
4.7.2.1.6	The system shall provide the capability to apply version control to work in progress content.	Release 1A; Could / Release 1C; Should; Release 2; Must

4.7.2.2	**Version Triggers**	
4.7.2.2.1	The system must apply rules for version triggers.	Release 2; Must
4.7.2.2.1.1	The system shall apply rules for version triggers to groups of related content as defined by GPO business units.	Release 2; Must
4.7.2.2.1.2	Content Evaluators must be able to modify rules for version triggers.	Release 2; Must
4.7.2.2.2	The system shall detect version triggers as defined by GPO business units. Version triggers include, but are not limited to, the following:	Release 2; Must
4.7.2.2.3	The system shall provide the capability to alert users when version triggers have been activated.	Release 2; Must
4.7.2.2.3.1	This will be done through channels that include push and pull technologies (e.g., notifications lists, RSS feeds).	Release 2; Must
4.7.2.2.4	The system shall provide the capability to notify designated GPO Service Specialists when a version cannot be determined.	Release 2; Must

4.7.2.3	**Version Detection**	
4.7.2.3.1	The system shall determine if version identifiers are present in content packages.	Release 1A; Must
4.7.2.3.1.1	Version identifiers will be stored in metadata.	Release 1A; Must

4.7.2.4	**Version Metadata**	
4.7.2.4.1	The system shall express version information in metadata.	Release 1A; Must
4.7.2.4.1.1	The system will update the metadata to indicate changes to attributes (e.g., structure, content, format, etc.).	Release 1A; Must
4.7.2.4.2	The system shall record chain of custody in metadata (e.g., who created the content, when it was created, who approved the content for release, etc.).	Release 1A; Must

4.7.2.5	**Version Relationships**	

4.7.2.5.1	The system shall determine and record relationships between versions (e.g., version links).	Release 1A; Must
4.7.2.5.1.1	The system will establish links to related documents identified through version information in metadata.	Release 1A; Must
4.7.2.5.1.2	Reference to these relationships will be permanently available.	Release 1A; Must
4.7.2.5.1.3	The system must be able to render relationship information so that it is human-readable.	Release 1A; Must

4.7.2.6	**Version Notification**	
4.7.2.6.1	The system shall have the capability to notify users which version of content they are accessing.	Release 1B; Must
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 1B; Must
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 1B; Must
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 1B; Must
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
4.7.2.6.1.5	The system shall have the capability to notify users that access to a version is restricted.	Release 1B; Must

3.2.5.1.2	Requirements for Workflow	
5.1.2.1	**Workflow Core Capabilities**	
5.1.2.1.1	The system shall provide the capability to define workflows.	Release 1A; Must
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 1A; Must
5.1.2.1.1.2	The system shall provide the capability to validate workflow definitions against the established schema.	Release 1A; Must
5.1.2.1.2	The system shall provide the capability to create new versions of existing workflows.	Release 1A; Must
5.1.2.1.3	The system shall provide the capability to test new versions of existing workflows without interrupting the current workflow.	Release 1A; Must
5.1.2.1.4	The system shall provide the capability to place new versions of workflow into production.	Release 1A; Must
5.1.2.1.4.1	The system shall provide the capability to deploy newly developed or modified workflows without interruption to other workflows.	Release 1A; Must
5.1.2.1.5	The system shall provide the capability to replace current versions of workflows with previous versions when required without interruption to other workflows.	Release 1A; Must
5.1.2.1.6	The system shall provide the capability to manage business rules.	Release 1A; Must
5.1.2.1.6.1	The business rules shall support user-defined hierarchy structure (e.g. related rules are self-aware of precedence).	Release 1A; Must
5.1.2.1.7	The system shall provide the capability to manage manual activities.	Release 1A; Must
5.1.2.1.8	The system shall provide the capability to manage automated activities.	Release 1A; Must
5.1.2.1.9	The system shall provide the capability to assign comments on jobs/activities.	Release 1B; Must
5.1.2.1.10	The system shall provide the capability for checkpointing critical workflow status and processes (e.g. taking a snapshot of the current system in the event of a system failure).	Release 1A; Must

5.1.2.1.10.1	The system shall provide the capability for saved data from checkpointing to be portable to other failover locations.	Release 1A; Must
5.1.2.1.10.2	The system shall provide the capability for the frequency of checkpointing the system to be controlled by the user.	Release 1A; Must
5.1.2.1.10.2.1	The system shall provide the capability for checkpointing to be automated or manually controlled.	Release 1A; Must
5.1.2.1.10.3	The system shall provide the capability for the user to control the scope of the data captured by checkpointing.	Release 1A; Must
5.1.2.1.10.4	The checkpointing of the system shall be transparent to the user.	Release 1A; Must
5.1.2.1.11	The system shall store information related to workflows in metadata.	Release 1A; Must
5.1.2.1.11.1	The system shall store information about workflows in metadata.	Release 1A; Must
5.1.2.1.11.2	The system shall store information about jobs in metadata.	Release 1A; Must
5.1.2.1.11.3	The system shall store information about activities in metadata.	Release 1A; Must

5.1.2.2	**Workflow - Control of Execution**	
5.1.2.2.1	The system shall provide the capability to control the execution of activities.	Release 1A; Must
5.1.2.2.1.1	The system shall provide the capability to sequence activities to optimize operations.	Release 1A; Could / Release 2; Must
5.1.2.2.1.2	The system shall provide the capability to schedule for manual and automated activities.	Release 1A; Could / Release 1B; Must
5.1.2.2.1.2.1	The system shall provide the capability to assign deadlines for jobs/activities.	Release 1A; Could / Release 1B; Must
5.1.2.2.1.2.2	The system shall provide the capability to assign estimated completion times for jobs/activities.	Release 1A; Could / Release 1B; Must
5.1.2.2.1.3	The system shall provide the capability to assign human resources to manual activities.	Release 1A; Could
5.1.2.2.1.4	The system shall provide the capability to suspend and resume activities.	Release 1A; Must
5.1.2.2.1.5	The system shall provide the capability to restart activities.	Release 1A; Must
5.1.2.2.1.6	The system shall provide the capability to cancel activities.	Release 1A; Must
5.1.2.2.1.7	The system shall provide the capability to log activities.	Release 1A; Must
5.1.2.2.1.8	The system shall provide the capability to manage work lists of activities.	Release 1A; Must
5.1.2.2.1.9	The system shall provide the capability to perform actions on a batch of activities.	Release 1A; Must
5.1.2.2.2	The system shall provide the capability to control the execution of jobs.	Release 1A; Must
5.1.2.2.2.1	The system shall provide the capability to sequence jobs to optimize operations.	Release 1A; Should
5.1.2.2.2.2	The system shall provide the capability to suspend and resume jobs.	Release 1A; Must
5.1.2.2.2.3	The system shall provide the capability to cancel a job.	Release 1A; Must
5.1.2.2.2.4	The system shall provide the capability to adjust the priority of a job at any time.	Release 1A; Must
5.1.2.2.2.4.1	The system shall provide the capability to adjust the priority of a job manually or automatically.	Release 1A; Must
5.1.2.2.2.5	The system shall provide the capability to log jobs.	Release 1A; Must
5.1.2.2.2.6	The system shall provide the capability to manage work lists of jobs.	Release 1A; Must
5.1.2.2.2.7	The system shall provide the capability to perform actions on a batch of jobs.	Release 1A; Must

5.1.2.3	**Workflow - Monitoring**	
5.1.2.3.1	The system shall provide a monitoring tool for all workflow activities.	Release 1A; Must

5.1.2.3.1.1	The monitoring tool shall provide the capability to visualize a set of activities.	Release 1A; Must
5.1.2.3.1.2	The monitoring tool shall provide the capability for the user to customize views.	Release 1A; Could / Release 2; Must
5.1.2.3.1.3	The monitoring tool shall provide the capability to save customized views for future use.	Release 1A; Could / Release 2; Must
5.1.2.3.1.4	The monitoring tool shall provide the capability for users to monitor processing history.	Release 1A; Must
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 1A; Could / Release 2; Must
5.1.2.3.1.5	The monitoring tool shall report performance measures, including but not limited to:	Release 1A; Must
5.1.2.3.2	The system shall provide the capability for users to monitor jobs or groups of jobs.	Release 1A; Must
5.1.2.3.2.1	The system shall provide the capability for users to monitor one or more jobs simultaneously.	Release 1A; Must
5.1.2.3.2.2	The system shall provide the capability to monitor planned, scheduled and actual times for selected jobs.	Release 1A; Must
5.1.2.3.2.3	The system shall provide the capability to group jobs with a defined status.	Release 1A; Must
5.1.2.3.3	The system shall provide the capability for users to monitor activities or groups of activities.	Release 1A; Must
5.1.2.3.3.1	The system shall provide the capability for users to monitor one or more activities simultaneously.	Release 1A; Must
5.1.2.3.3.2	The system shall provide the capability to monitor planned, scheduled and actual times for selected activities.	Release 1A; Must
5.1.2.3.3.3	The system shall provide the capability to group activities with a defined status.	Release 1A; Must

5.1.2.4	**Workflow - Resource Requirements**	
5.1.2.4.1	The system shall provide the capability to estimate resource requirements associated with internal workflow.	Release 1A; Could / Release 1B; Must
5.1.2.4.2	The system shall provide the capability to estimate resource requirements associated with external workflow.	Release 1A; Could / Release 1B; Must
5.1.2.4.3	The system shall provide the capability to estimate resource requirements for automated and manual activities.	Release 1A; Could / Release 1B; Must

5.1.2.5	**Workflow - Notification**	
5.1.2.5.1	The system shall provide the capability to associate notifications with workflows.	Release 1A; Must
5.1.2.5.2	The system shall provide the capability to manage notifications attached to workflows.	Release 1A; Must
5.1.2.5.3	The system shall send notifications including but not limited to e-mail and the user’s screen.	Release 1A; Must
5.1.2.5.4	The system shall provide the capability to configure the list of recipients of notifications.	Release 1A; Must
5.1.2.5.5	The system shall provide the capability to escalate notifications.	Release 1A; Should

5.1.2.6	**Workflow - Security**	
5.1.2.6.1	The system shall provide the capability to have security controls on workflow activities.	Release 1A; Must
5.1.2.6.1.1	The security control (allow or deny actions) shall be rule based.	Release 1A; Must
5.1.2.6.1.2	Manual activities in the workflows shall be assigned with one or more security rules.	Release 1A; Must

5.1.2.7	Workflow - Interface	
5.1.2.7.1	The system shall provide a Graphical User Interface (GUI) edit tool to manage workflow definitions and executions.	Release 1A; Must
5.1.2.7.2	The Monitoring Tool shall contain a GUI for all workflow monitoring capabilities.	Release 1A; Must

3.2.5.2.2	Requirements for Storage Management	
5.2.2.1	Storage Core Capabilities	
5.2.2.1.1	The system shall support error-free retrieval of data to network storage at rated network speeds (e.g., 2 Gbps).	Release 1A; Must
5.2.2.1.2	The system shall be capable of providing a secure repository environment for all storage.	Release 1A; Must
5.2.2.1.3	The system shall provide the ability to move content into and between stores transparently.	Release 1A; Must

5.2.2.2	Networked High Performance Storage	
5.2.2.2.1	Networked High Performance Storage shall have the ability to store data dynamically in high performance-high availability stores and external Content Delivery Networks (CDN) based on hit rate/criticality of content.	Release 1A; Must
5.2.2.2.1.1	Networked High Performance Storage shall have the capability to manage the threshold hit rate for content to automatically move to the Network High Performance Storage.	Release 1A; Must
5.2.2.2.1.2	Networked High Performance Storage shall have the capability to manage the criticality of specific content for Network High Performance Storage.	Release 1A; Must
5.2.2.2.2	The system shall have the capability to utilize external storage Service Providers.	Release 1A; Must
5.2.2.2.3	Networked High Performance Storage shall have the capability to support direct application access with latency in application performance less than 1 second.	Release 1A; Must
5.2.2.2.4	Networked High Performance Storage shall be able to support automated fail-over without buffer application data loss.	Release 1A; Must
5.2.2.2.5	Networked High Performance Storage shall operate reliably to allow less than 0.1% downtime.	Release 1A; Must
5.2.2.2.6	Networked High Performance Storage shall have record management capabilities.	Release 1A; Must
5.2.2.2.7	Networked High Performance Storage shall have redundant components that will take over in the event of a hardware failure in the primary part.	Release 1A; Must
5.2.2.2.7.1	The system shall allow the switchover to redundant components via either user action or automatic processes.	Release 1A; Must
5.2.2.2.8	Networked High Performance Storage shall be able to support hot-spare standby drives (e.g. extra drives installed in the disk array that automatically come online in the event of a disk failure).	Release 1A; Must
5.2.2.2.8.1	Networked High Performance Storage shall allow the switchover to redundant components via either user action or automatic in case of failure.	Release 1A; Must
5.2.2.2.9	Networked High Performance Storage shall have a full-system battery backup to allow the disk array to remain operational in the event of a power outage.	Release 1A; Must

5.2.2.3	Networked Moderate Performance Storage	

5.2.2.3.1	Networked Moderate Performance Storage shall support static and dynamic storage assignment.	Release 1A; Must
5.2.2.3.2	Networked Moderate Performance Storage shall have limited scalability (e.g., multi- tens of terabyte capacities).	Release 1A; Must
5.2.2.3.3	Networked Moderate Performance Storage shall have open support (control of its resources) for a consolidated storage management back plane.	Release 1A; Must
5.2.2.3.4	Networked Moderate Performance Storage shall operate reliably to allow less than 0.2% downtime.	Release 1A; Must
5.2.2.3.5	Networked Moderate Performance Storage shall have the capability to support direct application access with latency in application performance less than 3 seconds.	Release 1A; Must

5.2.2.4	**Low Criticality- Low Cost Storage**	
5.2.2.4.1	Low Criticality - Low Cost Storage shall support low cost devices (e.g., Serial ATA storage drives).	Release 1A; Must
5.2.2.4.2	Low Criticality - Low Cost Storage shall allow central control and allocation of storage resources.	Release 1A; Must
5.2.2.4.3	Low Criticality - Low Cost Storage shall allow RAID 0 thru 5 configurations.	Release 1A; Must
5.2.2.4.4	Low Criticality - Low Cost Storage shall allow scaling and partitioning.	Release 1A; Must
5.2.2.4.5	Low Criticality - Low Cost Storage shall operate reliably with less than 0.3% downtime.	Release 1A; Must

5.2.2.5	**Failover Storage**	
5.2.2.5.1	Failover Storage shall have a fault tolerance-system able to survive local environmental casualties.	Release 1A; Must
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 1A; Must
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 1A; Must
5.2.2.5.3	Failover Storage shall allow RAID 0 thru 5 configurations.	Release 1A; Must
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 1A; Must

5.2.2.6	**Backup Retrieval Media Storage**	
5.2.2.6.1	Back-up Retrieval Media Storage shall be able to accomplish periodic backup on mass removable storage media.	Release 1A; Must
5.2.2.6.1.1	Back-up Retrieval Media Storage shall allow users to manage periodic backup schedules.	Release 1A; Must
5.2.2.6.1.2	Back-up Retrieval Media Storage shall allow backups on multiple types of mass removable storage media.	Release 1A; Must
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 1A; Must
5.2.2.6.2.1	Back-up Retrieval Media Storage shall allow users to manage which data is listed as critical.	Release 1A; Must
5.2.2.6.2.2	Back-up Retrieval Media Storage shall allow users to manage the backup schedule.	Release 1A; Must
5.2.2.6.2.3	Back-up Retrieval Media Storage shall not interfere with current system processes.	Release 1A; Must

5.2.2.6.3	Back-up Retrieval Media Storage shall have battery backed-up cache (e.g., battery power that protects any data that happens to be in cache at the time of a power interruption).	Release 1A; Must
5.2.2.6.4	Back-up Retrieval Media Storage shall support mirrored cache (e.g., the process of mirroring the write data in cache as a further method of data protection).	Release 1A; Must
5.2.2.6.4.1	Back-up Retrieval Media Storage shall allow users to manage which data should be mirrored and where it should be stored.	Release 1A; Must
5.2.2.6.5	Back-up Retrieval Media Storage shall have cache or disk scrubbing (e.g., a method of proactively testing data for errors even when the cache or disk is inactive, so that problems can be detected before they can disrupt data flow).	Release 1A; Must
5.2.2.6.5.1	Back-up Retrieval Media Storage shall allow users the ability to both schedule and manually scrub disks/caches.	Release 1A; Must
5.2.2.6.6	Back-up Retrieval Media Storage must be able to support remote mirroring, or the process of copying data to a second disk array, often housed in a separate location from the originating disk array.	Release 1A; Must

