U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

ASSESSMENT REPORT 09-05

FEDERAL DIGITAL SYSTEM (FDSYS) INDEPENDENT VERIFICATION AND VALIDATION (IV&V) – RELEASE R1C.2 PRE-DEPLOYMENT STATUS REPORT

December 24, 2008

OFFICE OF INSPECTOR GENERAL

GPO 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) – Release R1C.2 Pre-Deployment Status Report
Report Number 09-05

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 1C.[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 1C. One tasking is to evaluate risks prior to the deployment of the first public release of FDsys (Release R1C.2). The FDsys Program Office plans to deploy Release R1C.2 in early January 2009.

The attached report prepared by American Systems provides their view of key risks to program activities that may adversely impact deployment of Release R1C.2. The contents of this report were briefed to the Chief Information Officer on December 18, 2009. Section 4 of the report contains two recommendations designed to address the most significant pre-deployment risks. These recommendations are provided for management's information only. No response is required as these issues have been addressed in previous IV&V reports. However, we urge management to ensure that they are appropriately addressed prior to deployment.

[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.

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

ATTACHMENT

IV&V QUICK LOOK REPORT

TO:	Brent Melson, COTR
FROM:	IV&V, Jon Valett
IV&V OF:	FDsys Program Development (Final - Doc Number 01-051)
SUBJECT:	State of the FDsys Program Activities to be Completed Prior to Deployment
DATE:	December 19, 2008
CC:	Dan Rose, David Harold, John Best, Shawn O'Rourke

1. Description of Task

Independent Verification and Validation (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. This report provides IV&V's delineation of the current issues/problems associated with these activities and a brief abstract describing their impact/consequences on the program. Associated program risks and recommendations are also provided.

IV&V examined the key activities of the FDsys program including code development, testing, requirements, training, and security. For each activity, the IV&V team identified issues that may jeopardize the integrity of the system to be deployed. IV&V then conducted internal meetings to better flesh out each issue and to determine the impact/consequence to the deployment of FDsys. This report is not an attempt to summarize the overall state of the program. Its intent is to identify risks to key program activities that may impact deployment of Release R1C.2 (R1C2) and may impact the development of Release R1C.3 (R1C3). In doing so, risks from previous IV&V reports may be repeated in an attempt to identify the truly critical risks facing the program right now.

Note that the list of activities/issues/consequences is based on the material IV&V has acquired from bi-weekly Risk Review Board meetings; weekly Configuration Control Board meetings; meetings with the FDsys Program Director; and information accessible in Caliber, ClearQuest, and Sharepoint.

2. Findings

While progress is being made on the FDsys program, there are still a number of key activities that remain to be completed as the FDsys program deployment date nears. Not completing the activities have consequences that manifest themselves as risks to deployment and/or deployment of a system with less than optimal functionality; potentially discouraging use of FDsys by the GPO community of users. Note also that these activities are often inter-related and dependent upon successful completion of a predecessor activity, e.g., conduct of User Acceptance Testing (UAT) is dependent upon successful completion of the System Integration and Test (SIT) activity.

At this juncture in the program (mid-December 2008), many of the key dates specified in the Integrated Master Schedule (IMS) have been missed and activities that need to be completed for successful deployment of FDsys are incomplete. These include the items discussed below:

- System integration and stand-up has taken longer than envisioned. This results in less time for testing and problem correction (if the deployment date is maintained), as well as, the possibility of an unstable system being deployed.
- Derived Requirements (DRs) are still being generated and requirements are not being adequately traced to software components and test cases. The generation of DRs and subsequent tracing of all requirements should have been completed prior to software development. There is no single report available that aligns the system requirements (RDs), DRs, software components, and Test Cases. This information may be spread across a number of documents, but it does not appear to have been consolidated anywhere. The flow from requirement to derived requirement to component allocation to test case is needed to confirm that each component appropriately addresses and satisfies the requirements from which it arose. The late completion of the DRs, along with the lack of adequate traceability creates substantial risks to testing, system maintenance, and to planning of R1C3.
- Requirements allocation to different software drops continued until early December. Some requirements have been moved to "post-launch" updates that are not currently scheduled. Deployment of these "post-launch" updates reduces the capabilities of the initial Release. These updates also introduce a risk of lack of acceptance by the user community as the changing functionality may cause user confusion.
- Testing is behind schedule. SIT for the three Drops for R1C2 has not been completed. Further compounding this issue is the incomplete test cases for Drop 3. SIT has also been significantly delayed by the inability of the program to integrate Documentum and create a stable system. Without sufficient SIT, the program risks deploying an unreliable and incorrect system.
- User Acceptance Test (UAT) and Beta Testing has only just begun for the public access part of the system. Only limited test cases for UAT have been developed. To-date, there is no evidence that test cases and procedures have been developed for Beta testing. The User Acceptance and Beta Test Plan for R1C2 is incomplete and unapproved. In addition, if UAT or Beta testing identifies any significant operational problems, it is unlikely that there will be sufficient time to fix these problems prior to the current deployment date.
- Test performance is not being adequately measured. Program Trouble Reports (PTRs) are being generated and tracked; however, no metrics to measure closure are being provided. As testing progresses, metrics, such as find, fix, verify curves, typically are used to monitor test progress. Without such metrics the program risks not knowing when testing will be complete.
- No Performance Testing has occurred. IV&V has not seen a Performance Test Plan and Performance Test Cases have not been developed. Without sufficient performance testing the program risks deploying a system that will not be responsive to user demand.

- Security testing has not occurred. There is no evidence that security test cases have been generated. There probably isn't insufficient time to create the necessary Certification and Accreditation package to meet the deployment date. Without sufficient security testing, the program risks deploying a vulnerable system.
- The delays in development and testing have impacted the development and conduct of FDsys Training. The Training materials are incomplete; and, user training is just beginning. As a result, the user community will may not be properly prepared to utilize FDsys when it is deployed.
- The databases needed for deployment are not complete and available for both public and internal users. The eight (8) GPO Access Collections targeted for FDsys R1C2 must be migrated and verified prior to deployment.
- Critical documentation has not been approved and a Production Baseline has not been established. The detailed design documentation does not reflect the "as-built" design and code, i.e., the Software Design Document (SDD) has not been updated for months. This creates a risk to maintenance and to the planning of R1C3, because without up-to-date documentation, maintenance will rely on the knowledge of the development team and the design of R1C3 will not start from the "as-built" baseline.

3. Identification and Assessment of Technical and Management Risks

The two most significant risks are as follows:

- Inadequate testing of FDsys increases the risk that the deployed system will function improperly and/or contain poor operational characteristics. This will jeopardize the acceptance and use of the system by the community of users that FDsys is supposed to serve.
- Inadequate tracing of requirements to system components and test cases, and lack of complete documentation of the system design creates a risk that system maintenance will be more difficult and costly, and that development of R1C3 will be more difficult and costly.

4. Recommendations

IV&V recommends:

- That the FDsys program ensure that the system is completely tested for functionality, performance, and security prior to deployment; and,
- That requirements traceability and documentation updates be completed prior to beginning design of R1C3.