U.S. GOVERNMENT PRINTING OFFICE

KEEPING AMERICA INFORMED

ASSESSMENT REPORT 09-07

FEDERAL DIGITAL SYSTEM (FDSYS) INDEPENDENT VERIFICATION AND VALIDATION (IV&V) – SIXTH QUARTER REPORT ON RISK MANAGEMENT, ISSUES, AND TRACEABILITY

March 20, 2009

OFFICE OF INSPECTOR GENERAL

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

Memorandum

OFFICE OF THE INSPECTOR GENERAL

DATE: March 20, 2009

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

SUBJECT: Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Sixth Quarter Report on Risk Management, Issues, and Traceability
Report Number 09-07

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. American Systems is required by the contract to issue to the OIG a quarterly Risk Management, Issues, and Traceability Report, providing observations and recommendations on the program's technical, schedule, and cost risks as well as requirements traceability of those risks and the effectiveness of the program management processes in controlling risk avoidance. Additionally, at the end of each FDsys release phase, American Systems is required to issue a release phase summary program management report that addresses delivery of the technical baseline per the FDsys Master Program Schedule and the risks that affect the schedule's critical path to the next phase.

The enclosed report is American Systems' quarterly report for the period October 1, 2008 to January 9, 2009. Section 7 of the report contains four recommendations designed to improve current and future FDsys project efforts. Management concurred with three of the recommendations and partially concurred with one. We consider the actions taken

---

[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.

and proposed by management responsive to each of the four recommendations. The recommendations are resolved and will remain open for reporting purposes until IV&V has verified that agreed upon actions have been taken by management. The status of each recommendation upon issuance of this report is included in Appendix B. The final report distribution is in Appendix C.

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.

Kevin J. Carson
Assistant Inspector General for Audits and Inspections

Attachment

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

ATTACHMENT

IV&V RISK MANAGEMENT, ISSUES, AND TRACEABILITY REPORT	
TO:	Brent Melson, COTR
FROM:	IV&V, Jon Valett
IV&V OF:	Quarterly Report (Final – Document Number 01-054)
SUBJECT:	October – December 2008 Quarterly Report
DATE:	January 15, 2009
CC:	Dan Rose, David Harold, John Best, Chris Parr, Shawn O'Rourke

This report presents the critical technical, schedule, and cost risks identified for the Government Printing Office (GPO) Federal Digital System (FDsys) Program. Specifically, it provides a high-level overview of the key risks and issues that IV&V has identified within the last quarter. This report also addresses IV&V assessments covering FDsys security and, state of program activities required for deployment, that were performed over this same time period.

This is the sixth IV&V quarterly report and covers the period from October 1, 2008 to January 9, 2009. It includes information taken from the following:

- IV&V Quick Look Report, *Evaluation of the State of the FDsys Program Activities to be Completed Prior to Deployment*, December 19, 2008;
- IV&V Task Report, *FDsys Security Analysis*, November 3, 2008;
- IV&V Documentation Reviews[4]; and
- IV&V observation of testing.

Over the last quarter several areas of the program made significant progress. Key observations over this period are as follows:

- The FDsys hardware design and installation group has documented the FDsys development, production, and test instances. Documentation includes the FDsys Site Preparation and Installation Plan, individual instance layouts, drawings, and parts lists. Additionally, this group maintains an Infrastructure Schedule and To-Do List that are updated frequently.
- A number of program related documents have been newly created while others have been updated. Peer reviews for some of these documents have occurred and some, e.g., the FDsys Site Preparation and Installation Plan, have been reviewed and approved by the Configuration Control Board.

[4] Note that the IV&V comments found against the following FDsys documents were provided to the FDsys Program Director to facilitate the document review process and were not part of a formal IV&V report delivery. IV&V reviewed the: FDsys R1C2 to ILS ICD; FDsys Release 1C2 Transition to Operations Plan; FDsys Data Migration Plan; FDsys Site Preparation and Installation Plan; FDsys Acceptance and Beta Test Plan Release 1 C.2; FDsys Documentation and Training Plan; and FDsys Performance Test Plan.

- An updated Documentation and Training Plan has been developed; however, individual training plans for the various user communities are still in development. Additionally, training for submission has not occurred and the training materials are incomplete.
- Software development for all three drops of Release R1C2 was completed. System integration has been problematic. Numerous difficulties have been encountered, especially related to the content management system (Documentum). These problems have impacted the testing and training efforts and the overall schedule for deployment.