5.2.2.7	**Mid-term Archival Storage**	
5.2.2.7.1	Mid-term Archival Storage shall have off-line storage and indexing capability for 100's of Terabytes of data.	Release 1C; Must
5.2.2.7.2	Mid-term Archival Storage shall preserve data integrity and quality for no less than 10 Years in a data center environment.	Release 1A; Must

5.2.2.8	**Long-term Permanent Archival Storage**	
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
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 1A; Must
5.2.2.8.3	Long-term Permanent Archival Storage site must preserve physical data integrity and quality for no less than 100 Years under controlled storage conditions (e.g., 70° F, 60% Humidity).	Release 1A; Must

5.2.2.9	**Functional Data Storage**	
5.2.2.9.1	Work In Progress (WIP) Storage	Release 1A; Must
5.2.2.9.1.1	WIP Storage shall contain Networked High Performance Storage.	Release 1A; Must
5.2.2.9.1.2	WIP Storage shall contain Mid-term Archival Storage.	Release 1A; Must
5.2.2.9.1.3	WIP Storage shall contain Failover Storage.	Release 1A; Must
5.2.2.9.1.4	WIP Storage shall contain Back-up Retrieval Media Storage.	Release 1A; Must
5.2.2.9.1.5	WIP Storage shall contain both content and metadata.	Release 1A; Must
5.2.2.9.2	Archival Information Storage (AIS)	Release 1A; Must
5.2.2.9.2.1	AIS shall contain Networked Moderate Performance Storage.	Release 1A; Must
5.2.2.9.2.2	AIS shall contain Long-term Permanent Archival Storage.	Release 1A; Must
5.2.2.9.2.3	AIS shall contain Failover Storage.	Release 1A; Must
5.2.2.9.2.4	AIS shall contain Back-up Retrieval Media Storage.	Release 1A; Must
5.2.2.9.2.5	AIS shall exist in isolation of other system stores.	Release 1A; Must
5.2.2.9.2.6	AIS content must remain free from corruption and remain accessible as GPO undergoes changes in information technology and infrastructure.	Release 1A; Must
5.2.2.9.2.7	AIS shall contain both content and metadata.	Release 1A; Must
5.2.2.9.3	Access Content Storage (ACS)	Release 1B; Must
5.2.2.9.3.1	ACS shall contain Networked High Performance Storage.	Release 1B; Must
5.2.2.9.3.2	ACS shall contain Networked Moderate Performance Storage.	Release 1B; Must

5.2.2.9.3.3	ACS shall contain Low Criticality - Low Cost Storage.	Release 1B; Must
5.2.2.9.3.4	ACS shall contain Mid-term Archival Storage.	Release 1B; Must
5.2.2.9.3.5	ACS shall contain Long-term Permanent Archival Storage.	Release 1B; Must
5.2.2.9.3.6	ACS shall contain Failover Storage.	Release 1B; Must
5.2.2.9.3.7	ACS shall contain Back-up Retrieval Media Storage.	Release 1B; Must
5.2.2.9.3.8	ACS shall contain both content and metadata.	Release 1B; Must
5.2.2.9.4	Business Process Storage (BPS)	Release 1A; Must
5.2.2.9.4.1	BPS shall contain Networked High Performance Storage.	Release 1A; Must
5.2.2.9.4.2	BPS shall contain Networked Moderate Performance Storage.	Release 1A; Must
5.2.2.9.4.3	BPS shall contain Low Criticality - Low Cost Storage.	Release 1A; Must
5.2.2.9.4.4	BPS shall contain Mid-term Archival Storage.	Release 1A; Must
5.2.2.9.4.5	BPS shall contain Long-term Permanent Archival Storage.	Release 1A; Must
5.2.2.9.4.6	BPS shall contain Failover Storage.	Release 1A; Must
5.2.2.9.4.7	BPS shall contain Back-up Retrieval Media Storage.	Release 1A; Must

5.2.2.10	**Storage System Standards**	
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 1A; Must
5.2.2.10.2	The system shall support multiple file systems including but not limited to: Windows XP Filesystem, Linux File System, SunOS File System, Solaris Filesystem, Apple, FAT, FAT32, VFAT, NTFS, HPFS, EXT2.	Release 1A; Must
5.2.2.10.3	The system shall utilize common Redundant Array of Independent Disks (RAID) Disk Data Format (DDF) architecture.	Release 1A; Must
5.2.2.10.4	The system shall conform to common protocols, including but not limited to: Apple File Protocol (AFP), Network File System (NFS), SMB and CIFS protocols, Simple Network Management Protocol (SNMP), Internet Small Computer Systems Interface (iSCSI), Internet Fibre Channel Protocol (iFCP), Fibre Channel over IP (FCIP), Serial across SCSI (SAS), and Serial ATA.	Release 1A; Must
5.2.2.10.5	The system shall allow interaction with management information bases (MIB) via SNMP, and must conform to or interoperate within Object-based Storage Device (OSD) specification.	Release 1A; Must
5.2.2.10.6	The system storage shall support ANSI INCITS 388-2004 Storage Management Initiative Specification.	Release 1A; Must
5.2.2.10.7	The system back-up tapes shall conform to Linear Tape-Open (LTO) standard.	Release 1A; Must

5.2.2.11	**Storage - Monitoring**	
5.2.2.11.1	The system shall have the capability to be monitored for real-time health of the system components.	Release 1A; Must
5.2.2.11.2	Monitoring shall have the capability to have conditional thresholds customized to allow timely preventative maintenance.	Release 1A; Must
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 1A; Must
5.2.2.11.3.1	The system shall send notifications including but not limited to notifications on appropriate user screen and e-mail.	Release 1A; Must
5.2.2.11.3.2	The system shall allow for the definition and management of different levels of notification by users.	Release 1A; Must
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 1A; Must

5.2.2.11.5	The system shall have the ability to monitor data access history and evaluate appropriate storage in terms of cost and performance, in accordance with the FDsys Data Mining requirements.	Release 1A; Must
5.2.2.11.6	The system shall have the ability to monitor health of externally hosted data stores.	Release 1A; Must
5.2.2.11.7	The system shall support user configurable RAID levels. (e.g., the ability to configure storage RAID levels in the field without vendor intervention).	Release 1A; Must

5.2.2.12	**Storage - Preventive Action**	
5.2.2.12.1	The system shall have the ability to have automated preventative actions configured to allow critical failures from causing data loss.	Release 1A; Must
5.2.2.12.2	The system shall have the ability to allow hot swapping of components should a failure condition be detected.	Release 1A; Must
5.2.2.12.3	The system shall have the ability to dynamically move data to improve system performance.	Release 1A; Must
5.2.2.12.4	The system shall be able to execute non-disruptive microcode updates or replacements or the ability to update or replace the RAID controller microcode without having to shut down the disk array.	Release 1A; Must

5.2.2.13	**Storage - Data Integrity**	
5.2.2.13.1	The system shall allow for securing of partitions.	Release 1A; Must
5.2.2.13.2	The system shall allow encryption of logical content.	Release 1A; Must
5.2.2.13.3	The system shall have the capability to limit access to data via role-based security.	Release 1A; Must

5.2.2.14	**Storage - Allocation**	
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 1A; Must
5.2.2.14.2	The system shall have capability to have conditional thresholds customized to allow automated reallocation of storage to meet application needs.	Release 1A; Must
5.2.2.14.3	The system shall be able to allocate any compliant serial drive, and near-line storage devices.	Release 1A; Must
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 1A; Must
5.2.2.14.5	The system shall be able to immediately allocate newly added storage assets.	Release 1A; Must

3.2.5.3.2	**Requirements for Security**	
5.3.2.1	**Security - System User Authentication**	
5.3.2.1.1	The system shall have the capability to authenticate users based on a unique user identity.	Release 1A; Must
5.3.2.1.1.1	The system shall authenticate system and security administrators.	Release 1A; Must
5.3.2.1.1.1.1	The system shall support user ID and password authentication.	Release 1A; Must
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 1A; Must
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 1A; Must

5.3.2.1.2	The system shall permit users to create a unique user identity for access to the system.	Release 1A; Must
5.3.2.1.2.1	The system shall enforce uniqueness of user identity. No two users shall be allowed to use the exact same user identity.	Release 1A; Must
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 1A; Must
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 1A; Must
5.3.2.1.2.3	A user shall only be allowed to manage attributes associated with their own user identity.	Release 1A; Must
5.3.2.1.3	The system shall display a message to users if they fail to authenticate.	Release 1A; Must
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 1A; Must
5.3.2.1.5	The system shall verify the identity and authority of the Content Originator.	Release 1A; Must

5.3.2.2	**Security - User Access Control**	
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 1A; Must
5.3.2.2.1.1	The system shall permit authorized system administrators to create and assign customized roles.	Release 1A; Must
5.3.2.2.1.1.1	The system shall provide access control limitations to support data mining .	Release 1C; Must.
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 1A; Must
5.3.2.2.1.3	The system shall allow the use of standards based LDAP technology for the role based access model.	Release 1A; Must
5.3.2.2.2	The system shall manage user accounts.	Release 1A; Must
5.3.2.2.3	The system shall provide the capability to create user accounts.	Release 1A; Must
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 1A; Must
5.3.2.2.4	The system shall provide the capability to access user accounts.	Release 1A; Must
5.3.2.2.5	The system shall provide the capability to delete user accounts.	Release 1A; Must
5.3.2.2.6	The system shall provide the capability to suspend user accounts.	Release 1A; Must
5.3.2.2.7	The system shall provide the capability to reactivate suspended user accounts.	Release 1A; Must
5.3.2.2.8	The system shall provide the capability for the renewal of user registrations.	Release 1A; Must
5.3.2.2.9	The system shall have the capability to expire user accounts.	Release 1A; Must
5.3.2.2.10	The system shall provide the capability for users to cancel their accounts.	Release 1A; Must
5.3.2.2.11	The system shall provide the capability for users to update their account information.	Release 1A; Must
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 1A; Must
5.3.2.2.13	The system shall securely store personal information (e.g. user names and passwords).	Release 1A; Must
5.3.2.2.14	The system shall provide the capability for authorized users to manage (add, modify, delete) information.	Release 1A; Must

5.3.2.2.15	The system shall have the capability to provide secure interfaces for FDsys operations.	Release 1A; Must

5.3.2.3	**Security - Capture and Analysis of Audit Logs**	
5.3.2.3.1	The system shall keep an audit log of all transactions in the system.	Release 1A; Must
5.3.2.3.1.1	Audit logs shall contain logged events which each contain:	Release 1A; Must
5.3.2.3.1.2	Audit logs shall contain a description of the event containing the following:	Release 1A; Must
5.3.2.3.1.3	Audit logs shall contain additional data fields where binary data can be displayed in bytes or words.	Release 1A; Must
5.3.2.3.1.4	The system shall maintain a system log containing events logged by the system components.	Release 1A; Must
5.3.2.3.1.4.1	The system shall allow system logs to be viewed by all authorized users.	Release 1A; Must
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 1A; Must
5.3.2.3.1.5.1	The system shall allow security logs to be viewed by all authorized users.	Release 1A; Must
5.3.2.3.1.6	The system shall maintain an application log containing events logged by applications.	Release 1A; Must
5.3.2.3.1.6.1	The system shall allow applications logs to be viewed by all authorized users.	Release 1A; Must
5.3.2.3.1.7	The system shall have an Audit Log manager for system administrator functions.	Release 1A; Must
5.3.2.3.1.7.1	The Audit Log manager must be searchable.	Release 1A; Must
5.3.2.3.1.8	The system shall have the capability to reconstruct complete transactions.	Release 1A; Must
5.3.2.3.1.9	The system shall keep an audit log of user ordering (request) transactions.	Release 1A; Must
5.3.2.3.1.10	The system shall keep an audit log of system administration transactions.	Release 1A; Must
5.3.2.3.1.11	The system shall keep an audit log of security administrator transactions.	Release 1A; Must
5.3.2.3.1.12	The system shall keep an audit log of system access rights.	Release 1A; Must
5.3.2.3.1.13	The system shall keep an audit log of preservation processes.	Release 1C; Must
5.3.2.3.1.14	The system shall keep an audit log of deposited, harvested and converted content activities.	Release 1A; Must
5.3.2.3.1.15	The system shall keep an audit log of Content Originator ordering activities.	Release 1C; Must
5.3.2.3.1.16	The system shall keep an audit log of content authentication activities.	Release 1A; Must
5.3.2.3.1.17	The system shall keep an audit log of version control activities.	Release 1A; Must
5.3.2.3.1.18	The system shall keep an audit log of cataloging activities.	Release 1A; Must
5.3.2.3.1.19	The system shall keep an audit log of support activities (e.g., support status).	Release 1A; Must
5.3.2.3.1.20	The system shall keep an audit log for data mining.	Release 1C; Must
5.3.2.3.2	The system shall have the capability to maintain integrity of audit logs.	Release 1A; Must
5.3.2.3.2.1	It shall not be possible for users to adjust the data in the audit logs.	Release 1A; Must
5.3.2.3.2.2	The system shall detect user attempts to edit audit logs.	Release 1A; Must
5.3.2.3.3	The system shall keep an audit log of attempts to access the system.	Release 1A; Must
5.3.2.3.3.1	The system shall keep an audit log of any detected breaches of security policy.	Release 1A; Must
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 1A; Must

5.3.2.3.4.1	The system shall save audit logs as specified in GPO Publication 825.33.	Release 1A; Must

5.3.2.4	**Security - User Privacy**	
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 1B; Must
5.3.2.4.1.1	The system shall conform to guidelines set forth in GPO Publication 825.33.	Release 1B; Must
5.3.2.4.1.2	The system shall support compliance outlined in Title 5 USC Sec. 552a (Records maintained on individuals).	Release 1B; Must
5.3.2.4.1.3	The system shall support the capability of maintaining access privacy (e.g., Search, Request).	Release 1B; Must
5.3.2.4.1.4	The system shall support the capability of maintaining support privacy (e.g., user identity).	Release 1B; Must
5.3.2.4.1.5	The system shall support the capability of maintaining Content Originator ordering privacy.	Release 1B; Must
5.3.2.4.1.6	The system shall provide measures that preclude a single authorized administrator from listing a user's orders.	Release 1B; Must

5.3.2.5	**Security - Confidentiality**	
5.3.2.5.1	The system shall support the capability of maintaining confidentiality of user data (e.g., passwords).	Release 1A; Must
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 1A; Must
5.3.2.5.1.1.1	FIPS certified encryption algorithms shall be used to provide confidentiality. Triple DES or AES shall be supported.	Release 1A; Must
5.3.2.5.1.1.2	For symmetric encryption, 128 bit keys are the minimum key length to be used.	Release 1A; Must
5.3.2.5.1.2	The system shall have the capability to provide confidentiality of user data, including user authentication data stored within the system (e.g., passwords).	Release 1A; Must
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 1A; Must
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 1A; Must

5.3.2.6	**Security Administration**	
5.3.2.6.1	The system shall provide an administrative graphical user interface to perform user administration and security administration.	Release 1A; Must
5.3.2.6.2	The system shall have the capability for authorized security administrators to set and maintain system security policy.	Release 1A; Must
5.3.2.6.2.1	System security policy parameters shall include, but not be limited to the following:	Release 1A; Must
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 1A; Must
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 1A; Must
5.3.2.6.4.1	The system shall provide the capability to support separation of functions between system administrators, policy makers, security administrators and auditors.	Release 1A; Must

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 1A; Must
5.3.2.6.4.3	The system shall provide the capability to limit security administrator’s authority to assigned logical elements.	Release 1A; Must

