U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED

ASSESSMENT REPORT 09-04

FEDERAL DIGITAL SYSTEM (FDSYS) INDEPENDENT VERIFICATION AND VALIDATION (IV&V) – SECURITY ANALYSIS REPORT

December 24, 2008

OFFICE OF INSPECTOR GENERAL

U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED
WASHINGTON, DC 20401

Memorandum

OFFICE OF THE INSPECTOR GENERAL

DATE: December 24, 2008

REPLY TO
ATTN OF: Assistant Inspector General for Audits and Inspections

SUBJECT: Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Final Security Analysis Report
Report Number 09-04

TO: Chief Information Officer

The GPO Office of Inspector General (OIG) is conducting independent verification and validation (IV&V) of GPO's Federal Digital System (FDsys)[1] implementation. The OIG contracted with American Systems[2] to conduct IV&V for the public release of FDsys Release 1.C.[3] As part of its contract with the OIG, American Systems is assessing the state of program management, technical, and testing plans and other efforts related to the rollout of Release 1.C. One tasking is to evaluate security planning and implementation. The attached report prepared by American Systems is intended to provide a high-level assessment of the most recent version of the FDsys System Security Plan (SSP). Appendix A provides more detailed findings on the SSP. The assessment results were briefed to the Chief Information Officer and the Chief Information Security Officer on November 5, 2008.

Section 6 of the report contains five recommendations designed to strengthen FDsys system security planning and implementation. Management concurred with each of the five recommendations. We consider the actions proposed by management responsive to each of the recommendations. Management's response is included in its entirety in Appendix B of the report. The recommendations are resolved and will remain open until management has completed actions and the IV&V team has completed follow-up work.

---

[1] The FDsys program is a multimillion dollar effort that GPO is funding and managing to modernize the GPO information collection, processing, and dissemination capabilities it performs for the three branches of the Federal Government.

[2] American Systems, located in Chantilly, Virginia, is a large information technology company with significant experience in the realm of IV&V for Federal civilian and Defense agencies, including the Department of State, the Navy, and the U.S. Agency for International Development.

[3] American Systems IV&V methodology is referenced to the framework established by the Institute of Electrical and Electronic Engineers (IEEE) Standard 1012-2004, the IEEE Standard for Software Verification and Validation.

The status of each recommendation upon issuance of this report is included in Appendix C. The final report distribution is in Appendix D.

If you have questions concerning this report or the IV&V process, please contact Mr. Brent Melson, Deputy Assistant Inspector General for Audits and Inspections at (202) 512-2037, or me at (202) 512-2009.

Brent Melson

for Kevin J. Carson
Assistant Inspector General for Audits and Inspections

Attachment

cc:
Chief of Staff
Chief Acquisition Officer
Chief Management Officer
Chief Technology Officer

IV&V TASK REPORT

TO:	Brent Melson, COTR
FROM:	IV&V, Jon Valett
IV&V OF:	GPO FDsys System Security Plan (Version 2.1 - Doc Number DCN 7024227)
SUBJECT:	Task 5.4.3.3 FDsys Security Analysis (Revised Final – Doc. No. 01-048)
DATE:	November 6, 2008
CC:	Dan Rose, David Harold, John Best, Chris Parr, Shawn O'Rourke, Mark LoGalbo

1. Description of Task

Independent Verification and Validation (IV&V) performed a second assessment of the *Government Printing Office (GPO) FDsys System Security Plan (SSP)* and its applicability to the FDsys program. Specifically, IV&V reviewed the:

- GPO FDsys System Security Plan, 12 September 2008 version 1.0
- GPO FDsys System Design Document, 5 September 2008 version 2.0

2. Summary of Task Results

GPO FDsys PMO now has the responsibility for the development of the *GPO FDsys SSP*. In reviewing the *GPO FDsys SSP,* the following policy, standards and guides were used:

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- GPO Directive 825.33A, Information Technology (IT) Security Program Statement of Policy

The previous IV&V report was delivered on 15 April 2008 and was conducted on the initial SSP. The initial SSP did not detail any security controls in accordance with NIST SP 800-53. Since this time, it is apparent that a positive effort to include relevant security controls has been made and the current SSP is a greatly improved document. While this is

an improvement, the IV&V findings suggest that the current *GPO FDsys SSP* still does not adequately detail the security controls in place, or those planned to be in place for the protection of the confidentiality, integrity, and availability of the systems data and associated resources.