1. Technical Risks Identified

During the last quarter several technical risks were identified:

- Testing during the course of any Information Technology (IT) program is critical to the successful deployment and operation of the proposed system. There are often levels of testing that should be performed on the proposed system. Each level of testing often builds upon the previous level of testing, e.g., software integration testing builds upon the code and unit testing that was performed. In this way, errors at the lowest levels can be discovered and corrected; increasing the likelihood of a more stable system. The FDsys program is implementing System Integration Testing (SIT); User Acceptance Testing (UAT), Beta Testing, Performance Testing, and Security Testing and Evaluation (ST&E).

  SIT is then used to integrate the various functional entities and integrate them with other system components including hardware. During this period, experienced testers familiar with the system, repeatedly run tests and begin to formally document problems that are discovered. Once stable, i.e., few system errors are produced, the system is often turned over to representatives of the user community to run tests different from SIT.

  UAT is testing that is performed by representatives of the user community in order for stakeholders to exercise the system and discover problems that could prevent them from performing in their roles, i.e., errors that prevent the user community from performing business processing.

  Beta Testing for FDsys is essentially the last testing to be performed prior to deployment. All known problems have been fixed and incorporated into the deployment build. Errors found here must be fixed for deployment to occur.

  Performance testing is used to test the proposed system to ensure that the system runs as expected under load conditions, i.e., the system must be able to support a peak number of concurrent users without degradation of performance. Being able to accomplish this ensures that the system will be able to support the projected number of users without slowing down or going down.

ST&E is performed once all other testing has been successfully executed. ST&E is performed as required and tests to ensure that the safeguards for the system are in place and functioning as expected. ST&E is required before Certification and Accreditation of the FDsys can occur.

The risks for testing include:

- SIT continues to be executed. Numerous errors have been found and are being documented on Program Tracking Reports (PTRs). Drop 1, Drop 2, and Drop 3 testing results received by IV&V to-date, show that numerous tests have failed, e.g., in Drop 1, 61 of the 114 system requirements (RDs) "Passed" (53.5%) and 53 of the 114 system requirements (RDs) "Failed" (46.5%). Failure to complete SIT threatens the integrity and quality of the FDsys.
- While some UAT has been performed, this testing has failed to complete and the limited testing that was performed yielded errors. Lack of sufficient UAT increases the risk that the needs of the user community will not be met and increases the likelihood of user dissatisfaction.
- Beta testing has begun. The objective of the Beta testing is to allow the user community at large to run tests which reflect their business processes. Finding problems at this juncture in the program risks not being able to provide the fix in time for deployment of FDsys thus the system may lack certain functionality.
- Limited performance testing has been performed. While the program has produced a Performance Test Plan, the plan itself is a first attempt, lacking critical information. The program is attempting to define and understand what constitutes performance based testing. Lack of performance testing increases the risk that FDsys will be unable to meet the load and availability requirements for the FDsys user community.
- Security testing is incomplete. Without sufficient security testing, the program risks deploying a vulnerable system.

- The system is unstable because numerous Severity 1 and 2 problems have been found and remain open; affecting the quality and integrity of the FDsys system. These problems are documented using PTRs. In accordance with the provisions of the FDsys Master Test Plan, PTRs are categorized based upon their severity[5]. The FDsys program has stated that all Severity 1 PTRs must be closed prior to deployment. This is not consistent with industry best practice, which is that all Severity 1 and Severity 2 PTRs should be closed prior to deployment;
- The Operations and support effort is undeveloped and unplanned. Currently there is no backup for the production system; system maintenance schedules have not

[5] The FDsys Master Test Plan, version 2.0, defines: Severity 1 - Prevents the accomplishment of an operational or mission-essential capability specified by the requirements. Severity 2-Adversely affects the accomplishment of an operational or mission-essential capability specified by the requirements so as to degrade performance and no alternative work-around solution is known.

been developed; system component sparing[6] has not been planned; formal acceptance of FDsys by GPO IT Operations Management is in process; and operations manuals, though delivered to GPO IT Operations Management, is still in the process of being reviewed;

- Training materials are still in development and training is incomplete. Additionally, the system is still unstable and conducting training in this environment is a risk;
- The integration of the Integrated Library System (ILS) interface is incomplete. The impact of FDsys not being able to interface with ILS results in the inability to maintain consistent catalogs, i.e., FDsys needs to integrate with the ILS for bibliographic information synchronization, to keep both systems up to date about the content available from GPO.
- IV&V reviewed numerous FDsys artifacts that have been generated in support of the FDsys program. In an effort to facilitate and foster communication between IV&V and the program, and with the approval of the OIG, IV&V forwarded the results of these reviews to the FDsys Program Director for dissemination to the respective document owners/authors for review and update using the IV&V comments as appropriate. The results of IV&V review re-affirmed what was reported by IV&V in the previous quarterly, i.e., that the document peer review process is inefficient; little or no Quality Assurance is being performed on program documents; and the document approval process is less than desirable. The impact of incomplete or out-of-date documentation can have a negative effect on the system maintenance effort due to insufficient system information required to respond to user questions/issues; the inability to trace the design from requirements to test; and the inability to begin the development of Release 1.C3 with an established baseline.