5.3.2.7	**Security - Availability**	
5.3.2.7.1	The system shall provide appropriate backup and redundant components to ensure availability to meet customer and GPO needs.	Release 1A; Must
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 1A; Must
5.3.2.7.1.1.1	The system shall return to normal operations post-disaster.	Release 1A; Must
5.3.2.7.1.2	The system shall adhere to GPO’s Continuity of Operations (COOP) plans.	Release 1A; Must
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 1A; Must
5.3.2.7.1.2.2	The system shall adhere to guidelines set forth in Federal Preparedness Circular 65.	Release 1A; Must
5.3.2.7.1.3	The system shall have appropriate failover components.	Release 1A; Must
5.3.2.7.1.4	The system shall be operational at appropriate GPO alternate facilities.	Release 1A; Must
5.3.2.7.1.5	The system shall back up system and data at a frequency as determined by business requirements.	Release 1A; Must
5.3.2.7.1.5.1	The system applications and data shall be backed up at off-site storage location.	Release 1A; Must
5.3.2.7.1.6	The system shall interface with designated GPO Service Providers (e.g., Oracle).	Release 1A; Must
5.3.2.7.1.7	The system shall maintain data integrity during backup processing.	Release 1A; Must
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 1A; Must
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 1A; Must
5.3.2.7.1.9.1	Mutually authenticated, high speed connection between GPO offices and hosting site shall be utilized.	Release 1A; Must
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 1A; Must

5.3.2.8	**Security - Integrity**	
5.3.2.8.1	The system shall have the capability to assure integrity of business process information (BPI).	Release 1A; Must
5.3.2.8.2	The system shall check content for malicious code (e.g., worms and viruses) prior to ingest to maintain system integrity.	Release 1A; Must
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 1A; Must

5.3.2.9	**Security Standards**	
5.3.2.9.1	The system must have the capability to support the following industry integrity standards.	Release 1A; Must
5.3.2.9.2	The system must have the capability to support the following confidentiality standards.	Release 1A; Must
5.3.2.9.3	The system must have the capability to support the following access control standards.	Release 1A; Must

3.2.5.4.2	Requirements for Enterprise Service Bus	
5.4.2.1	**ESB Core Capabilities**	
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 1A; Must
5.4.2.1.1.1	The supported operating systems shall include: Microsoft Windows Server 2003 and higher versions, Linux (Red Hat Enterprise Advanced Server 2.1 and above), Solaris 9 and above, Apple OS X.2 and above.	Release 1A; Must
5.4.2.1.1.2	The supported programming languages shall include: C/C++, J2EE, .NET in C#. PERL, Python.	Release 1A; Must
5.4.2.1.2	The system shall provide the capability to integrate internal and external services or applications.	Release 1A; Must
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 1A; Must
5.4.2.1.4	The system shall provide the capability to integrate existing (or legacy) services or applications.	Release 1A; Must
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 1A; Must
5.4.2.1.6	The system shall provide the capability to support synchronous and asynchronous communications between services or applications.	Release 1A; Must
5.4.2.1.6.1	The system shall provide the capability to queue communications between services and applications.	Release 1A; Must
5.4.2.1.7	The system shall provide the capability to run process transactions.	Release 1A; Must
5.4.2.1.7.1	The system shall provide the capability to manage process transactions declaratively via system configurations.	Release 1A; Must
5.4.2.1.7.2	The system shall provide the capability to execute pre-defined process transactions.	Release 1A; Must
5.4.2.1.7.3	The system shall provide the capability to manually commit and roll back process transactions.	Release 1A; Must
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 1A; Must
5.4.2.1.8.1	The system shall provide the capability to validate communications against the appropriate published schema.	Release 1A; Must
5.4.2.1.8.2	The system shall provide the capability to transform communications to different published schemas.	Release 1A; Must
5.4.2.1.9	The system shall provide the capability to perform XML document-based routing between services or applications.	Release 1A; Must
5.4.2.1.10	The system shall provide the capability to support incremental implementations.	Release 1A; Must
5.4.2.1.11	The system shall provide the capability to support exception handling.	Release 1A; Must
5.4.2.1.11.1	The system shall provide the capability to generate compensating transactions for exceptions where possible.	Release 1B; Should
5.4.2.1.12	The system shall store information related to the ESB in metadata.	Release 1A; Must
5.4.2.1.12.1	The system shall store information about schemas in metadata.	Release 1A; Must
5.4.2.1.12.2	The system shall store information about transactional operations in metadata.	Release 1A; Must
5.4.2.1.12.3	The system shall store information about communications in metadata.	Release 1A; Must
5.4.2.1.12.4	The system shall store information about business processes in metadata.	Release 1A; Must

5.4.2.2	**ESB Configuration**	
5.4.2.2.1	The system shall provide the capability to perform integration configurations.	Release 1A; Must
5.4.2.2.1.1	The system shall provide the capability to perform integration configurations in XML.	Release 1A; Must
5.4.2.2.2	The system shall provide the capability to add redundancy to critical ESB functions.	Release 1A; Must

5.4.2.3	**ESB Administration**	
5.4.2.3.1	The system shall provide the capability to impose rule-based security control over administrative tasks.	Release 1A; Must
5.4.2.3.2	The system shall provide the capability to manage services or applications dynamically.	Release 1A; Must
5.4.2.3.3	The system shall provide the capability to enable and disable services dynamically.	Release 1A; Must
5.4.2.3.4	The system shall provide the capability to manage business processes.	Release 1A; Must
5.4.2.3.5	The system shall provide the capability to terminate, suspend and resume business processes.	Release 1A; Must
5.4.2.3.6	The system shall provide the capability to monitor ESB processes.	Release 1A; Must
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 1A; Must
5.4.2.3.6.2	The system shall provide the capability to monitor communication latencies.	Release 1A; Must
5.4.2.3.6.3	The system shall provide the capability to send notifications in the event of problems with ESB functions.	Release 1A; Must

5.4.2.4	**ESB Interface**	
5.4.2.4.1	The system shall provide the capability to perform configuration tasks via a Graphical User Interface (GUI) tool.	Release 1A; Must
5.4.2.4.2	The system shall provide the capability to perform administrative tasks via a GUI tool.	Release 1A; Must

3.2.5.5.2	**Requirements for Data Mining**	
5.5.2.1	**Data Mining - Data Extraction**	
5.5.2.1.1	The system shall be capable of extracting data from the entire collection of BPI.	Release 1C; Must
5.5.2.1.2	The system shall be capable of extracting data from the entire collection of metadata.	Release 1C; Must
5.5.2.1.3	The system shall be capable of extracting data from select GPO data sources (e.g., Oracle).	Release 1C; Must
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
5.5.2.1.5	The system shall be able to extract data according to user parameters (e.g., date range, action type).	Release 1C; Must
5.5.2.1.6	The system shall be able to extract random samples of data.	Release 1C; Could / Release 2; Must
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
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
5.5.2.1.7.2	The system shall allow users to enter data.	Release 1C; Should / Release 2; Must

5.5.2.1.7.3	The system shall allow users to restrict access to supplemental data.	Release 1C; Should / Release 2; Must
5.5.2.1.7.4	The system shall allow users to store supplemental data for future use.	Release 1C; Should / Release 2; Must
5.5.2.1.8	The system shall be capable of extracting data from multiple formats (e.g., XML, PDF, XLS).	Release 1C; Must
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

5.5.2.2	**Data Mining - Data Normalization**	
5.5.2.2.1	The system shall be able to normalize data based on administrator defined parameters, including but not limited to:	Release 1C; Must
5.5.2.2.1.1	The system shall be able to identify missing values or metadata elements.	Release 1C; Must
5.5.2.2.1.2	The system shall be able to identify data anomalies in BPI and metadata.	Release 1C; Must
5.5.2.2.1.3	The system shall be able to identify data formats.	Release 1C; Must
5.5.2.2.1.4	The system shall be able to identify format discrepancies.	Release 1C; Must
5.5.2.2.1.5	The system shall be able to identify standard data elements.	Release 1C; Must
5.5.2.2.1.6	The system shall be able to identify data types.	Release 1C; Must
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 1C; Must

5.5.2.3	**Data Mining - Data Analysis and Modeling**	
5.5.2.3.1	The system shall be able to perform single variable and multivariable analysis operations on extracted data.	Release 1C; Must
5.5.2.3.1.1	The system shall be able to calculate averages (mean, median, mode).	Release 1C; Must
5.5.2.3.1.2	The system shall be able to perform cross tabulations.	Release 1C; Could / Release 2; Must
5.5.2.3.1.3	The system shall be able to perform clusterization.	Release 1C; Could/ Release 2; Must
5.5.2.3.1.4	The system shall be able to perform categorization.	Release 1C; Could/ Release 2; Must
5.5.2.3.1.5	The system shall be able to perform association and link analyses.	Release 1C; Could/ Release 2; Must
5.5.2.3.1.6	The system shall be able to perform regression analysis.	Release 1C; Could / Release 2; Must
5.5.2.3.1.7	The system shall be able to expose hierarchical or parent/child relationships.	Release 1C; Could/ Release 2; Must
5.5.2.3.1.8	The system shall be able to expose sequential relationships and patterns.	Release 1C; Could/ Release 2; Must
5.5.2.3.1.9	The system shall be able to expose temporal relationships and patterns.	Release 1C; Could/ Release 2; Must
5.5.2.3.1.10	The system shall be able to expose inferences and rules that led to a result set.	Release 1C; Could/ Release 2; Must
5.5.2.3.2	The system shall be able to prompt users attempting illogical operations (e.g., calculating averages out of categorical data).	Release 1C; Could
5.5.2.3.2.1	The system shall be capable of showing the user the rule violation that led to the prompt of the operation.	Release 1C; Could
5.5.2.3.3	The system shall allow users to suspend, resume, or restart analysis	Release 1C; Should / Release 2; Must
5.5.2.3.4	The system shall be capable of providing the user with an estimated analysis time.	Release 1C; Could

5.5.2.4	**Data Mining - Report Creation and Data Presentation**	
5.5.2.4.1	The system shall be able to produce reports summarizing the analysis of BPI and metadata.	Release 1C; Must
5.5.2.4.1.1	The system must allow users to choose from the data types available in BPI and metadata and choose operations performed on that data.	Release 1C; Must
5.5.2.4.1.2	The system must be able to produce a report summarizing system usage for a user-defined time range.	Release 1C; Must
5.5.2.4.1.3	The system must be able to produce a report analyzing the usage of search terms.	Release 1C; Must
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
5.5.2.4.3	The system shall allow a set of default report templates to be accessible for each user class.	Release 1C; Must
5.5.2.4.3.1	The system shall allow System Administrators to manage the default templates.	Release 1C; Must
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
5.5.2.4.5	The system shall be capable of real-time population of report templates.	Release 1C; Should / Release 2; Must
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
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
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
5.5.2.4.7	The system shall be capable of delivering reports to users.	Release 1C; Could / Release 2; Must
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
5.5.2.4.8	The system shall be capable of supporting real-time reporting.	Release 1C; Should / Release 2; Must
5.5.2.4.9	The system shall allow users to create alerts or notifications based on real-time analysis of BPI or metadata.	Release 1C; Should / Release 2; Must
5.5.2.4.10	The system shall be able to link analysis results to data.	Release 1C; Could
5.5.2.4.11	The system shall be able to expose analysis criteria and algorithms.	Release 1C; Could
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 1C; Must
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 1C; Must

5.5.2.5	**Data Mining - Security and Administration**	
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 1A; Must
5.5.2.5.2	The system shall log all user interactions with the system in metadata.	Release 1A; Must
5.5.2.5.2.1	Whenever possible, each log entry shall include at least the user identification, user class, date, time, action, and referring page, subject to GPO privacy rules.	Release 1A; Must
5.5.2.5.3	The system shall log all processes in metadata.	Release 1A; Must
5.5.2.5.4	The system shall perform records management functions on logs.	Release 1A; Must

5.5.2.6	**Data Mining - Storage**	

5.5.2.6.1	The system shall store extracted data.	Release 1C; Must
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 1C; Must
5.5.2.6.2	The system shall store metadata, supplemental data, reports, report templates, analysis criteria, and algorithms in Business Process Storage.	Release 1A; Must
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 1A; Must

3.2.6.1	Requirements for Content Submission	
6.1.1	**Content Submission Core Capabilities**	
6.1.1.1	The system shall accept digital content and metadata.	Release 1A; Must
6.1.1.2	The system shall create a SIP from content and metadata.	Release 1A; Must

6.1.2	**Content Submission - System Administration**	
6.1.2.1	The system shall have the capability to accept and process encrypted files.	Release 2; Could
6.1.2.2	The system shall provide notification to the submission agency/authority that the content has been received.	Release 1A; Must
6.1.2.3	The system shall provide notification to the submission agency/authority that the content has been released.	Release 1A; Could / Release 1B; Must
6.1.2.4	The system shall identify files with security restrictions upon submission.	Release 1A; Must
6.1.2.4.1	Information about the files will be recorded in metadata.	Release 1A; Must
6.1.2.5	The system shall identify content that has copyright limitations.	Release 1A; Must
6.1.2.5.1	Copyright information will be recorded in metadata.	Release 1A; Must
6.1.2.6	The system shall provide WIP storage for content prior to ingest.	Release 1A; Must
6.1.2.7	The system shall check content prior to ingest.	Release 1A; Must
6.1.2.7.1	Content must be checked for malicious code (e.g., viruses).	Release 1A; Must
6.1.2.7.1.1	In case of a virus or other malicious code, content will follow processes as described in the FDsys security requirements.	Release 1A; Must
6.1.2.7.2	Zipped files (.zip) shall be unzipped.	Release 1A; Must
6.1.2.7.3	Stuffed files (.sit) shall be unstuffed.	Release 1A; Must
6.1.2.8	The system shall accept content with specialized character sets (e.g., non-Roman, scientific notations).	Release 1A; Must

6.1.3	**Content Submission Metadata**	
6.1.3.1	The system shall accept all administrative and descriptive metadata supplied by the submission agency/authority.	Release 1A; Must
6.1.3.1.1	The system shall provide the capability to record Title or caption of content.	Release 1A; Must
6.1.3.1.2	The system shall provide the capability to record content identifiers assigned to content including but not limited to:	Release 1A; Must
6.1.3.1.3	The system shall provide the capability to record Author/Creator of the content.	Release 1A; Must
6.1.3.1.4	The system shall provide the capability to record Publisher/Authority of the content.	Release 1A; Must
6.1.3.1.5	The system shall provide the capability to record Rights Owner of the content.	Release 1A; Must
6.1.3.1.6	The system shall provide the capability to record version information of the content.	Release 1A; Must
6.1.3.1.7	The system shall provide the capability to record relationships between content packages and digital objects.	Release 1A; Must

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 1A; Must
6.1.3.1.8	The system shall provide the capability to record content description information (e.g., abstract, summary).	Release 1A; Must
6.1.3.1.9	The system shall provide the capability to record Structure Information of the content.	Release 1A; Must
6.1.3.1.10	The system shall provide the capability to record Intended Output of the content.	Release 1A; Must
6.1.3.1.11	The system shall provide the capability to record Intended Audience of the content.	Release 1A; Must
6.1.3.1.12	The system shall provide the capability to record 13 Digit ISBN Numbers to content.	Release 1A; Must
6.1.3.2	The system shall accept and capture the following elements when available and applicable.	Release 1A; Must
6.1.3.2.1	Elements relating to documents including but limited to:	Release 1A; Must
6.1.3.2.2	Elements relating to audio including but limited to:	Release 1A; Must
6.1.3.2.3	Elements relating to video including but limited to:	Release 1A; Must
6.1.3.2.4	Elements relating to other formats to be determined	Release 1A; Must

3.2.6.2.2	**Requirements for Deposited Content**	
6.2.2.1	**Deposited Content Core Capabilities**	
6.2.2.1.1	The system shall accept digital content and metadata provided by Content Originators.	Release 1A; Must
6.2.2.1.2	The system shall have the capability to inform Content Evaluators that new content has been submitted.	Release 1A; Must

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

6.2.2.3	**Deposited Content Interfaces**	
6.2.2.3.1	Deposited content interface shall enable Congressional Content Originators and Agency Content Originators to:	multiple releases
6.2.2.3.1.1	Submit digital content and metadata	Release 1A; Must
6.2.2.3.1.2	Submit content chain of custody information to the system	Release 1A; Must
6.2.2.3.1.3	Submit intended use information to the system	Release 1A; Must
6.2.2.3.1.4	Submit “approved for release” information	Release 1A; Must
6.2.2.3.1.5	Receive notification of receipt of content and content ID	Release 1A; Must
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 1A; Must
6.2.2.3.1.7	Receive notification of release of content	Release 1B; Must
6.2.2.3.1.8	Support Content Originator ordering	Release 1C; Must
6.2.2.3.2	Deposited content interface shall enable GPO Service Providers and external Service Providers to:	multiple releases
6.2.2.3.2.1	Submit digital content and metadata	Release 1A; Must
6.2.2.3.2.2	Receive notification of receipt of content and content ID	Release 1A; Must
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 1A; Must
6.2.2.3.2.4	Support Content Originator ordering	Release 1C; Must