3. Summary of Anomalies and Resolutions

No anomaly reports were written as a result of this task.

4. Assessment of Quality

The task assessed the *GPO FDsys SSP* and the System Design Document to determine if the content of the document provided an adequate security strategy. Based on this assessment, IV&V has drawn the following conclusions.

- The SDD appears to be a comprehensive system level document, but lacks some security architecture details. It is unclear from the diagram (figure 11.2-1) what the data flow is from external interfaces. Two firewalls are depicted on the hardware diagram, but no detailed information as to the type of firewall, make or model is included. It is understood that these may not be part of the certification boundary, but information regarding these devices will be necessary to determine the level of risk exposed to FDsys.

- Assuming a December 2008 deployment, the program may not currently have the resources with sufficient time to complete the *GPO FDsys SSP*.

- The *GPO FDsys SSP* has had much of the detailed functional data removed as recommended in the previous report, but still does not provide an adequate description of the security controls either in place, or planned for FDsys. The Management, Operational and Technical control headers have been included and some controls have been adequately answered. There are however a considerable number of controls that have either not been answered, or lack sufficient detail. This system has been classified as a *high-impact* system [4]and as a result, there are numerous control enhancements that must be included in the design of FDsys.

- The last SSP review that was conducted on 15 April, noted that the SSP version was 2.1. The latest version (12 September) is listed as 1.0. The document version control now starts at 0.9, with no mention of the previous versions of this document.

[4] The potential impact of a system is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

- The *GPO FDsys SSP* still does not identify the Authorizing Official, Certification Authority, or the Information System Security Officer. It is worthy to note that as FDsys has been classed as a *high-impact* system, the Certification Authority/Agent will need to be an independent third-party with no perceived or actual connection to the system.

- It is still unclear from the *GPO FDsys SSP* what the exact boundary of the system is. There is mention of several internal and external connections, but the SSP does not detail if any of these are part of their boundary and if not, if there are currently any Memorandum of Agreements in place.

- The general description of this system in the SSP is unclear and somewhat confusing. There does not need to be a lengthy technical description of the system, as references to the System Design documents can be made, there does however need to be a high level functional description of what the system is, its function, users and when it is planned for production.

- The SSP's main function is to describe the baseline security controls in place, or intended to be in place once the system is operational. The current SSP is difficult to decipher when trying to establish if all controls have been met. When writing statements to satisfy a particular control, it is strongly advised to list that control number and any required control enhancements.

Please see **Attachments** at the end of this report for a detailed list of comments against the *GPO FDsys Systems Security Plan (SSP)*.

5. Identification and Assessment of Technical and Management Risks

The above results create the following potential risks:

- The confidentiality, integrity and availability protection of FDsys is critical for successful operational purposes, regulatory compliance and public confidence. The purpose of the *GPO FDsys SSP* is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. This system has been categorized as a *high-impact* system in accordance with FIPS 199. As a result there are a number of control enhancements that must be addressed above the normal baseline controls. If not adequately answered, it would likely lead to a Denial of Authority To Operate (DATO) from the Authorizing Official.

- The *GPO FDsys SSP* fails to clearly and concisely provide sufficient detail for the Certification Authority and the Authorizing Official to base their initial acceptance and agreement of the security posture and residual risk associated with FDsys. Failure to clearly define the complete system architecture and associated security controls puts the system receiving a final Approval To Operate (ATO) in

jeopardy and therefore delays the operational deployment to the GPO stakeholders, and the public.