2. Schedule Risks Identified

Schedule risks incurred by technical risks previously presented are provided below.

- The deployment date of late 2008 has not been met. A January 2009 deployment is now forecast, though the system may lack all of the original functionality that was once planned.
- Incomplete areas of testing and the lack of a stable system jeopardize the January 2009 deployment.
- Conducting User Training the week before deployment is to occur, on an unstable system, threatens the January 2009 deployment. The risk is that if significant problems are found at this late date, the deployment is threatened.
- Incomplete user operations documentation and lack of a documented Help Desk support strategy jeopardize the January 2009 deployment, as well as making

[6] Sparing is the ability of the program to procure and have at the ready, backup components that can be used in the event of a component failure. There are a number of sparing strategies that can be used to determine the critical components that must be available should failures occur.

maintenance of the system more difficult, even if the January 2009 deployment date is achieved.

3. Cost Risks Identified

There are inherent cost risks associated with the technical and schedule risks. Program cost has been presented during Program Review meetings with the indication that 2009 funding has been approved; however, there is no correlation between the cost to-date and performance (e.g., amount of total software completed). Additionally, status against the IMS is no longer being performed nor is the IMS being updated.

- By their nature, cost risks are directly correlated with schedule risks. Any schedule increase generally results in additional costs.

4. Evaluation of the State of the FDsys Program Activities to be Completed Prior to Deployment

IV&V reviewed the state of program activities that have been identified by the Federal Digital System (FDsys) Program Management Office (PMO) as being required to deploy FDsys in early January 2009. The results of that assessment are included in report # 09-05, located on the Office of the Inspector General (OIG) web page, http://www.gpo.gov/oig/oa_reports.htm.

5. FDsys Security Analysis

IV&V task assessed the *GPO FDsys SSP* and the *FDsys System Design Document (SDD)* to determine if the content of the document provided an adequate security strategy. The results of that assessment are included in report # 09-04, located on the OIG web page, http://www.gpo.gov/oig/oa_reports.htm.

6. IV&V Test Witnessing

IV&V witnessed SIT on a number of occasions. During these sessions, search, Documentum, and Section 508[7] compliance testing was witnessed. As test results are provided from the FDsys program, IV&V will develop a separate analysis of FDsys testing.

[7] Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

7. Recommendations

The IV&V recommendations are provided below. Recommendations previously included in the IV&V Task Reports during this quarter can be found in the reports that were issued by the OIG (as indicated above).

IV&V recommends that:

1. The FDsys Program ensure that the system is completely tested for functionality, performance, and security prior to deployment.

Management's Response. Concur. The PMO implemented daily tracking reports of PTRs to keep close track of their performance in closing out known issues with the performance of the system. Additionally, they partitioned the system into two major sections for this release; the search and access section, and the submission section. By doing so, they have been able to more clearly track the performance in each of these sections and enable each section separately.

Evaluation of Management's Response. The actions proposed and taken by management are responsive to the recommendation. Follow-up discussions with management regarding their response determined that they are in the process of providing American Systems with testing documentation. American Systems will review the adequacy of testing once the documentation is received. This recommendation is resolved, but will remain undispositioned and open for reporting purposes pending review of the testing documentation by American Systems.

2. FDsys should be stable before security testing, i.e., Certification and Accreditation (C&A), is performed.

Management's Response. Concur. Security testing was completed and an approval to operate was issued on January 15th, which the Chief Information Officer signed.

Evaluation of Management's Response. The actions taken by management are responsive to the recommendation. Security testing (C&A) is currently being reviewed by American Systems. This recommendation is resolved, but will remain undispositioned and open for reporting purposes pending review of the security testing by American Systems.