3.2.6.3.2	**Requirements for Converted Content**	

6.3.2.1	**Converted Content Core Capabilities**	
6.3.2.1.1	The system shall accept digital content and metadata provided by converted content processes.	Release 1A; Must
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 1A; Must

6.3.2.2	**Converted Content Interfaces**	
6.3.2.2.1	Converted content interface shall enable GPO Service Providers and external Service Providers to:	multiple releases
6.3.2.2.1.1	Submit approved content, metadata, and BPI	Release 1A; Must
6.3.2.2.1.2	Receive notification of receipt of content and content ID	Release 1A; Must
6.3.2.2.1.3	Provide notification of release of content	Release 1B; Must
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 1A; Must
6.3.2.2.1.5	Manage converted content	Release 1A; Must

3.2.6.4.2 Requirements for Harvested Content

6.4.2.1	**Harvested Content Core Capabilities**	
6.4.2.1.1	The system shall accept digital content and metadata delivered by the harvesting function.	Release 1A; Must

6.4.2.2	**Harvested Content Metadata**	
6.4.2.2.1	The system shall provide the capability to record the date and time of harvest of content.	Release 1A; Must

6.4.2.3	**Harvester Requirements**	
6.4.2.3.1	The harvester shall have the capability to discover, assess, and harvest in-scope content from targeted Web sites.	Release 1B; Must
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 1B; Could / Release 2; Must
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 1B; Could / Release 2; Must
6.4.2.3.4	The harvester shall have capability to perform simultaneous harvests.	Release 1B; Must
6.4.2.3.5	The harvester shall locate and harvest all levels of Web pages within a Web site.	Release 1B; Must
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 1B; Should / Release 2; Must
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 1B; Must
6.4.2.3.8	The harvester shall stop the discovery process when a linked Web page does not contain in-scope content.	Release 1B; Should / Release 2; Must
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 1B; Must
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 1B; Must
6.4.2.3.11	The harvester shall collect in-scope discovered content and available metadata.	Release 1B; Must
6.4.2.3.11.1	The harvester shall deliver all in-scope content and metadata to WIP storage.	Release 1B; Must

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 1B; Must
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 1B; Must
6.4.2.3.13	The harvester shall have the ability to maintain the directory structure of Web sites that constitute entire publications.	Release 1B; Must
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 1B; Must
6.4.2.3.15	The harvester must be able to harvest hidden Web information.	Release 1C; Could / Release 2; Must
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
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
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
6.4.2.3.15.4	The harvester must be able to harvest content contained on FTP servers.	Release 1C; Could / Release 2; Must
6.4.2.3.15.5	The harvester must be able to harvest content contained behind proxy servers.	Release 1C; Could / Release 2; Must
6.4.2.3.15.6	The harvester must be able to harvest content contained behind firewalls.	Release 1C; Could / Release 2; Must
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:	Release 1B; Must
6.4.2.3.17	The harvester shall have the capability to time and date stamp content that has been harvested.	Release 1B; Must

6.4.2.4	**Metadata Requirements for Harvester**	
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 1B; Must
6.4.2.4.2	The harvester shall have the ability to locate and collect unique ID and title/caption information.	Release 1B; Must
6.4.2.4.3	The harvester shall have the ability to locate and collect author/creator, publisher/authority, and rights owner information.	Release 1B; Must
6.4.2.4.4	The harvester shall have the ability to locate and collect topical information and bibliographic descriptions.	Release 1B; Must
6.4.2.4.5	The harvester shall have the ability to locate and collect version, fixity, relationship, and provenance information.	Release 1B; Must
6.4.2.4.6	The harvester shall have the ability to locate and collect technical, structural, file format, packaging and representation information.	Release 1B; Must
6.4.2.4.7	The harvester shall have the ability to locate and collect administrative metadata.	Release 1B; Must
6.4.2.4.8	The harvester shall have the capability to record the time and date of harvest.	Release 1B; Must

6.4.2.5	**Harvester Rules and Instructions**	
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 1B; Must

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 1B; Must
6.4.2.5.3	The harvester must be able to create and store rule and instruction profiles for individual targeted Web sites.	Release 1B; Could / Release 2; Must

6.4.2.6	**Harvester Interface**	
6.4.2.6.1	The harvester shall provide a user interface to accommodate workflow management and scheduling of harvesting activities.	Release 1B; Must
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 1B; Must
6.4.2.6.2.1	Must accommodate the scheduling of harvests, including but not limited to hourly, daily, weekly, biweekly, monthly, and yearly.	
6.4.2.6.3	The user interface must be able to manage rule and instruction profiles.	Release 1B; Could / Release 2; Must

6.4.2.7	**System Administration for Harvester**	
6.4.2.7.1	The harvester shall provide quality control functions to test accuracy/precision of rule application.	Release 1B; Could / Release 2; Must
6.4.2.7.2	The harvester shall be able to incorporate results of quality control functions into rule and instruction creation/refinement.	Release 1B; Could / Release 2; Must
6.4.2.7.3	The harvester shall have the capability to log and produce reports on harvesting activities.	Release 1B; Could / Release 2; Must
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 1B; Must
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 1B; Must
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 1B; Must
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 1B; Must
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 1B; Must
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 1B; Could / Release 2; Must
6.4.2.7.4	The discovery and harvesting tools shall have the ability to identify GPO as the owner of the tools.	Release 1B; Must
6.4.2.7.5	The harvester's method of identification shall not be intrusive to targeted Web site.	Release 1B; Must
6.4.2.7.6	The harvester shall have the ability to collect integrity marks associated with content as it is being harvested.	Release 1B; Must

3.2.6.5.2	**Requirements for Style Tools**	
6.5.2.1	**Style Tools Core Capabilities**	
6.5.2.1.1	Style tools shall accept content from authorized Content Originators, Service Providers, and Service Specialists for document creation.	Release 1C; Could / Release 3; Must
6.5.2.1.2	Style tools shall accept metadata from authorized users (e.g., title, author).	Release 1C; Could / Release 3; Must
6.5.2.1.3	Style tools shall provide the capability for users to create new content for document creation.	Release 1C; Could / Release 3; Must

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 1C; Could / Release 3; Must
6.5.2.1.4.1	Style tools shall allow users to compose content based on pre-defined design rules.	Release 1C; Could / Release 3; Must
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 1C; Could / Release 3; Must
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 1C; Could / Release 3; Must
6.5.2.1.5	Style tools shall allow multiple users to work collaboratively on the same content, prior to publication.	Release 1C; Could / Release 3; Must
6.5.2.1.5.1	Style tools shall allow authorized users to approve/reject content changes made by collaborators.	Release 1C; Could / Release 3; Must
6.5.2.1.5.1.1	Style tools shall track approval/rejection of changes to content, prior to publication.	Release 1C; Could / Release 3; Must
6.5.2.1.5.1.2	Style tools shall allow for approval of content.	Release 1C; Could / Release 3; Must
6.5.2.1.5.1.3	Style tools shall allow for approval of content presentation.	Release 1C; Could / Release 3; Must
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 1C; Could / Release 3; Must
6.5.2.1.7	Style tools shall provide the capability to track and undo changes to WIP content.	Release 1C; Could / Release 3; Must
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 1C; Could / Release 3; Must
6.5.2.1.9	Style tools shall interface with Content Originator ordering.	Release 1C; Could / Release 3; Must

6.5.2.2	**Style Tools - Automated Composition**	
6.5.2.2.1	Style tools shall have the capability to automatically compose content.	Release 2; Could / Release 3; Must
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
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
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
6.5.2.2.2	Style tools shall allow users to modify automatically composed content.	Release 2; Could / Release 3; Must

6.5.2.3	**Style Tools - System Administration**	
6.5.2.3.1	The system shall accept content based on the access rights and privileges of the user submitting the content.	Release 1C; Could / Release 3; Must
6.5.2.3.2	The system shall assign unique ID's to digital objects created by style tools.	Release 1C; Could / Release 3; Must
6.5.2.3.3	The system shall provide storage for WIP style tools content.	Release 1C; Could / Release 3; Must
6.5.2.3.3.1	The system shall allow management of WIP content based on access rights and privileges.	Release 1C; Could / Release 3; Must
6.5.2.3.3.2	The system shall provide tracking of all WIP activities.	Release 1C; Could / Release 3; Must
6.5.2.3.3.3	The system shall provide search and retrieval capabilities for WIP content.	Release 1C; Could / Release 3; Must

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 1C; Could / Release 3; Must

3.2.6.6.2	**Content Originator ordering Requirements**	
6.6.2.1	**Content Originator Ordering Core Capabilities**	
6.6.2.1.1	The system shall provide a user interface for Content Originator ordering.	Release 1C; Must
6.6.2.1.2	The system shall have the capability to process jobs prior to content being approved for publication prior to ingest.	Release 1C; Must
6.6.2.1.3	The system shall have the capability to process jobs prior to content being received.	Release 1C; Must
6.6.2.1.4	The system shall have the capability to track jobs using the unique ID requirements.	Release 1C; Must
6.6.2.1.5	The system shall have the capability to support a Content Originator specific tracking number and link to a unique ID.	Release 1C; Could / Release 2; Must
6.6.2.1.6	The system shall have the capability to be interoperable with external Content Originator ordering systems (e.g., Treasury Integrated Print Procurement System).	Release 1C; Could
6.6.2.1.7	The system shall adhere to policies set forth in GPO Publication 305.3.	Release 1C; Must

6.6.2.2	**Content Originator Ordering - Job Management**	
6.6.2.2.1	The system shall provide the capability to create, acquire, edit and store BPI data specific to ordering functions, preservation needs, version, and job specifications (e.g., SF1, 952, 2511, 3868, etc.).	Release 1C; Must
6.6.2.2.2	The system shall allow users to generate and submit jobs electronically.	Release 1C; Must
6.6.2.2.2.1	The system shall ensure users are authorized to submit jobs (e.g., are authorized to spend funds) based upon business rules.	Release 1C; Must
6.6.2.2.2.2	The system shall allow authorized users to approve content for publication.	Release 1C; Must
6.6.2.2.2.3	The system shall support credential technologies (e.g. PKI) per the FDsys security requirements.	Release 1C; Must
6.6.2.2.3	The system shall allow users to view and search similar job specifications.	Release 1C; Should / Release 2; Must
6.6.2.2.4	The system shall have the capability to identify similar jobs and specifications (e.g., strapping jobs) based upon business rules.	Release 1C; Should / Release 2; Must
6.6.2.2.4.1	The system shall notify Service Specialists of similar jobs and job specifications.	Release 1C; Should / Release 2; Must
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 1C; Must
6.6.2.2.6	The system shall provide the capability for Content Evaluators and Content Originators to ride jobs as defined by GPO business rules.	Release 1C; Must
6.6.2.2.7	The system shall provide the capability to notify Content Evaluators and Content Originators that riders have been placed.	Release 1C; Should / Release 2; Must
6.6.2.2.8	The system shall provide the capability to alert Content Evaluators and Content Originators that GPO is accepting riders for content as defined by GPO business rules.	Release 1C; Must
6.6.2.2.9	The system shall have the capability to determine contract types (e.g., one-time bids, SPA, term contract) based upon specification and business rules.	Release 1C; Could
6.6.2.2.10	The system shall allow users to request a contract type.	Release 1C; Should / Release 2; Must

6.6.2.2.11	The system shall allow users to view a history of all previous jobs based on user rights.	Release 1C; Should / Release 2; Must
6.6.2.2.12	The system shall provide estimated costs to authorized users for jobs based upon job specifications.	Release 1C; Should / Release 2; Must
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 solicitation release.	Release 1C; Must
6.6.2.2.14	The system shall have the capability to inform authorized users that a job specification has been edited..	Release 1C; Should / Release 2; Must
6.6.2.2.15	The system shall provide the capability for Content Originators to specify Content Delivery options (hard copy, electronic presentation, digital media) based upon the content submitted.	Release 1C; Must
6.6.2.2.16	The system shall allow users to select fulfillment options for content delivery.	Release 1C; Must
6.6.2.2.16.1	The system shall provide the capability to support multiple hard copy fulfillment options including, but not limited to: Customer pick-up, Ship, Deliver, Mail, Free on Board (FOB) Contractor City, Free on Board (FOB) Destination, and Government Bills of Lading.	Release 1C; Must
6.6.2.2.16.2	The system shall provide the capability to enter multiple shipping and fulfillment destinations.	Release 1C; Must
6.6.2.2.16.3	The system shall provide the capability for Content Originators to select ship, fulfillment, mail, or pickup dates.	Release 1C; Must
6.6.2.2.16.4	The system shall provide the capability for Content Originators and Service Providers to select shipping providers (e.g., Fed-Ex, UPS, USPS).	Release 1C; Must
6.6.2.2.16.5	The system shall have the capability to provide estimated fulfillment costs based upon job specifications.	Release 1C; Could
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 1C; Must
6.6.2.2.17	The system shall maintain Service Provider information.	Release 1C; Must
6.6.2.2.17.1	Authorized users shall have the capability to access Service Provider information.	Release 1C; Must
6.6.2.2.17.2	The system shall provide the capability for Service Providers and GPO users to manage Service Provider information.	Release 1C; Must
6.6.2.2.17.2.1	Service Provider contact information shall include, but not be limited to: Name of company, Physical address, Mailing address (if different), Fulfillment address (if different), Names of contact personnel, Phone number, Cell phone number, E-mail, Fax, State & Contractor code.	Release 1C; Must
6.6.2.2.17.2.2	The system shall provide the capability for multiple contact personnel for each Service Provider.	Release 1C; Must
6.6.2.2.17.3	The Service Provider shall be able to select equipment categories from a predefined list.	Release 1C; Could / Release 2; Must
6.6.2.2.17.3.1	Authorized GPO personnel shall be able to manage the predefined list of equipment categories.	Release 1C; Could / Release 2; Must
6.6.2.2.17.4	The Service Provider shall be able to select capabilities from a predefined list.	Release 1C; Must
6.6.2.2.17.4.1	Authorized GPO personnel shall be able to manage the predefined list of capabilities.	Release 1C; Must
6.6.2.2.17.4.2	The service provider shall be able to input customized capabilities not included on the predefined list.	Release 1C; Must
6.6.2.2.17.5	The Service Provider shall be able to manage preferences including, but not limited to:	Release 1C; Could / Release 2; Must
6.6.2.2.17.6	The system shall maintain Service Provider performance information.	Release 1C; Must
6.6.2.2.17.6.1	The system shall allow GPO users to manage Service Provider performance data.	Release 1C; Must

6.6.2.2.17.6.2	Quality levels shall be assigned by authorized GPO personnel in accordance with GPO Publication 310.1.	Release 1C; Must
6.6.2.2.17.6.3	Quality history data shall include, but not be limited to:	Release 1C; Must
6.6.2.2.17.6.4	Compliance history shall include, but not be limited to:	Release 1C; Must
6.6.2.2.17.6.5	Notices received shall include, but not be limited to:	Release 1C; Must
6.6.2.2.17.6.6	Notes	Release 1C; Must
6.6.2.2.18	The system shall provide the capability to search for Service Providers based on job specifications and Service Providers capabilities, location, and equipment.	Release 1C; Must
6.6.2.2.19	The system shall generate a list of Service Providers based upon job specifications and Service Providers capabilities, location, minimum acceptable quality level, and equipment.	Release 1C; Must
6.6.2.2.19.1	The system shall provide the capability for Content Originator and Service Specialists to select from approved Service Providers based upon GPO business rules and GPO procurement regulations.	Release 1C; Must
6.6.2.2.20	The system shall allow Service Specialists to generate and distribute solicitations (e.g., post online, send to specified Service Providers).	Release 1C; Must
6.6.2.2.21	The system shall accept bids from Service Providers.	Release 1C; Must
6.6.2.2.21.1	The system shall accept bids with multiple line items.	Release 1C; Must
6.6.2.2.21.2	The system shall accept fixed bids with an indefinite quantity.	Release 1C; Must
6.6.2.2.21.3	The system shall electronically stamp bids with time, date, and user data.	Release 1C; Must
6.6.2.2.21.4	The system shall allow Service Specialists to announce bid results electronically.	Release 1C; Must
6.6.2.2.22	The system shall allow Service Specialists and Content Originators to award jobs to Service Providers.	Release 1C; Must
6.6.2.2.22.1	The system shall have the capability to send content and order information to Service Providers after award.	Release 1C; Must
6.6.2.2.23	The system shall allow Service Providers to request contract modifications based upon business rules.	Release 1C; Should / Release 2; Must
6.6.2.2.24	The system shall allow Service Specialists to request, authorize, and manage contract modifications based upon business rules.	Release 1C; Should / Release 2; Must
6.6.2.2.25	The system shall allow Content Originators to request and authorize contract modifications based upon business rules.	Release 1C; Should / Release 2; Must
6.6.2.2.26	The system shall provide the capability for users to request re-orders.	Release 1C; Must