6. Recommendations

IV&V recommends the following:

1. GPO FDsys PMO follows the NIST SP 800-37 for a successful process in which to ensure the system receives an ATO. The C&A process is a team process and clear responsibilities need to be documented.

Management's Response. Concur. The C&A process, when it is performed for the FDsys system, will use a team oriented approach, and the roles and responsibilities of the parties will be documented. The complete text of management's response is in Appendix B.

Evaluation of Management's Response. Management's proposed actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are verified by the IV&V team.

2. Although the majority of the functional description in the original *GPO FDsys SSP* has been removed, there still needs to be a clearer, more detailed version of the system description, users, information flow, dependencies, security requirements, and security features.

Management's Response. Concur. IT&S agrees to enhance the document to address these recommendations (see Appendix B).

Evaluation of Management's Response. Management's proposed actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are verified by the IV&V team.

3. The NIST SP 800-53 should be used extensively as a guide to establish the required baseline security controls *GPO FDsys* will need to incorporate, or accept the risk. The document should list each control number and title and then a response as to how the control is implemented, or planned to be implemented should follow.

Management's Response. Concur. The FDsys SSP already lists HIGH NIST-53A security controls as required. The GPO Risk Assessment template, which complies with NIST SP 800-26, will provide the recommended information. The FDsys Risk

Assessment is in the process of creation now and is planned for completion in December 2008 to meet the requirements of the GPO C&A process (see Appendix B).

Evaluation of Management's Response. Management's proposed actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are verified by the IV&V team.

4. Any connection to systems outside of FDsys needs to be thoroughly documented. For any connections that are made to other systems inside GPO, there should be a Memorandum of Understanding/Agreement. For any connections to systems outside of GPO, there should be an Interconnection Security Agreement (ISA).

Management's Response. Concur. MOU/MOAs will be prepared for the general support systems and major applications that FDsys interfaces to within GPO. An ISA will be completed for the ILS, which is the only external system interface. IT&S plans to complete these activities in December 2008, to support the C&A process for FDsys (see Appendix B).

Evaluation of Management's Response. Management's proposed actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are verified by the IV&V team.

5. Update the SSP to respond to the detailed comments provided in the Attachment to this report.

Management's Response. Concur. IT&S will provide a detailed matrix of intended updates to the FDsys SSP. IT&S plans to provide that to the OIG in December 2008, and to update the SSP accordingly (see Appendix B).

Evaluation of Management's Response. Management's proposed actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are verified by the IV&V team.

Appendix A.
IV&V Document Review Comments

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
1	N/A	General	This system has been classified as Sensitive But Unclassified (SBU); therefore correct document labeling should be followed in accordance with relevant GPO policy. Recommend the document should be labeled, "For Official Use Only (FOUO)" on every page and correct handling instructions added to the front cover.
2	2	Signature Page	It is unclear who is responsible for the system, based on the roles currently listed on the SSP signature page. The signature page is still missing the signature line for the Authorizing Official (AO), Certification Authority/Agent (CA), Information System Security Officer (ISSO), and the System Owner. The signature page currently has six people listed and some of these are probably the identified missing signatories (e.g., the CIO is probably the AO, but looks like the CIO could also be the system owner?), but is not clear.
3	3	Document Version Control	The version control on this SSP starts at 0.9. The previous records depicting what was changed in the SSP needs to be kept as a record of change.
4	6	1.1 -1.5 (System Identification)	This section is greatly improved from the last review, however the AO and CA is still missing and are key members of the Certification and Accreditation (C&A) management team.
5	8	1.6 (System Purpose and Description)	The general description of FDsys is still disconnected and somewhat confusing. This section should be a very high explanation of what the system purpose, capabilities, users,