3. The system should not be deployed until all Severity 1 and Severity 2 PTRs have been corrected and tested.

Management's Response. Partially Concur. The PMO chose to address and close all Severity Level 1 PTRs. They determined that closing Severity level 1 PTRs would provide a very stable and reliable system. FDsys will be in a public beta configuration for an extended period of time while the remaining collections in GPO Access are migrated into the system. GPO Access will remain the system of record until the full

migration is completed. This time period will allow the FDsys team to continue to monitor the overall performance of FDsys and allow them to collect and respond to end user comments.

Evaluation of Management's Response. The actions proposed and taken by management are responsive to the recommendation. American Systems agrees with management's response given the program's approach to PTRs. The FDsys program has used Severity 1 PTRs to include most any problem that would either cause the system to fail or cause business processing to be incorrect. Given this definition of Severity 1 PTRs, the system should be stable and reliable enough to release when they are closed. Further, given the extended Beta configuration, the program may have additional time to resolve Severity 2 PTRs. American Systems will continue to monitor the status of PTRs. This recommendation is resolved, but will remain undispostioned and open for reporting purposes pending American System's ongoing review of the PTRs.

4. Required documentation for the operations and support effort be completed and include identification of sparing strategy to be implemented.

Management's Response. Concur. FDsys is transitioning to IT Operations. IT Operations is now beginning to use existing documentation. The extended beta period for FDsys will allow the required operational expertise to be developed within the GPO IT Operations group.

Evaluation of Management's Response. The actions proposed and taken by management are responsive to the recommendation. This recommendation is resolved, but will remain undispositioned and open for reporting purposes pending review of the adequacy of the documentation by American Systems.

Appendix A. Management's Response

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

MEMORANDUM

DATE: January 30, 2009

REPLY TO ATTN OF: Chief Information Officer

SUBJECT: Quarterly Report (Document Number 01-054) – October 1, 2008 through January 9, 2009

TO: Assistant Inspector General for Audits and Inspections

Thank you for the opportunity to respond to the recent QUARTERLY REPORT (01-054) regarding GPO's Federal Digital System (FDsys).

The program leadership team and I agree with some of the IV&V observations and recommendations. Overall, we remain confident that we continue to take the necessary steps to ensure that FDsys is delivered successfully.

This response deals primarily with the recommendations as presented in the document.

Recommendations:

Recommendation#1: Ensure the FDsys program that the system is completely tested for functionality, performance, and security prior to deployment.

The team completely agrees with this. We have implemented daily tracking reports of PTRs to keep a close track at our performance in closing out known issues with the performance of the system. Additionally, we have partitioned the system into two major sections for this release; the search and access section, and the submission section. By doing so, we have been able to more clearly track the performance in each of these sections and enable each section separately, which is the approach we settled on for the first release.

The first aspect of FDsys to be launched was the search and access element. We completely closed all Severity Level 1 issues, completed a very successful beta, and complete the security screening.

Recommendation #2: FDsys should be stable before security testing (C&A) is performed.

We again agree with this recommendation. Security testing was completed and an approval to operate (ATO) was issued on January 15th, which I signed.

Recommendation #3: The system should not be deployed until all Severity 1 and Severity 2 PTRs have been corrected and tested.

Appendix A

We chose to address and close all Severity Level 1 PTRs. As you know, this is the first major program at GPO to conform to a disciplined project management approach and as such, the team is still developing their skills on categorizing severity levels. As we reviewed the PTRs, it was clear that many were promoted to a high severity level. Through this assessment we determined that closing Severity level 1 PTRs would provide a very stable and reliable system.

Also, please remember that FDsys will be in a public beta configuration for an extended period of time while the remaining collections in GPO Access are migrated into the system. GPO Access will remain the system of record until the full migration is completed. This time period will allow us to continue to monitor the overall performance of FDsys and allow us to collect and respond to end use comments.

Recommendation #4: Required documentation for the operations and support effort be completed and include identification of sparing strategy to be implemented.

FDsys is transitioning to IT Operations. IT Operations is now starting to support the regular data backups for the Test and Production instances. They will be using the documentation that has been developed for the system and in effect accrediting this documentation throughout the transition process. As you know desk reviews work well at reviewing documentation, but the real test is when you use it. Again, the extended beta period for FDsys will allow us to develop the required operational expertise within the GPO IT Operations group.

Additionally, we are now completing plans for the failover instance of FDsys. This will be located at the Alternate Computing Facility (ACF) and is expected to be completed before the final data is migrated into the FDsys, allowing us to confidently decommission GPO Access and make FDsys the system of record.

MICHAEL L. WASH

2

Appendix B. Status of Recommendations

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

*Estimated Completion Date

Appendix C. Report Distribution

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