6.6.2.3	**Content Originator Ordering - Job Tracking**	
6.6.2.3.1	The system shall have the capability to log activities and communications with Content Originators, Service Providers, and Service Specialists including but not limited to: .	Release 1C; Must
6.6.2.3.1.1	The system shall provide a means to add notes to each job.	Release 1C; Must
6.6.2.3.2	The system shall provide the capability to contact Service Providers for job status (e.g., tracking of job).	Release 1C; Should / Release 2; Must
6.6.2.3.2.1	The system shall automatically contact Service Providers.	Release 1C; Should / Release 2; Must
6.6.2.3.2.2	The system shall have the capability for authorized users to request automated notifications for job activities.	Release 1C; Should / Release 2; Must
6.6.2.3.3	The system shall allow Service Specialists to generate and distribute notification to Service Providers and Content Originator (e.g., show cause, cure notice, 907, specification amendments).	Release 1C; Should / Release 2; Must
6.6.2.3.4	The system shall have the capability to provide notification of fulfillment to users.	Release 1C; Should / Release 2; Must

6.6.2.3.4.1	Notification of fulfillment shall include, but not be limited to:	Release 1C; Should / Release 2; Must
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 1C; Should / Release 2; Must
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 1C; Should / Release 2; Must
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 1C; Should / Release 2; Must
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 1C; Should / Release 2; Must
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 1C; Should / Release 2; Must
6.5.2.3.4.2.5	The system shall have the capability for users to elect not to receive notification of fulfillment.	Release 1C; Should / Release 2; Must
6.5.2.3.4.2.6	The system shall allow authorized users to manage fulfillment notification.	Release 1C; Should / Release 2; Must
6.6.2.3.5	The system shall have the capability to provide users with confirmation of fulfillment.	Release 1C; Should / Release 2; Must
6.6.2.3.5.1	The system shall have the capability to receive and store product fulfillment tracking numbers (e.g., Fed-Ex Tracking Number) from Service Providers.	Release 1C; Should / Release 2; Must
6.5.2.3.5.1.1	The system shall have the capability to store multiple tracking numbers for each order.	Release 1C; Should / Release 2; Must
6.5.2.3.5.1.2	The system shall provide a hyperlink to a fulfillment provider tracking website.	Release 1C; Should / Release 2; Must
6.6.2.3.5.2	The system shall have the capability to receive confirmation of fulfillment from the agency or end user.	Release 1C; Should / Release 2; Must
6.5.2.3.5.2.1	The system shall have the capability to receive multiple confirmations of fulfillment.	Release 1C; Should / Release 2; Must
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	
7.2.1	**Access Core Capabilities**	
7.2.1.1	The system must provide open and interoperable access to content.	Release 1B; Must
7.2.1.2	The system must provide open and interoperable access to metadata.	Release 1B; Must
7.2.1.3	The system must provide access to content at the minimum level of granularity that is specified in the FDsys unique ID requirements.	Release 1B; Must
7.2.1.4	The system shall provide the capability for End Users to use persistent names to access content.	Release 1B; Must
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 1B; Must
7.2.1.6	The system must provide the capability for users to access information about relationships between content packages, between digital objects, and between digital objects and content packages.	Release 1B; Must
7.2.1.7	The system must provide the capability to use GPO's ILS to access metadata repositories not resident within the system.	Release 1B; Must
7.2.1.8	The system must provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including the following.	Release 1B; Must

7.2.2	**Access to Content Packages**	

7.2.2.1	The system must provide the capability for GPO to manage access to content packages according to GPO business rules.	Release 1A; Must
7.2.2.2	The system must accept access rules for content packages.	Release 1A; Must
7.2.2.3	The system must provide the capability to limit access to content with re-dissemination restrictions as specified by the Content Originator.	Release 1B; Must
7.2.2.4	The system must provide the capability to limit access to content with limited distribution as specified by the Content Originator.	Release 1B; Must
7.2.2.5	The system must provide the capability to limit access to classified content as specified by the Content Originator.	Release 1B; Must
7.2.2.6	The system must provide the capability to limit access to copyrighted content as specified by the Content Originator.	Release 1B; Must
7.2.2.7	The system must provide the capability to limit access to content that is out of scope for GPO’s dissemination programs.	Release 1B; Must
7.2.2.8	The system must provide the capability to limit access to content that has not been approved by the Content Originator for public release.	Release 1B; Must
7.2.2.9	The system must provide the capability to limit access to embargoed content until the appropriate release data and time as specified by the Content Originator.	Release 1B; Must
7.2.2.10	The system must provide the capability to limit access to content based on criteria specified by the Content Originator.	Release 1B; Must
7.2.2.11	The system must provide access to content currently available on GPO Access.	Release 1B; Must
7.2.2.12	The system must provide the capability to notify users of limitations on access to content.	Release 1B; Must
7.2.2.13	The system shall provide the capability to provide customized access to content packages.	Release 1C; Should / Release 2; Must
7.2.2.14	The system shall provide the capability to provide personalized access to content packages.	Release 1C; Could / Release 2; Must
7.2.2.15	The system must provide the capability for users to access in scope final published versions of ACPs.	Release 1C; Could / Release 2; Must
7.2.2.16	The system must provide the capability for authorized users to access final approved versions of ACPs that are not in scope for GPO’s dissemination programs.	Release 1B; Must

7.2.3	**Access to the System**	
7.2.3.1	The system must have the capability to provide access to system functions by user class.	Release 1A; Must
7.2.3.2	The system must provide access to public End Users that does not require them to log-in or register with the system.	Release 1B; Must
7.2.3.3	The system must provide the capability for authorized Content Originators, Service Providers, Service Specialists, and Content Evaluators to access WIP storage.	Release 1A; Must
7.2.3.3.1	The system shall have the capability to allow Content Originators to authorize access to content in WIP.	Release 1A; Must
7.2.3.3.2	The system must provide “check in and check out” capabilities for content in WIP.	Release 1C; Could / Release 2; Must
7.2.3.4	The system shall provide the capability to provide customized access to the system.	Release 1C; Should / Release 2; Must
7.2.3.5	The system shall provide the capability to provide personalized access to the system.	Release 1C; Could / Release 2; Must

7.2.4	**Access - User Registration**	
7.2.4.1	The system must provide the capability for users to register with the system.	Release 1A; Must

7.2.4.2	The system must provide the capability to establish a user account for each registered user.	Release 1A; Must
7.2.4.3	The system must provide the capability to create user records for registered users.	Release 1A; Must
7.2.4.4	The system must have capability to store and manage an unlimited number of user records.	Release 1A; Must
7.2.4.5	The system must provide the capability for authorized users to access user records.	Release 1A; Must
7.2.4.6	The system must provide the capability for GPO System Administrators to set required fields in user records.	Release 1A; Must
7.2.4.7	The system must provide the capability to record information submitted by users during registration with system.	Release 1A; Must
7.2.4.8	The system must provide the capability to for GPO to customize what information is collected during user registration.	Release 1A; Must
7.2.4.8.1	The system must have the capability to collect name from the user during registration (e.g., honorific title, first name, last name, job title).	Release 1A; Must
7.2.4.8.2	The system must 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 1A; Must
7.2.4.8.3	The system shall provide the capability to collect security clearance information from the user during registration.	Release 1A; Must
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 1A; Must
7.2.4.8.4.1	Users may be members of multiple user classes simultaneously.	Release 1A; Must
7.2.4.8.4.2	The system shall associate registered users with at least one user class.	Release 1A; Must
7.2.4.8.5	The system shall provide the capability to collect role-based information from the user during registration.	Release 1A; Must
7.2.4.8.6	The system shall provide the capability to collect proof of identity information from the user during registration.	Release 1A; Must
7.2.4.8.7	The system shall provide the capability to collect authority to publish information from the user during registration.	Release 1A; Must
7.2.4.9	The system shall provide the capability to perform records management functions on user records.	Release 1B; Must

7.2.5	**Access - User Preferences**	
7.2.5.1	The system must provide the capability for authorized users to manage user preferences including but not limited to the following:	Release 1C; Should / Release 2; Must
7.2.5.2	The system must provide the capability for authorized users to manage other users' preferences.	Release 1C; Should / Release 2; Must
7.2.5.3	The system must provide the capability for GPO to establish and manage default user preferences.	Release 1C; Should / Release 2; Must
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
7.2.5.5	The system shall provide the capability to provide customized user preferences.	Release 1C; Should / Release 2; Must
7.2.5.6	The system shall provide the capability to provide personalized user preferences.	Release 1C; Could / Release 2; Must

7.2.6	**Access Processing**	
7.2.6.1	The system must provide the capability to process and manage ACPs.	Release 1B; Must

7.2.6.1.1	The system must provide the capability to process and manage digital objects that are used for access.	Release 1B; Must
7.2.6.1.2	The system must provide the capability to manage metadata that are used for access.	Release 1B; Must
7.2.6.2	The system must provide the capability to create access derivatives.	Release 1B; Must
7.2.6.3	The system must provide the capability to apply cataloging and reference tools processes.	Release 1B; Must
7.2.6.4	The system must provide the capability to assign persistent names.	Release 1B; Must
7.2.6.5	The system must provide the capability for access processing to request that an ACP be modified or created from an AIP.	Release 1B; Must
7.2.6.6	The system shall provide the capability for access processing to provide content, metadata, business process information, and other metadata as necessary to delivery processing for the purpose of fulfilling an End User request or Content Originator order.	Release 1B; Must
7.2.6.7	The system must provide the capability to perform records management functions on ACPs.	Release 1B; Must
7.2.6.7.1	Records management functions must comply with GPO and Federal records management policies.	Release 1B; Must
7.2.6.7.2	Records management functions must be performed according to records management schedules for content and metadata within the system.	Release 1B; Must
7.2.6.8	The system must provide the capability to identify and manage relationships between digital objects, between content packages, and between digital objects and content packages, including, but not limited to the following:	Release 1A; Must

3.2.7.3.2	Requirements for Accessibility	
7.3.2.1	**Accessibility Core Capabilities**	
7.3.2.1.1	The system must provide the capability to assess content for compliance with Section 508 technical standards.	Release 1B; Must
7.3.2.1.2	The system must provide the capability to create content that is compliant with Section 508 technical standards.	Release 1B; Must
7.3.2.1.3	The system must provide the capability to validate content for compliance with Section 508 technical standards.	Release 1B; Must
7.3.2.1.4	The system must accept accessibility requirements and implementation guidance from Content Originators.	Release 1A; Must
7.3.2.1.5	The system must provide Section 508 compliant access to the system.	Release 1A; Must
7.3.2.1.6	In order to achieve compliance with Section 508 technical standards, established best practices should be followed.	Release 1B; Could
7.3.2.1.7	The system must create content that contain well formed code which conforms to World Wide Web Consortium (W3C) Guidelines.	Release 1B; Must

7.3.2.2	**Accessibility - Section 508 Technical Standards**	
7.3.2.2.1	FDsys software applications and operating systems shall be Section 508 compliant according to 36 CFR Part 1194.21 to the extent possible.	Release 1A; Should
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 1A; Should

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 1A; Should
7.3.2.2.1.3	A well-defined on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes. The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.	Release 1A; Should
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 must also be available in text.	Release 1A; Should
7.3.2.2.1.5	When bitmap 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 1A; Should
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 1A; Should
7.3.2.2.1.7	Applications shall not override user selected contrast and color selections and other individual display attributes.	Release 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 to the extent possible.	Release 1A; Should
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 1A; Should
7.3.2.2.2.2	Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Release 1A; Should
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 1A; Should
7.3.2.2.2.4	Documents shall be organized so they are readable without requiring an associated style sheet.	Release 1A; Should
7.3.2.2.2.5	Redundant text links shall be provided for each active region of a server-side image map.	Release 1A; Should

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 1A; Should
7.3.2.2.2.7	Row and column headers shall be identified for data tables.	Release 1A; Should
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 1A; Should
7.3.2.2.2.9	Frames shall be titled with text that facilitates frame identification and navigation.	Release 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
7.3.2.2.2.13	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) through (l).	Release 1A; Should
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 1A; Should
7.3.2.2.2.15	A method shall be provided that permits users to skip repetitive navigation links.	Release 1A; Should
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 1A; Should
7.3.2.2.3	FDsys telecommunications products shall be Section 508 compliant according to 36 CFR Part 1194.23 to the extent possible.	Release 1A; Should
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 1A; Should
7.3.2.2.3.2	Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer non-proprietary standard TTY signal protocols.	Release 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should

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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
7.3.2.2.3.11	Products which have mechanically operated controls or keys, shall comply with the following:	Release 1A; Should
7.3.2.2.4	FDsys video and multimedia products shall be Section 508 compliant according to 36 CFR Part 1194.24 to the extent possible.	Release 1A; Should
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 stand-alone 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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
7.3.2.2.4.5	Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.	Release 1A; Should
7.3.2.2.5	FDsys self contained, closed products shall be Section 508 compliant according to 36 CFR Part 1194.25 to the extent possible.	Release 1A; Should
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 1A; Should
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 1A; Should

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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
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 1A; Should
7.3.2.2.6	FDsys desktop and portable computer products shall be Section 508 compliant according to 36 CFR Part 1194.26 to the extent possible.	Release 1A; Should
7.3.2.2.6.1	All mechanically operated controls and keys shall comply with §1194.23 (k) (1) through (4).	Release 1A; Should
7.3.2.2.6.2	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	Release 1A; Should
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 1A; Should
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 1A; Should

3.2.7.4.2	Requirements for Search	
7.4.2.1	**Search Core Capabilities**	
7.4.2.1.1	The system must provide the capability to search for and retrieve content from the system.	Release 1B; Must
7.4.2.1.2	The system must provide the capability to search for and retrieve metadata from the system.	Release 1B; Must
7.4.2.1.3	The system must provide the capability to search across multiple internal content and metadata repositories simultaneously and separately.	Release 1B; Must
7.4.2.1.4	The system must provide the capability to search content that is currently available on the GPO Access public Web site.	Release 1B; Must

7.4.2.1.5	The system must provide the capability to search cataloging records in order to provide access to select external repositories with which GPO has formal partnership agreements.	Release 1B; Must
7.4.2.1.6	The system must provide the capability to search and retrieve unstructured content (e.g., text).	Release 1B; Must
7.4.2.1.7	The system must provide the capability to match character strings (e.g., search exact phrases).	Release 1B; Must
7.4.2.1.8	The system must provide the capability to search and retrieve semi-structured content (e.g., inline markup).	Release 1B; Must
7.4.2.1.9	The system must provide the capability to search and retrieve structured content (e.g., fielded).	Release 1B; Must
7.4.2.1.10	The system must provide the capability to search for content by means of querying metadata.	Release 1B; Must
7.4.2.1.11	The system must provide the capability for users to search collections based on user class, user role, and access rights.	Release 1B; Must
7.4.2.1.12	The system must provide the capability to search in Access Content Storage and Work in Progress storage both simultaneously and separately.	Release 1B; Must