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			and information dataflow. This section should be written for a non-technical reader, with no prior knowledge of the system. In the prior report the following example was given: *"GPO's Future Digital System (FDsys) system is currently under development and does not currently store, or process government data apart from test data. When operational it will reside on the GPO communications network and will be a world-class system for managing official Government content. FDsys will automate the collection and dissemination of electronic information from all three branches of government. The system will verify and track versions, assure authenticity, preserve content, and provide permanent public access. The system will be Rules based, Policy neutral, Modular and adaptable. The information contained within the system will be permanently available in electronic format, authenticated and versioned, accessible for Web searching, viewing, downloading and printing, and available for conventional and on-demand printing". FDsys will be built to include all known Federal Government publications falling within the scope of GPO's Federal Depository Library Program (FDLP), including text, graphics, video, audio, numeric, and other emerging forms of content."*
6	8	1.6 (System Purpose and Description)	The accreditation boundary is still unclear for the system. Recommend adding a section that explains what the accreditation boundary is limited to.

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			An example may include: "The accreditation boundary is limited to the FDsys Major Application which includes firewalls, switches, workstations, printers, web servers, file servers, and other devices connected to the network as identified in the hardware equipment list in Appendix A". Recommend moving the system diagram in section 5.1 and placing it into the accreditation boundary section. This will be useful when explaining the accreditation boundary and should be easier for the reader to follow. The boundary should match both the diagram and the hardware list. There are a couple of firewalls depicted in the diagram and if they are in the accreditation boundary then explain and if not, also need to explain that they are part of another system and whether that system has a current Approval To Operate.
7	10	1.6.4 (System Interconnection/Information Sharing)	Internal interfaces have been listed as the Integrated Library System (ILS) and the Enterprise Service Bus (ESB). The section states that these are components of the FDsys. It is unclear if these components are part of the FDsys accreditation boundary, or covered under a separate System Security Plan (SSP). The external interfaces need to be explained in more detail. • How do these external interfaces communicate with the system and why? • If they are another separate

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			system, is there a Memorandum of Agreement or similar in place? • Are the other system currently accredited
8	15-32	Management, Operational and Technical Controls	These sections are currently difficult to assess if all base-line controls have been included at the correct high watermark. Recommend that each sub section has the NIST SP 800-53 control number listed and the control name. This will make it easier for the certifier and also make it easier for the author to ensure that no controls are missed. An example would be: **2.1 Risk Assessment (RA)** **2.1.1 Risk Assessment Policy and Procedures (RA-1)**
9	16	2.1 (Risk Assessment and Risk Management)	This section should cover security controls RA-1 thru RA-5(1)(2). The description references GPO directive 825.33A, but does not state if an actual risk assessment has been performed at this stage. There are some general risk descriptions and threat descriptions, but there are no risk levels (high, medium, low), or likelihood associated with them. Recommend utilizing the NIST SP 800-30 to assist with this section.
10	16-17	2.1 (Risk Assessment and Risk Management)	Security control RA-5 (Vulnerability Scanning) has not been answered in the SSP. As this is a high system, control enhancements RA-5(1) and RA-5(2) also need to be addressed.
11	18-24	2.3 thru 2.4.5	These sections are discussing the security controls for Planning (PL). There are some controls missing that should either be in place, or intended to be in place for this system. There is

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			currently no mention of a Privacy Impact Assessment (PIA) being completed as an example.
12	24-25	2.5 (Certification and Accreditation)	Need to ensure that all CA security controls are answered. This section is very generic and needs to include detail as to how the system will meet these controls. Some details to include are: • What is the frequency of the security assessments and when is the first one scheduled? • What are the risk considerations from external connections? • Has an independent certifier been identified for the system? • Has a Plan of Action and Milestones (POA&M) document been created yet? There could already be open items discovered from the risk assessment. • Has the Authorizing Official been identified? • How will continuous monitoring be put in place for this system and what activities are planned to be included?
13	N/A	2 (Management controls)	The System and Services Acquisition (SA) controls have not been included within this section.
14	25	3.1 (Personnel Security Controls)	The following controls are missing detail in this section: • Personnel Security Policy and Procedures (PS-1). Is there a current GPO policy that covers this control? • Position Categorization (PS-2).