7.4.2.2	**Search - Query**	
7.4.2.2.1	The system must provide the capability for users to select content collections to search.	Release 1B; Must
7.4.2.2.2	The system must 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
7.4.2.2.3	The system must provide the capability for users to select search complexity levels (e.g., simple search, advanced/fielded search).	Release 1B; Must
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
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 1B; Must
7.4.2.2.4	The system shall allow users to limit searches by available qualifiers, options, or limits as defined by GPO business rules.	Release 1B; Must
7.4.2.2.5	The system must provide the capability for GPO Business Managers to customize search qualifiers, options, or limits including but not limited to the following:	Release 1B; Must
7.4.2.2.6	The system must allow users to perform a search for conceptually related terms (e.g., search for "World Series" returns articles on the Red Sox).	Release 1B; Must
7.4.2.2.6.1	The system shall allow GPO administrators to add, modify, and delete concept relationships.	Release 1B; Must
7.4.2.2.6.2	The system shall process content, metadata, and BPI to create and update existing concept relationships.	Release 1B; Must
7.4.2.2.6.3	The system shall process user input (e.g. search terms) to help define concept relationships.	Release 1B; Must
7.4.2.2.7	The system must support standard Boolean search language.	Release 1B; Must
7.4.2.2.7.1	The system shall support full Boolean operators, including but not limited to: AND, OR, NOT, BEFORE, NEAR, and ADJACENT.	Release 1B; Must
7.4.2.2.7.2	The system shall support implied Boolean operators, including but not limited to “+” and “-“.	Release 1B; Must
7.4.2.2.7.3	The system shall support the nesting of Boolean operators via parentheses.	Release 1B; Must
7.4.2.2.7.4	Boolean operators must not be case-sensitive.	Release 1B; Must

7.4.2.2.8	The system must allow users to perform a natural language search that does not require connectors or a specific syntax.	Release 1B; Must
7.4.2.2.9	The system must support a customizable list of stop words.	Release 1B; Must
7.4.2.2.10	The system must allow for right and left truncation.	Release 1B; Must
7.4.2.2.11	The system must allow users to use wildcard characters to replace characters within words.	Release 1B; Must
7.4.2.2.12	The system must support proximity searching.	Release 1B; Must
7.4.2.2.13	The system must support synonyms searching.	Release 1B; Must
7.4.2.2.14	The system may provide the capability for contextual searching	Release 1B; Could
7.4.2.2.15	The system must conform to ISO 239.50 or other international standards for search interoperability.	Release 1B; Must
7.4.2.2.16	The system must provide the capability to perform searches across internal repositories including legacy repositories.	Release 1B; Must
7.4.2.2.17	The system must have a documented interface (e.g., API) to allow search by non-GPO systems.	Release 1B; Must
7.4.2.2.18	The system must have the capability to comply with OAI-PHM.	Release 1B; Must
7.4.2.2.19	The system must allow users to select specified search functionality.	Release 1B; Must
7.4.2.2.20	The system must support queries of variable lengths.	Release 1B; Must
7.4.2.2.21	The systems must have the ability to limit search query length.	Release 1B; Must
7.4.2.2.22	The system must provide the capability to weight search terms (e.g., term must appear, term must not appear, term is part of an exact phrase).	Release 1B; Must

7.4.2.3	**Search - Refine**	
7.4.2.3.1	The system must provide the capability for users to modify previous search queries to enable execution of subsequent searches.	Release 1B; Must
7.4.2.3.1.1	The system shall provide the capability to direct subsequent queries against different content collections.	Release 1B; Must
7.4.2.3.1.2	The system shall provide the capability for users to retain selected targets while modifying queries.	Release 1B; Must
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 1B; Must
7.4.2.3.2.1	The system shall provide users with the ability to directly execute a search from conceptually related terms.	Release 1B; Must
7.4.2.3.3	The system must recognize alternate spellings of terms and provide suggestions for alternative terms.	Release 1B; Must
7.4.2.3.3.1	The system shall suggest corrected spellings of terms.	Release 1B; Must

7.4.2.4	**Search - Results**	
7.4.2.4.1	The system must provide search results to users.	Release 1B; Must
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
7.4.2.4.3	The system must provide the capability to sort results lists.	Release 1B; Must
7.4.2.4.4	The system must provide the capability to categorize results.	Release 1B; Must
7.4.2.4.5	The system must provide the capability to cluster results.	Release 1B; Could
7.4.2.4.6	The system may provide the capability to analyze results lists.	Release 1B; Could
7.4.2.4.7	The system shall provide the capability to display results graphically.	Release 1B; Could
7.4.2.4.8	The system must provide the capability to apply one or multiple taxonomies.	Release 1B; Could
7.4.2.4.9	The system must provide the capability for users to limit the number of results displayed.	Release 1B; Must
7.4.2.4.10	The system must provide the capability to display the total number of results in the result set returned by the search.	Release 1B; Must

7.4.2.4.11	The system must provide the capability to configure the elements in a result.	Release 1B; Must
7.4.2.4.11.1	The system must display, at a minimum, title, file size, version, content collection (source), and an identifier (link).	Release 1B; Must
7.4.2.4.11.2	The system shall have the capability to display other elements in a result (e.g., relevance rank, description of content) when available.	Release 1B; Must
7.4.2.4.12	The system shall provide the capability to highlight query terms in the results list.	Release 1B; Could
7.4.2.4.13	The system must provide the ability to generate error messages for failed searches.	Release 1B; Must
7.4.2.4.14	The system must provide the capability to display inline image thumbnails of content in a results list.	Release 1B; Must
7.4.2.4.15	The system must allow users to save search results individually or as a batch (e.g., without selecting each result individually) for export.	Release 1B; Should / Release 2; Must
7.4.2.4.16	The system must provide the capability to deliver search results at the finest level of granularity supported by the target content package and as required in the FDsys Unique ID requirements.	Release 1B; Must
7.4.2.4.17	The system shall provide the capability to modify relevancy ranking factors based on business rules.	Release 1B; Should / Release 2; Must

7.4.2.5	**Saved Searches**	
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 1B; Should / Release 2; Must
7.4.2.5.2	The system shall provide the capability to automatically execute saved searches on a schedule defined by the user.	Release 1B; Should / Release 2; Must
7.4.2.5.3	The system shall provide the capability to notify users when automatically executed searches return results.	Release 1B; Should / Release 2; Must

7.4.2.6	**Search Interface**	
7.4.2.6.1	The system must provide a search interface that allows users to submit queries to the system and receive results.	Release 1B; Must
7.4.2.6.2	The system must provide the capability to have multiple search interfaces based on search skill level and user class.	Release 1B; Must
7.4.2.6.3	The system must provide the capability to have customizable search interfaces based on user preferences and requirements.	Release 1C; Should / Release 2; Must
7.4.2.6.4	The system must provide the capability to have navigational elements to allow users to navigate through results.	Release 1B; Must
7.4.2.6.5	The system must have the capability to store and access user search preferences (e.g., preferred layout, preferred search method, frequently used content collections).	Release 1C; Should / Release 2; Must

7.4.2.7	**Search Administration**	
7.4.2.7.1	The system must provide the capability to manage user search interfaces.	Release 1B; Must
7.4.2.7.2	The system must provide a Web-based administrator graphical user interface (GUI).	Release 1B; Must
7.4.2.7.3	The system must provide the capability to configure an unlimited number of search portals.	Release 1B; Must
7.4.2.7.4	The system must provide for the control of search run times, including the ability to preempt runtimes by an administrator-defined limit.	Release 1B; Must
7.4.2.7.5	The system must provide the capability to support user search while other system functions are being performed (e.g., re-indexing databases, updating content).	Release 1B; Must

7.4.2.7.6	The system must provide the capability to log search activities.	Release 1B; Must

3.2.7.5.2	Requirements for Request	
7.5.2.1	**Request Core Capabilities**	
7.5.2.1.1	The system shall provide the capability for users to request delivery of content.	Release 1B; Must
7.5.2.1.2	The system shall provide the capability for users to request delivery of metadata.	Release 1B; Must
7.5.2.1.3	The system must comply with GPO and Federal privacy, security, and records management policies.	Release 1B; Must

7.5.2.2	**No Fee Requests**	
7.5.2.2.1	The system must provide the capability for End Users to request no-fee content delivery as defined by GPO business units.	Release 1B; Must
7.5.2.2.1.1	The system must not restrict or otherwise diminish access to items that are currently available through GPO Access.	Release 1B; Must
7.5.2.2.1.2	The system must provide the capability for users to print and download information currently available through GPO Access.	Release 1B; Must
7.5.2.2.2	The system must provide the capability for Federal Depository Library End Users to select and request content and metadata for delivery to their library based on their unique profile and preferences.	Release 1B; Must
7.5.2.2.3	The system shall comply with GPO policies related to selection of tangible and electronic titles by Federal Depository Library End Users.	Release 1B; Must
7.5.2.2.4	The system shall provide the capability to interface with “Authorized Representatives” as designated by GPO’s Library Services and Content Management business unit for processing of no-fee delivery requests.	Release 1B; Must
7.5.2.2.5	The system must provide the capability to interface with GPO’s Integrated Library System and other legacy systems as defined by GPO business units for processing of no-fee requests.	Release 1B; Must
7.5.2.2.6	The system must provide the capability to process no-fee requests for delivery of content with access restrictions.	Release 1B; Must
7.5.2.2.7	The system must support the delivery of serials and periodicals.	Release 1B; Must
7.5.2.2.8	The system must provide the capability for users to cancel full or partial requests prior to fulfillment.	Release 1B; Must
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
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
7.5.2.2.10	The system must provide the capability to provide authorized users with a detailed transaction summary according to GPO business rules.	Release 1B; Should / Release 2; Must
7.5.2.2.11	The system shall provide the capability for GPO to configure transaction summaries to include but not be limited to the following:	Release 1B; Should / Release 2; Must
7.5.2.2.12	The system must provide the capability to generate reports for no-fee transactions.	Release 1B; Must

7.5.2.3	**Fee-based Requests**	
7.5.2.3.1	The system must provide the capability for users to request fee-based content delivery as defined by GPO business rules.	Release 1C; Must

7.5.2.3.2	The system must 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 1C; Must
7.5.2.3.3	The system must provide the capability to interface with GPO’s financial and inventory systems for processing of fee-based requests.	Release 1C; Must
7.5.2.3.4	The system must ensure that user transactions are conducted in a secure environment at the industry standard level of integrity.	Release 1C; Must
7.5.2.3.5	The system must have the capability to generate price information for the delivery of content.	Release 1C; Must
7.5.2.3.6	The system must have the capability to adjust price information for fee-based content delivery.	Release 1C; Must
7.5.2.3.6.1	Pricing structures must comply with GPO’s legislative mandates under Title 44 of the United States Code and GPO’s Sales Program policies.	Release 1C; Must
7.5.2.3.6.2	The system must provide the capability to manually adjust the price.	Release 1C; Must
7.5.2.3.6.3	The system must provide the capability to dynamically adjust the price.	Release 1C; Must
7.5.2.3.6.4	The system must provide the capability to apply price schedules.	Release 1C; Must
7.5.2.3.7	The system must adhere to industry best practices for performance of a Web-accessible e-commerce system.	Release 1C; Must
7.5.2.3.8	The system must include an online bookstore web interface that complies with the FDsys interface requirements and includes but is not limited to the following features:	Release 1C; Must
7.5.2.3.9	The system must provide the capability to process international and domestic requests for publications, subscriptions, and standing orders according to GPO business rules.	Release 1C; Must
7.5.2.3.10	The system must provide the capability to process fee-based requests for the delivery of content with access restrictions.	Release 1C; Must
7.5.2.3.11	The system must support methods of payment as defined by GPO business rules. The system must provide the capability to accept the following payment methods:	Release 1C; Must
7.5.2.3.12	The system must provide the capability to automatically verify and validate payment information submitted by users prior to delivery fulfillment.	Release 1C; Must
7.5.2.3.13	The system must 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
7.5.2.3.14	The system must 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
7.5.2.3.15	The system must 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 1C; Must
7.5.2.3.15.1	The system shall provide the capability to manage, secure, and maintain End User information associated with subscriptions.	Release 1C; Must
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
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
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
7.5.2.3.17	The system must provide the capability for users to cancel full or partial requests prior to fulfillment.	Release 1C; Must

7.5.2.3.18	The system must provide the capability to provide authorized users with a detailed transaction summary according to GPO business rules.	Release 1C; Must
7.5.2.3.19	The system shall provide the capability for GPO to configure transaction summaries to include but not be limited to the following:	Release 1C; Should / Release 2; Must
7.5.2.3.20	The system must provide the capability to manage transaction records according to GPO and Federal policies.	Release 1C; Must
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 1C; Must
7.5.2.3.21	The system must provide the capability to generate reports for fee-based transactions (e.g., order histories, sales transactions, inventory data).	Release 1C; Must

7.5.2.4	**Request - Delivery Options**	
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 1B; Must
7.5.2.4.2	The system must provide the capability for users to request delivery of content or metadata from available options as defined by GPO business units.	Release 1B; Must
7.5.2.4.3	The system must 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 1B; Must
7.5.2.4.4	The system must provide the capability for users to select file type from available options (e.g., DOC, MP3, PDF).	Release 1B; Must
7.5.2.4.5	The system must provide the capability for users to select resolution (e.g., images, video) from available options.	Release 1B; Could / Release 2; Must
7.5.2.4.6	The system must provide the capability for users to select color space from available options (e.g. RGB, CMYK).	Release 1B; Could / Release 2; Must
7.5.2.4.7	The system must provide the capability for users to select compression and size from available options.	Release 1B; Could / Release 2; Must
7.5.2.4.8	The system must provide the capability for users to select transfer rate from available options.	Release 1B; Could / Release 2; Must
7.5.2.4.9	The system must provide the capability for users to select platform from available options.	Release 1B; Must
7.5.2.4.10	The system must provide the capability for users to select the version of content from available options.	Release 1B; Must
7.5.2.4.11	The system must provide the capability for users to select delivery of related content from available options.	Release 1B; Could / Release 2; Must
7.5.2.4.12	The system must 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 1B; Must
7.5.2.4.13	The system must provide the capability for users to select quantity of items requested for delivery (e.g., one, five, batch).	Release 1B; Must
7.5.2.4.14	The system must provide the capability for users to select output type from available options (e.g., hard copy, electronic presentation, digital media).	Release 1B; Must
7.5.2.4.15	The system must provide the capability for users to select data storage device from available options (e.g., CD, DVD, server).	Release 1B; Must
7.5.2.4.16	The system must provide the capability for users to select level of granularity from available options (e.g., title, part, section, paragraph, graphic, page).	Release 1B; Must
7.5.2.4.17	The system must provide the capability for users to select electronic delivery method from available options (e.g., FTP, RSS, email, download, broadcast).	Release 1B; Must
7.5.2.4.18	The system must provide the capability for users to schedule delivery from the system.	Release 1B; Should

7.5.2.4.19	The system must provide the capability for users to select tangible delivery method from available options (e.g., air transportation, ground transportation, pickup, overnight, priority, freight).	Release 1C; Must
7.5.2.4.20	The system must provide the capability for GPO to offer users separate “bill to” and “ship to” options for delivery or shipment of tangible content.	Release 1C; Must
7.5.2.4.21	The system must provide the capability for users to submit multiple address options for delivery or shipment of tangible content.	Release 1C; Must
7.5.2.4.22	The system must provide the capability to preview requested content.	Release 2; Should / Release 3; Must
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

7.5.2.5	**Request - User Accounts**	
7.5.2.5.1	The system must provide the capability to create a secure user account with the system.	Release 1B; Must
7.5.2.5.2	The system shall provide the capability for End Users and Service Providers to manage their accounts which includes but is not limited to the following:	Release 1B; Should / Release 1C; Must

7.5.2.6	**Order Numbers and Request Status**	
7.5.2.6.1	The system must provide the capability to create and assign an alphanumeric order number for requests.	Release 1B; Must
7.5.2.6.2	The system must not repeat an order number.	Release 1B; Must
7.5.2.6.3	The system must record order numbers in metadata.	Release 1B; Must
7.5.2.6.4	The system must have the capability to provide order numbers to users.	Release 1B; Must
7.5.2.6.5	The system must provide the capability for users to track the status of their requests.	Release 1B; Must

3.2.7.6.2	**Requirements for Cataloging and Reference Tools**	
7.6.2.1	**Cataloging and Reference Tools - Metadata Management**	
7.6.2.1.1	The system shall provide for the creation of metadata for content.	Release 1A; Must
7.6.2.1.2	The system shall support creation of metadata according to specified cataloging rules.	Release 1A; Must
7.6.2.1.3	The system will apply authority control to provide cross-referencing of terms. (e.g., a user enters any form of a name, title, or subject in a search and all database items associated with that form must be retrieved).	Release 1B; Must
7.6.2.1.4	The system shall support the creation of metadata meeting book industry requirements (e.g., ONIX).	Release 1C; Must
7.6.2.1.5	The system shall support the creation of library standard bibliographic records (e.g., MARC).	Release 1A; Must
7.6.2.1.6	The system shall support the creation of metadata by the system (e.g., automatically create).	Release 1A; Must
7.6.2.1.7	The system shall provide for the creation of metadata by authorized users (e.g., manually create).	Release 1A; Must
7.6.2.1.8	The system shall provide for the creation of new metadata records based on existing metadata records.	Release 1A; Must
7.6.2.1.9	The system shall provide the capability to acquire and integrate metadata from external sources.	Release 1A; Must

7.6.2.1.10	The system shall relate descriptive metadata with the content described.	Release 1A; Must
7.6.2.1.11	The system shall provide capability for authorized users to manage metadata.	Release 1A; Must
7.6.2.1.12	The system shall support versioning of metadata.	Release 1A; Must
7.6.2.1.13	The system shall have the ability to provide access to metadata throughout the lifecycle of the content.	Release 1A; Must
7.6.2.1.14	The system must provide the capability to add metadata specifically for GPO sales purposes (e.g., book jacket art, reviews, summaries).	Release 1C; Could
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 1A; Must

7.6.2.2	**Cataloging and Reference Tools - Metadata Delivery**	
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 1B; Must
7.6.2.2.2	The system will provide for display and output of brief citations.	Release 1B; Must
7.6.2.2.3	The system will provide for display and output of basic bibliographic citations.	Release 1B; Must
7.6.2.2.4	The system will provide for display and output of full records.	Release 1B; Must
7.6.2.2.5	The system will provide for display and output of MARC records.	Release 1B; Must
7.6.2.2.6	The system will provide for the delivery of output in a variety user-specified methods or formats, including but not limited to electronic mail or Web pages.	Release 1B; Must
7.6.2.2.7	The system shall output metadata in formats specified by the user, including but not limited to MARC, ONIX, ASCII text, or comma delimited text.	Release 1B; Must

7.6.2.3	**Reference Tools**	
7.6.2.3.1	The system shall have the ability to generate lists based on any indexed metadata field.	Release 1B; Must
7.6.2.3.2	The system should have the capability to generate lists based on user defined criteria (e.g., that match a library's item selection profile).	Release 1B; Must
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 1B; Must
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 1B; Must
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 1B; Should
7.6.2.3.6	The system shall have the capability to link to external content and metadata.	Release 1B; Must
7.6.2.3.7	The system shall be interoperable with third party reference tools (e.g., search catalogs of other libraries).	Release 2; Should
7.6.2.3.8	The system shall have the capability to dynamically generate reference tools.	Release 2; Could
7.6.2.3.9	The system will allow GPO to manage reference tools.	Release 1B; Must
7.6.2.3.10	The system must be able to generate lists based on user preferences.	Release 1C Should / Release 2; Must
7.6.2.3.11	The system shall provide the capability for users to customize reference tools.	Release 1C; Should / Release 2; Must
7.6.2.3.12	The system shall support interactive processes so users can create reference tools.	Release 2; Should

7.6.2.4	**Cataloging and Reference Tools - Interoperability and Standards**	
7.6.2.4.1	The system shall interface with, and allow full functionality of, the GPO Integrated Library System.	Release 1A; Must
7.6.2.4.2	The system must be compliant with the following NISO and ISO standards: Z39.2 - Information Interchange Format, Z39.9 - International Standard Serial Numbering-ISSN, Z39.29 – 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 1A; Must
7.6.2.4.3	The system must 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 1A; Must
7.6.2.4.4	The system shall support the creation of ONIX records.	Release 1C; Must
7.6.2.4.5	The system shall provide the capability to support search of GPO local data elements that identify unique attributes of the FDLP (e.g., GPO Superintendent of Documents (SuDocs) classification number, Item number, Depository Library number).	Release 1A; Must

3.2.7.7.2	**Requirements for User Interface**	
7.7.2.1	**User Interface Core Capabilities**	
7.7.2.1.1	The system must provide a default Graphical User Interface (GUI) for each functional element as required in accordance with the system release schedule.	Release 1A; Must
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 1A; Must
7.7.2.1.2.1	The system must provide the capability to provide default workbenches that do not require users to register with the system.	Release 1A; Must
7.7.2.1.2.2	The system must provide the capability for GPO to create workbenches for subsets of user classes.	Release 1A; Must
7.7.2.1.2.3	The system must provide the capability for GPO to manage the toolsets that are available on default workbenches.	Release 1A; Must
7.7.2.1.2.4	The system must provide a default public End User workbench that allows users to access official Federal Government information without registering with the system.	Release 1B; Must
7.7.2.1.2.5	The default public End User workbench must be Section 508 compliant.	Release 1B; Must
7.7.2.1.2.6	The system must provide a default Service Specialist workbench that provides the capability for Service Specialists to handle exception processing.	Release 1A; Must
7.7.2.1.2.7	The system must 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 1A; Must

7.7.2.1.3	The system must provide the capability to maintain a consistent look and feel throughout workbenches and GUIs to the extent possible.	Release 1A; Should
7.7.2.1.3.1	GUIs must conform to GPO design guidelines and GPO business rules.	Release 1A; Should
7.7.2.1.4	The system must support web-based GUIs.	Release 1A; Must
7.7.2.1.5	The system must support non web-based GUIs, as necessary.	Release 1A; Should
7.7.2.1.6	The system must provide GUIs capable of displaying supported types of electronic files (e.g., electronic presentation).	Release 1A; Must
7.7.2.1.7	The system shall provide for non-English language extensibility such that GUIs could contain non-English language text.	Release 1A; Could / Release 2; Must
7.7.2.1.8	The system must provide GUIs that accept input of information by users.	Release 1A; Must
7.7.2.1.9	The system must provide GUIs that accept submission of content by users.	Release 1A; Must
7.7.2.1.10	The system must provide GUIs that allow users to input and submit registration information and login to the system.	Release 1A; Must
7.7.2.1.11	The system must display the appropriate default GUIs and workbenches based on a user's access rights, user role, user class, or registration information.	Release 1A; Must
7.7.2.1.12	The system must provide the capability to integrate search, cataloging and reference tools, request, and user support seamlessly into an End User workbench.	Release 1B; Must
7.7.2.1.13	The system must provide GUIs that can be displayed on Macintosh, Unix, and Windows environments.	Release 1A; Must
7.7.2.1.14	The system must provide GUIs that are capable of providing feedback, alerts, or notices to users.	Release 1A; Must
7.7.2.1.15	The system must provide GUIs that are capable of providing context specific help and user support.	Release 1A; Must

7.7.2.2	**User Interface Standards and Best Practices**	
7.7.2.2.1	The system shall comply with best practices and guidelines regarding usability for graphical user interface design.	Release 1A; Should
7.7.2.2.1.1	GUIs should be developed in accordance with guidance issued by the Research-Based Web Design & Usability Guidelines function as best practices for Federal Agencies.	Release 1A; Should
7.7.2.2.1.2	Web GUIs should be developed in accordance with the Web Style Guide, 2nd edition.	Release 1A; Should
7.7.2.2.2	The system must conform to current World Wide Web Consortium (W3C) guidelines for interoperable technologies including but not limited to the following.	Release 1A; Must
7.7.2.2.2.1	The system must conform to Extensible Markup Language (XML).	Release 1A; Must
7.7.2.2.2.2	The system must conform to Extensible Style sheet Language (XSL).	Release 1A; Must
7.7.2.2.2.3	The system must conform to Document Type Definition (DTD) and schema.	Release 1A; Must
7.7.2.2.2.4	The system must conform to XSL Transformations (XSLT).	Release 1A; Must
7.7.2.2.2.5	The system must conform to XML Path Language (XPath).	Release 1A; Must
7.7.2.2.2.6	The system must conform to Extensible HyperText Markup Language (XHTML).	Release 1A; Must
7.7.2.2.2.7	The system must conform to Cascading Style Sheets (CSS).	Release 1A; Must
7.7.2.2.2.8	The system must conform to Document Object Model (DOM).	Release 1A; Must
7.7.2.2.2.9	The system must conform to Hypertext Transfer Protocol (HTTP).	Release 1A; Must

7.7.2.3	**User Interface Customization and Personalization**	

7.7.2.3.1	The system must provide the capability for authorized users who have registered with the system to customize default GUIs and workbenches.	Release 1C; Should / Release 2; Must
7.7.2.3.1.1	The system must provide the capability to add tools.	Release 1C; Should / Release 2; Must
7.7.2.3.1.2	The system must provide the capability to remove tools.	Release 1C; Should / Release 2; Must
7.7.2.3.1.3	The system must provide the capability to hide tools.	Release 1C; Should / Release 2; Must
7.7.2.3.1.4	The system shall provide the capability to modify the placement of tools.	Release 1C; Should / Release 2; Must
7.7.2.3.1.5	The system shall provide the capability to modify the size of tools.	Release 1C; Should / Release 2; Must
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
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
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
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
7.7.2.3.4	The system must provide the capability for users to revert to their original default GUIs and workbenches.	Release 1C; Should / Release 2; Must
7.7.2.3.5	The system must provide the capability to maintain interface configurations across user sessions.	Release 1C; Should / Release 2; Must

7.7.2.4	**User Interface Default Workbenches**	
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 1A; Must
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.	Release 1A; Must
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.	Release 1A; Must
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.	Release 1A; Must
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.	Release 1B; Must
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.	Release 1B; Must
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.	Release 1B; Could / Release 2; Must
7.7.2.4.8	The system must provide a default interface for authorized Systems Administrators / Operations Managers that includes but is not limited to the following tools.	Release 1A; Must

3.2.7.8.2 Requirements for User Support

7.8.2.1	**User Support Core Capabilities**	
7.8.2.1.1	The system shall provide multiple methods of contact for user assistance.	multiple releases
7.8.2.1.1.1	The system shall provide multiple methods for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	multiple releases
7.8.2.1.1.1.1	The system shall provide Web form for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	Release 1A; Should / Release 1B; Must
7.8.2.1.1.1.2	The system shall provide Phone service for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	Release 1A; Could
7.8.2.1.1.1.3	The system shall provide E-Mail for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	Release 1A; Must
7.8.2.1.1.1.4	The system shall provide Mail for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	Release 1A; Could
7.8.2.1.1.1.5	The system shall provide Real-time text chat for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	Release 1A; Could
7.8.2.1.1.1.6	The system shall provide Facsimile for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	Release 1A; Could
7.8.2.1.1.1.7	The system shall provide Desktop Facsimile for End Users, Service Providers and Content Originators to contact GPO Service Specialists for user assistance.	Release 1A; Could
7.8.2.1.1.2	The system shall provide multiple methods for GPO Service Specialists to contact End Users, Service Providers and Content Originators for user assistance.	multiple releases
7.8.2.1.1.2.1	The system shall provide Phone services for GPO Service Specialists to contact End Users, Service Providers and Content Originators for user assistance.	Release 1A; Could
7.8.2.1.1.2.2	The system shall provide E Mail for GPO Service Specialists to contact End Users, Service Providers and Content Originators for user assistance.	Release 1A; Must
7.8.2.1.1.2.3	The system shall provide Real-time text chat for GPO Service Specialists to contact End Users, Service Providers and Content Originators for user assistance.	Release 1A; Could
7.8.2.1.1.2.4	The system shall provide Facsimile for GPO Service Specialists to contact End Users, Service Providers and Content Originators for user assistance.	Release 1A; Could
7.8.2.1.1.2.5	The system shall provide Desktop Facsimile for GPO Service Specialists to contact End Users, Service Providers and Content Originators for user assistance.	Release 1A; Could
7.8.2.1.2	The system shall provide users with the ability to opt-out of user support features.	Release 1B; Could
7.8.2.1.2.1	The system shall provide users with the ability to turn on each user support feature individually.	Release 1B; Could
7.8.2.1.2.2	The system shall provide users with the ability to turn off each user support feature individually.	Release 1B; Could

7.8.2.2	**User Support - Context Specific Help**	
7.8.2.2.1	The system shall provide context-specific help on user interfaces.	Release 1B; Could / Release 1C; Must

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 1B; Could / Release 1C; Must
7.8.2.2.1.2	Content of context specific help shall be specific to user class.	Release 1B; Could / Release 1C; Must
7.8.2.2.1.3	Context specific help shall consist of help menus.	Release 1B; Could / Release 1C; Must
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
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
7.8.2.2.1.3.3	Authorized Service Specialists shall have the ability to manage information (text, images, audio, video, multimedia) in the help menu.	Release 1B; Could / Release 1C; Must
7.8.2.2.1.3.4	All users shall have the ability to search the help menu.	Release 1B; Could / Release 1C; Must
7.8.2.2.1.3.5	The system shall return search results to the user.	Release 1B; Could / Release 1C; Must
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
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
7.8.2.2.1.4.1	GPO Service Specialists shall have the ability to manage customizable descriptive text.	Release 1B; Could / Release 1C; Must
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
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
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
7.8.2.2.1.5.3	Authorized GPO Service Specialists shall have the ability to manage information (text, images, audio, video, multimedia) displayed as a result of clicking on help icons or text.	Release 1B; Could / Release 1C; Must
7.8.2.2.1.5.4	Authorized GPO Service Specialists shall have the ability to place help icons or text where needed on the user interface.	Release 1B; Could / Release 1C; Must
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

7.8.2.3	**User Support - Helpdesk**	
7.8.2.3.1	The system shall have the capability to support a helpdesk to route, track, prioritize, and resolve user inquiries to GPO Service Specialists.	Release 1B; Must
7.8.2.3.2	Information collected and maintained by the helpdesk must comply with GPO and Federal privacy policies.	Release 1B; Must
7.8.2.3.2.1	Information collected and maintained by the helpdesk must comply with “Records maintained on individuals” Title 5 U.S. Code Sec. 552a, 2000 edition.	Release 1B; Must
7.8.2.3.2.2	Information collected and maintained by the helpdesk must comply with H.R. 2458, E-Government Act of 2002.	Release 1B; Must
7.8.2.3.3	The system shall have the capability to receive inquiries from registered and non-registered users.	Release 1B; Must
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 1B; Must
7.8.2.3.4	Users shall have the capability to select from lists of categories when submitting inquiries.	Release 1B; Could / Release 1C; Must
7.8.2.3.4.1	Users shall have the capability to select from subgroups of categories when submitting inquiries.	Release 1B; Could / Release 1C; Must

7.8.2.3.4.2	Authorized users shall have the capability to manage categories and subcategories.	Release 1B; Could / Release 1C; Must
7.8.2.3.5	Content Originators and End Users shall have the capability to attach files when submitting inquiries.	Release 1B; Could / Release 1C; Must
7.8.2.3.6	The system shall have the capability to notify users that their inquiry has been received.	Release 1B; Could / Release 1C; Must
7.8.2.3.7	The system shall have the capability to time and date stamp all inquiries and responses.	Release 1B; Could / Release 1C; Must
7.8.2.3.8	The system shall have the capability to notify designated Service Specialists that they have been assigned an inquiry.	Release 1B; Could / Release 1C; Must
7.8.2.3.9	The system shall have the capability to route, track, and prioritize inquiries and responses received.	Release 1B; Must
7.8.2.3.10	The system shall allow a Service Specialist to manually create a new inquiry in order to accommodate inquiries that do not enter the system electronically.	Release 1B; Must
7.8.2.3.11	The system shall provide the capability to queue inquiries.	Release 1B; Could / Release 1C; Must
7.8.2.3.12	The system shall support priority processing.	Release 1B; Could / Release 1C; Must
7.8.2.3.13	The system shall allow authorized users to manage the status categories for inquires.	Release 1B; Could / Release 1C; Must
7.8.2.3.14	The system shall provide the capability for authorized users to restrict access to inquiry tracking.	Release 1B; Must
7.8.2.3.15	The system shall provide automated routing of inquiries to the departments/individuals according to workflow guidelines, including but not limited to.	Release 1B; Could / Release 2; Must
7.8.2.3.15.1	Automated inquiry routing shall be based on selections made by the user when an inquiry is made.	Release 1B; Could / Release 2; Must
7.8.2.3.15.2	Automated inquiry routing shall be based on keywords in the inquiry sent by the user.	Release 1B; Could / Release 2; Must
7.8.2.3.15.3	Automated inquiry routing shall be based on the user class of the inquirer.	Release 1B; Could / Release 2; Must
7.8.2.3.15.4	The system shall allow authorized users to set routing preferences based on selections made, keywords and user class.	Release 1B; Could / Release 2; Must
7.8.2.3.16	GPO Service Specialists shall have the capability to route inquiries to other Service Specialists based on the needs of the End User or Content Originator.	Release 1B; Could / Release 1C; Must
7.8.2.3.16.1	GPO Service Specialists shall have the ability to route an inquiry to a selected individual.	Release 1B; Could / Release 1C; Must
7.8.2.3.16.2	GPO Service Specialists shall have the ability to route an inquiry to a selected department.	Release 1B; Could / Release 1C; Must
7.8.2.3.16.3	GPO Service Specialists shall have the ability to route inquiries to users who do not have access to the system using e-mail.	Release 1B; Could / Release 1C; Must
7.8.2.3.17	The system shall allow the user to determine the departments or individuals they wish to request answers from.	Release 1B; Could / Release 1C; Must
7.8.2.3.18	The system shall provide the capability to request user feedback regarding quality of response given.	Release 1B; Could / Release 1C; Must
7.8.2.3.19	The system shall provide users with access to history of their inquiries and responses.	Release 1B; Could / Release 1C; Must
7.8.2.3.20	The system shall store inquiries and responses.	Release 1B; Must
7.8.2.3.21	The system shall have the capability to allow authorized users to amend inquiries and responses.	Release 1B; Could / Release 1C; Must
7.8.2.3.22	The system shall have the capability for users to search inquiries and responses.	Release 1B; Must