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			Are personnel assigned a risk categorization and if so what are they? • Third-Party Personnel Security (PS-7). Need to discuss how the agency meets this control.
15	26	3.2 (Physical and Environmental Protection Controls)	This section needs to include more detail regarding PE-1 thru PE-19 security controls. Items to be addressed include: • Physical access to the system. Where is/will the system be located, is it in a server room, air conditioned etc? • How is the facility monitored. Are there cameras, alarms, armed guards? • Are there real-time intrusion alarms (PE-6(1) and PE-6(2))? • Are visitor access records maintained and do they meet the requirements of security control PE-8, PE-8(1), and PE-8(2)? • How does the organization protect power equipment/cabling from damage or destruction? • Discuss emergency shutoff for the system • Discuss emergency power for both short term (uninterruptible) and long term alternate power supply • Discuss emergency lighting • Discuss fire protection, including automatic detection and notification, and fire suppression devices

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			• Discuss the temperature and humidity controls for the system • How does the system protect against water damage? • Discuss how delivery and removal of IT equipment is achieved • Is there an alternate work site? • Explain information leakage protection
16	27	3.3 (Production Input / Output Controls)	This section appears to be relating to Media protection (MP) controls. There needs to be greater detail explaining the GPO media protection policy/procedures, access, labeling, storage, transportation, and finally sanitization and disposal.
17	27	3.4 (Incident Response Capability)	It is OK to reference the GPO Computer Security incident Response Team (CSIRT) procedure document in this section, but it is strongly advised the Information Assurance Officer (IAO) for FDsys ensures that the document and GPO CSIRT procedures meet all the controls relating to IR-1 thru IR-7, paying particular attention to the enhancement requirements.
18	28-29	3.7 (Security Awareness and Training)	This section provides a good overview of user awareness training, but does not have any information to support the following controls under Awareness and Training (AT): • Security Training (AT-3). Need to discuss how security staff are identified and receive specialized training (NIST SP 800-50) • Security Training Records

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			(AT-4). Need to discuss how training records are kept and how you monitor users training needs/requirements
19	N/A	3 (Operational Controls)	There are no Configuration Management (CM) controls listed in this section. The following need to be addressed as either in-place, planned, or inherited: • Configuration Management Policy and Procedures (CM-1) • Baseline Configuration (CM-2) (1) (2) • Configuration Change Control (CM-3) (1) • Monitoring Configuration Changes (CM-4) • Access Restriction for Change (CM-5) (1) • Configuration Settings (CM-6) (1) • Least Functionality (CM-7) (1) • Information System Component Inventory (CM-8) (1) (2)
20	N/A	3 (Operational Controls)	There are no Contingency Planning (CP) controls listed in this section. The following need to be addressed as either in-place, planned, or inherited: • Contingency Planning Policy and Procedures (CP-1) • Contingency Plan (CP-2) (1) (2) • Contingency Training (CP-3) (1) • Contingency Plan Testing and Exercises (CP-4) (1) (2) • Contingency Plan Update (CP-5)

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			• Alternate Storage Site (CP-6) (1) (2) (3) • Alternate Processing Site (CP-7) (1) (2) (3) (4) • Telecommunications Services (CP-8) (1) (2) (3) (4) • Information System Backup (CP-9) (1) (2) (3) (4) • Information System Recovery and Reconstitution (CP-10) (1)
21	N/A	3 (Operational Controls)	There are no Maintenance (MA) controls listed in this section. The following need to be addressed as either in-place, planned, or inherited: • System Maintenance Policy and Procedures (MA-1) • Controlled Maintenance (MA-2) (1) (2) • Maintenance Tools (MA-3) (1) (2) (3) • Remote Maintenance (MA-4) (1) (2) (3) • Maintenance Personnel (MA-5) • Timely Maintenance (MA-6)
22	N/A	3 (Operational Controls)	There are no System and Information Integrity (SI) controls listed in this section. The following need to be addressed as either in-place, planned, or inherited: • System and Information Integrity Policy and Procedures (SI-1) • Flaw Remediation (SI-2) (1) (2) • Malicious Code (SI-3) (1) (2) • Information System Monitoring Tools and Techniques (SI-4) (2) (4) (5) • Security Alerts and Advisories