7.8.2.3.23	The system shall allow authorized users to search by user-specific fields, including but not limited to job number, order number, agency, status, and inquiry number.	Release 1B; Must
7.8.2.3.24	The system shall support the capability to monitor the quality of responses given by helpdesk staff.	Release 1B; Could; / Release 2; Must
7.8.2.3.25	The system shall have the capability to provide users with access to questions and answers from other users related to their queries.	Release 1B; Could / Release 1C; Must
7.8.2.3.25.1	The system shall allow for search of questions and answers from other users.	Release 1B; Could / Release 1C; Must
7.8.2.3.25.2	The system shall provide the capability to assign user access rights to individual questions and answers.	Release 1B; Could / Release 1C; Must
7.8.2.3.26	The system shall provide the capability to identify GPO users responding to user inquiries.	Release 1B; Must
7.8.2.3.27	The system shall provide the capability to log information exchanges.	Release 1B; Must
7.8.2.3.27.1	Information exchange logs shall store metadata relating to what is being discussed.	Release 1B; Must
7.8.2.3.28	The system shall provide the capability to spell-check inquiries and responses before submission.	Release 1B; Could

7.8.2.4	**User Support - Knowledge Base**	
7.8.2.4.1	The system shall allow GPO Service Specialists, GPO Business Managers, and other users as authorized to add information to a knowledge base.	Release 1B; Must
7.8.2.4.2	The system shall provide the ability for GPO Service Specialists, GPO Business Managers, and other users as authorized to add electronic files to the knowledge base as attachments.	Release 1B; Must
7.8.2.4.3	The system shall provide the capability to create customized templates for knowledge base entries.	Release 1B; Could
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 1B; Could
7.8.2.4.4	The system shall have the capability to time and date stamp all knowledge base entries.	Release 1B; Must
7.8.2.4.5	The system shall provide the ability for authorized users to manage information in the knowledge base.	Release 1B; Must
7.8.2.4.6	The system shall provide the capability to add inquiries and answers from the helpdesk to the knowledge base.	Release 1B; Must
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 1B; Must
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 1B; Must
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 1B; Must
7.8.2.4.8	The system shall provide the capability to store standard responses for use by specific user groups or subgroups.	Release 1B; Could / Release 1C; Must
7.8.2.4.9	The system shall allow for information stored in the knowledge base to have role-based access restrictions.	Release 1B; Must
7.8.2.4.9.1	The system shall allow for access restrictions to be applied to complete categories.	Release 1B; Must
7.8.2.4.9.2	The system shall allow for access restrictions to be applied to individual knowledge base entries.	Release 1B; Must
7.8.2.4.10	The system shall provide the capability for all users to search the knowledge base.	Release 1B; Must
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 1B; Must

7.8.2.4.10.2	The system shall provide the capability for all users to search the knowledge base by phrase.	Release 1B; Must
7.8.2.4.10.3	The system shall provide the capability for all users to search the knowledge base by identification number.	Release 1B; Must
7.8.2.4.11	The system shall provide the capability to sort results of knowledge base searches.	Release 1B; Must
7.8.2.4.11.1	The system shall provide the capability to sort search results by category.	Release 1B; Must
7.8.2.4.11.2	The system shall provide the capability to sort search results by subject.	Release 1B; Must
7.8.2.4.11.3	The system shall provide the capability to sort search results by a default sort.	Release 1B; Must
7.8.2.4.12	The system shall provide the capability for all users to receive e-mail updates when the content of information stored in a knowledge base entry is updated.	Release 1B; Could / Release 2; Must
7.8.2.4.13	The system shall provide the capability to perform records management functions on knowledge base data.	Release 2; Must
7.8.2.4.14	The system shall provide the capability to spell-check knowledge base entries before submission.	Release 1B, Could

7.8.2.5	**User Support - Alerts**	
7.8.2.5.1	The system shall have the capability to provide alert services.	multiple releases
7.8.2.5.1.1	The system shall allow all users to subscribe and unsubscribe to alert services.	Release 1C; Could / Release 2; Must
7.8.2.5.1.2	Alert services shall be provided in the following formats:	Release 1C; Could / Release 2; Must
7.8.2.5.1.3	The system shall allow users to customize alert services.	Release 1C; Could / Release 2; Must
7.8.2.5.1.4	The system shall provide alerts based on user profiles and history.	Release 1C; Could / Release 2; Must
7.8.2.5.1.5	The system shall have the capability to automatically send alerts based on system events.	Release 1C; Could / Release 2; Must
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 1C; Could / Release 2; Must
7.8.2.5.1.7	The system shall have the capability to automatically send alerts based on job processing events. (e.g., order submitted, proofs returned, order shipped)	Release 1C; Must
7.8.2.5.1.8	Authorized users shall be able to create new alert categories where new alerts are manually generated.	Release 1C; Could / Release 2; Must
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
7.8.2.5.1.10	The system shall have the capability for GPO users to recommend alerts for addition to the knowledge base.	Release 1C; Could / Release 2; Must

7.8.2.6	**User Support - Training and Events**	
7.8.2.6.1	The system shall provide users access to training materials and training history.	Release 1C; Could
7.8.2.6.1.1	The system shall provide access to training materials supplied as digital video.	Release 1C; Could
7.8.2.6.1.2	The system shall provide access to training materials supplied as digital documents.	Release 1C; Could
7.8.2.6.1.3	The system shall provide access to training materials supplied as digital audio.	Release 1C; Could

7.8.2.6.1.4	The system shall provide access to training materials supplied as digital multimedia.	Release 1C; Could
7.8.2.6.1.5	The system shall provide access to training materials supplied in other formats.	Release 1C; Could
7.8.2.6.2	The system shall allow authorized users as determined by GPO Operations Managers to manage training materials and training history.	Release 1C; Could
7.8.2.6.3	The system shall have the capability for authorized users as determined by GPO Operations Managers to restrict access to training material and training history.	Release 1C; Could
7.8.2.6.3.1	Access restrictions to training materials shall be based on user class.	Release 1C; Could
7.8.2.6.3.2	Access restrictions to training materials shall be based on individual users.	Release 1C; Could
7.8.2.6.4	The system shall allow users to enroll in training and events.	Release 1C; Could
7.8.2.6.5	The system shall allow authorized users as determined by GPO Operations Managers to manage training and events.	Release 1C; Could
7.8.2.6.6	The system shall provide interactive training.	Release 2; Could
7.8.2.6.6.1	The system shall provide interactive self-paced training.	Release 2; Could
7.8.2.6.6.2	The system shall provide interactive instructor-led training.	Release 2; Could
7.8.2.6.7	The system shall provide users verification of enrollment in training and events.	Release 2; Could
7.8.2.6.8	The system shall provide the capability for users to measure their progress and performance.	Release 3; Could
7.8.2.6.9	The system shall provide the capability for users to provide feedback on training.	Release 3; Could
7.8.2.6.10	The system shall provide online tutorials.	Release 2; Could

3.2.8.2	**Requirements for Content Delivery and Processing**	
8.2.1	**Content Delivery Core Capabilities**	
8.2.1.1	The system shall have the capability to retrieve ACPs from Access Content Storage based on user request.	Release 1B; Must
8.2.1.2	The system shall have the capability to create DIPs from ACPs in delivery processing based upon a user request.	Release 1B; Must
8.2.1.3	The system shall have the capability to create pre-ingest bundles in delivery processing.	Release 1B; Must
8.2.1.4	The system shall have the capability to deliver DIPs and pre-ingest bundles based on requests.	Release 1B; Must
8.2.1.5	The system shall have the capability to push DIPs and pre-ingest bundles to users.	Release 1B; Must
8.2.1.6	Users shall have the ability to pull DIPs and pre-ingest bundles from the system.	Release 1B; Must
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 1B; Must
8.2.1.8	The system shall have the capability to determine if delivery is possible.	Release 1C; Must
8.2.1.8.1	The system shall have the capability to determine if delivery is possible based upon business rules.	Release 1C; Must
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
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

8.2.1.8.4	The system shall have the capability to inform users that delivery is not possible.	Release 1C; Must
8.2.1.8.5	The system shall have the capability to inform users why delivery is not possible.	Release 1C; Must
8.2.1.9	The system shall have the capability to provide users with estimated transfer time for delivery.	Release 1B; Could
8.2.1.10	The system shall have the capability to provide notification of fulfillment to users.	Release 1C; Must
8.2.1.10.1	The system shall have the capability to provide notification based on user preferences.	Release 1C; Should / Release 2; Must
8.2.1.10.2	The system shall have the capability to provide notification based on information gathered at time of request.	Release 1C; Must

8.2.2	**Content Delivery Processing**	
8.2.2.1	The system shall have the capability to package DIPs containing the digital object, metadata, and BPI.	Release 1B; Must
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 1B; Must
8.2.2.3	The system shall have capability to transform digital objects to different formats.	Release 1B; Must
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
8.2.2.4.1	The system shall have the capability to adjust the resolution of digital objects.	Release 1B; Could / Release 2; Must
8.2.2.4.2	The system shall have the capability to resize digital objects.	Release 1B; Could / Release 2; Must
8.2.2.4.3	The system shall have the capability to adjust the compression off digital objects.	Release 1B; Could / Release 2; Must
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
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
8.2.2.4.6	The system shall have the capability to rasterize digital objects.	Release 1B; Could / Release 2; Must
8.2.2.5	The system shall have the capability to process DIPs based on user request.	Release 1B; Must
8.2.2.6	The system shall have the capability to repurpose content from multiple packages into a single DIP.	Release 2; Must

8.2.3	**Content Delivery Mechanisms**	
8.2.3.1	The system shall have the capability to push DIPs and pre-ingest bundles to users using various delivery mechanisms, including, but not limited to the following:	Release 1B; Must
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**	
8.3.2.1	**Hard Copy Output Core Capabilities**	
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

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
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
8.3.2.1.3	The system shall have the capability to support hard copy output for variable data printing processes.	Release 1C; Could
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 1B; Could
8.3.2.1.4.1	The system shall allow users to manually add the Imprint line.	Release 1B; Could
8.3.2.1.4.2	The system shall automatically add the Imprint Line.	Release 1B; Could
8.3.2.1.4.3	The system shall allow users to manually adjust the location of the Imprint line.	Release 1B; Could
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
8.3.2.1.5.1	The system shall have the capability to deliver files in their native application file format.	Release 1B; Must
8.3.2.1.5.1.1	The system shall have the capability to convert native files to PDF.	Release 1B; Must
8.3.2.1.5.2	The system shall have the capability to deliver optimized (print, press) PDFs.	Release 1B; Must
8.3.2.1.5.2.1	Optimized PDFs shall have fonts and images embedded.	Release 1B; Must
8.3.2.1.5.2.2	Image resolution of PDF's shall conform to industry best practices as defined in GPO's press optimized PDF settings.	Release 1B; Must
8.3.2.1.5.3	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files, including but not limited to:	Release 1B; Must
8.3.2.1.5.4	The system shall have the capability to deliver vector graphics.	Release 1B; Must
8.3.2.1.5.5	The system shall have the capability to deliver raster images.	Release 1B; Must
8.3.2.1.5.6	The system shall have the capability to deliver Microsoft Office Suite application files, including but not limited to:	Release 1B; Must
8.3.2.1.5.7	The system shall have the capability to deliver XML.	Release 1B; Must
8.3.2.1.5.7.1	The system shall support cascading style sheets.	Release 1B; Must
8.3.2.1.5.7.2	The system shall support document type definition/schema.	Release 1B; Must
8.3.2.1.5.8	The system shall have the capability to deliver text files, including but not limited to:	Release 1B; Must
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
8.3.2.1.5.10	The system shall have the capability to deliver postscript files.	Release 1B; Must
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**	
8.4.2.1	**Electronic Presentation Core Capabilities**	
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 1B; Must
8.4.2.1.2	The system shall have the capability to render content for presentation on end user devices.	Release 1B; Must
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 1B; Must
8.4.2.1.4	The system shall have the capability to render content for presentation on non-desktop electronic devices, including but not limited to:	Release 1B; Should / Release 1C; Must

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 1B; Could
8.4.2.1.6	The system shall provide the capability to deliver DIPs that support static and dynamic text in multiple formats, including, but not limited to:	Release 1B; Must
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
8.4.2.1.6.2	The system shall have the capability to deliver electronic content in HTML with linked files (e.g., JPEG, GIV, MPEG, MP3) referenced in the HTML code conforming to the HTML 4.0.1 Specification.	Release 1B; Must
8.4.2.1.6.3	The system shall have the capability to deliver electronic content in XHTML with linked files (e.g., JPEG, GIV, MPEG, MP3) referenced in the XHTML code conforming to the XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition) specification.	Release 1B; Must
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
8.4.2.1.6.4.1	The system shall have the capability to convert images to descriptive ASCII text.	Release 1B; Must
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
8.4.2.1.6.5.1	The system shall have the capability to convert images to descriptive Unicode text.	Release 1B; Must
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; Could
8.4.2.1.6.7	The system shall have the capability to deliver electronic content in MS Office formats.	Release 1B; Must
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
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 1B; Could
8.4.2.1.7	The system shall provide the capability to deliver DIPs that support static and dynamic images in multiple formats, including, but not limited to:	Release 1B; Must
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
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
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
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
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
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
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

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 1B; Must
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 1B; Could
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 1B; Could
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 1B, Must
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 1C, Should / Release 2; Must
8.4.2.1.10	The system shall have the capability to deliver electronic content that maintains desired user functionality.	Release 1B; Must
8.4.2.1.10.1	The system shall deliver electronic content that maintains hyperlinks to the extent possible.	Release 1B; Must
8.4.2.1.10.2	The system shall deliver electronic content that maintains interactive content.	Release 1B; Must

3.2.8.5.2	Requirements for Digital Media	
8.5.2.1	**Digital Media Core Capabilities**	
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
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.	multiple releases
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, including, but not limited to:	multiple releases
8.5.2.1.2.1.1	Compact Discs (CD)	Release 1B, Must
8.5.2.1.2.1.2	Digital Versatile Discs (DVD)	Release 1B, Must
8.5.2.1.2.1.3	Blu-ray Discs (BD)	Release 1B, Could
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, including but not limited to:	Release 1B, Must
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, including but not limited to:	Release 1B, Must
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
8.5.2.1.2.4.1	The system shall have the capability to generate ISO image files.	Release 1B, Could / Release 2; Should
8.5.2.1.2.4.2	The system shall have the capability to generate VCD image files.	Release 1B, Could / Release 2; Should
8.5.2.1.2.4.3	The system shall have the capability to generate UDF image files.	Release 1B, Could / Release 2; Should
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
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

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
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 1B, Must
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
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:	Release 1B; Should / Release 1C; Must