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			(SI-5) (1) • Security Functionality Verification (SI-6) • Software and Information Integrity (SI-7) (1) (2) • Spam Protection (SI-8) (1) • Information Input restrictions (SI-9) • Information Accuracy, Completeness, Validity, and Authenticity (SI-10) • Error Handling (SI-11) • Information Output Handling and Retention (SI-12)
23	29	4.1.1 (Inactive User IDs)	The paragraph states that inactive user accounts are disabled after a specific time (e.g., six or twelve months) in accordance with GPO Directive 825.33A. There needs to be specifics and not examples. The 825.33A does not currently specify a inactive time frame.
24	29	4.1.2 (Authentication)	As FDsys is a high system, there is a need for multi factor identification to meet the IA-2 control enhancements 2 and 3. This needs to be at the level 4 when consulting the NIST SP 800-63. This section discusses internal users, but what about public credentials? Will the system have digital certificates and/or session based cookies etc?
25	29-32	4 (Technical Controls)	There is a large portion of the Access Controls (AC) deficient. Most of the lower AC controls (AC-1 thru AC-7) have been addressed, but the remaining controls (AC-8 thru AC-20) need to be documented. Particular attention needs to be made to the

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			control enhancements as this is a high system.
26	32	4.7 (Audit Trails)	This section is inadequate to answer the Audit and Accountability (AU) controls. Items that need to be addressed include: • Is there a GPO policy that addresses Audit Trails (825.33A)? • What are auditable events for FDsys? • How often are these auditable events reviewed? • Are sufficient audit records kept that can capture sufficient information to establish what events occurred? • Are the audit records centrally managed…CCIRT? • Is there sufficient audit storage allocated for FDsys? • Does FDsys alert appropriate staff in the event of an audit processing failure and is it a real time alert (needed for a high system)? • How often does the organization review and analyze the audit logs? • Does FDsys provide audit reduction and report generation tools that support after-the-fact investigations of security incidents without altering original audit records?
27	N/A	4 (Technical Controls)	The technical controls for System and Communications Protection (SC) are missing from this section. Need to discuss the current, or planned security

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
			controls for SC-1 thru SC-23, including all required enhancements for a high system.
28	33	5.1 (Appendix A – Equipment List)	The network diagram shows two firewalls, four Cisco switches, and two load balancers that are not accounted for on the hardware list. There is also a Digital Application Server, a SAN, and a NAS storage unit that is listed on the hardware list, but not on the diagram.
	Miscellaneous Editorial Comments		
1	18	2.2 (Review of Security Controls)	Change reference from NIST SP 800-53A, to NIST SP 800-53. Also recommend that this section is removed and placed as an opening statement for the main section 2. It makes a good opening remark, but does not really fit in its current section.
2	18-24	2.3 thru 2.4.5	These sections are discussing the security controls for Planning (PL). Recommend reordering the sections so they line up with the controls as follows: 2.3 Planning (PL) 2.3.1 Security Planning Policy and Procedures (PL-1) 2.3.2 System Security Plan (PL-2) 2.3.3 System Security Plan Update (PL-3) 2.3.4 Rules of Behavior (PL-4) 2.3.5 Privacy Impact Assessment (PL-5) 2.3.6 Security-Related Activity Planning (PL-6) Recommend using this format for each control group/family.

Document Reviewed: GPO FDsys System Security Plan (dated 12 September 2008) Date of Review Comments: 27 October 2008 Conducted by: Mark LoGalbo			
Item #	**Page #**	**Para/Section #**	**Comments**
3	13	1.6.5 (Applicable Laws or Regulations Affecting the System)	Recommend updating this section. Some NIST references are out of date, or no longer used as follows: • SP 800-53 is now Revision 2, December 2007 • SP 800-53A is no longer draft and is June 2008 • SP 800-61 is now Revision 1, March 2008 • SP 800-64 is now Revision 2, October 2008 • SP 800-92 is no longer draft and is September 2006 • NIST Pubs. 31, 73, 83, and 102 are no longer used

IT&S Response:
Draft OIG IV&V Assessment Report on FDsys

December 10, 2008

Introduction

The Office of the Inspector General (OIG) issued a Draft Report on November 25, 2008, concerning an Independent Verification and Validation (IV&V) of the FDsys System Security Plan (SSP).

This document is the GPO Information Technology and Systems (IT&S) response to the OIG recommendations contained in that Draft Assessment Report.

OIG Recommendations and IT&S Response

The OIG IV&V recommendations and IT&S responses to each recommendation are listed below.

OIG Recommendation #1:

The IV&V recommends that the GPO FDsys PMO follows the NIST SP 800-37 for a successful process in which to ensure the system receives an ATO. The C&A process is a team process and clear responsibilities need to be documented.

IT&S Response:

IT&S agrees that SP 800-37 provides a reasonable framework for a C&A process that complies with GPO IT Security Policy requirements and GPO policy, and further, that the C&A process is a team oriented process. The C&A process, when it is performed for the FDsys system, will use a team oriented approach, and the roles and responsibilities of the parties will be documented.

OIG Recommendation #2:

The IV&V recommends that although the majority of the functional description in the original GPO FDsys SSP has been removed, there still needs to be a clearer, more detailed version of the system description, users, information flow, dependencies, security requirements and security features.

IT&S Response:

1

IT&S agrees to enhance the document to address these recommendations.

OIG Recommendation #3:

The IV&V recommends that the NIST SP 800-53 should be used extensively as a guide to establish the required baseline security controls GPO FDsys will need to incorporate, or accept the risk. The document should list each control number and title and then a response as to how the control is implemented, or planned to be implemented should follow.

IT&S Response:

The FDsys SSP already lists all HIGH NIST 800-53A security controls as required for the control baseline (this is contained in Appendix A of the SSP). Thus that element of the recommendation is already adequately covered in the FDsys SSP. The GPO Risk Assessment template, which complies with NIST SP 800-26, will provide the recommended information, in accordance with the GPO IT Security Policy (GPO Directive 825.33A) and GPO SDLC, and is the GPO document that will list the recommended state of control implementation or risk acceptance. The Risk Assessment for FDsys is in the process of creation now and is planned for completion in December 2008, to meet the requirements of the GPO C&A process.

OIG Recommendation #4:

The IV&V recommends that any connections to systems outside of FDsys need to be thoroughly documented. For any connections that are made to other systems inside GPO, there should be a Memorandum of Understanding/Agreement. For any connections to systems outside of GPO, there should be an Interconnection Security Agreement (ISA).

IT&S Response:

The GPO IT Security Policy (GPO Directive 825.33A) does not require MOU/MOA's between GPO systems or major applications. IT&S believes this extra level of documentation may be worthwhile and will plan to do for the GSS and major applications that FDsys interfaces to within GPO. IT&S agrees that ISA's should be performed for external system interfaces, outside of GPO, and will complete ISA's for this purpose. The ILS is the only system interface of that type for FDsys at this time. IT&S plans to complete these activities in December 2008, to support the C&A process for FDsys.

OIG Recommendation #5:

The IV&V recommends that the SSP be updated to respond to the detailed comments provided in the Attachment to the Assessment report.

IT&S Response:

2

IT&S will assess the detailed comments and provide a detailed matrix of intended updates to the FDsys SSP. IT&S plans to provide that to the OIG in December 2008, and to update the SSP accordingly.

3

Appendix C. Status of Recommendations

Recommendation No.	Resolved	Unresolved	Open/ECD*	Closed
1	X		TBD	
2	X		TBD	
3	X		12/31/08	
4	X		12/31/08	
5	X		12/31/08	

*Estimated Completion Date

Appendix D. Report Distribution

Public Printer
Chief of Staff
General Counsel
Chief Acquisition Officer
Chief Management Officer
Chief Technology Officer