U.S. GOVERNMENT
PRINTING OFFICE
KEEPING AMERICA INFORMED

ASSESSMENT REPORT 08-04

FEDERAL DIGITAL SYSTEM (FDSYS) INDEPENDENT VERIFICATION AND VALIDATION (IV&V) – FIRST QUARTER OBSERVATIONS AND RECOMMENDATIONS

March 28, 2008

OFFICE OF INSPECTOR GENERAL

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

Memorandum

OFFICE OF THE INSPECTOR GENERAL

DATE: March 28, 2008

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

SUBJECT: Federal Digital System (FDsys) Independent Verification and
Validation (IV&V) – First Quarter Observations and Recommendations
Report Number 08-04

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 tasked with 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 report to the OIG each quarter 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.

For the period July 2007 to September 2007, American Systems completed an initial assessment of Harris Corporation's FDsys program management practices used for the Release 1.B, pilot system. The goal of that assessment was to analyze current practices, assess effectiveness, and provide potential recommendations for improvements in managing implementation of Release 1.C. American Systems reviewed the Harris Program Management Plan, Risk Management Plan, Risk Database, the results of an Independent Risk assessment, several Harris monthly reports and program reviews, Harris variance analysis reports, and configuration management plans and practices.

[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. More information on FDsys can be found at www.gpo.gov/projects/fdsys.htm.

[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 initial IV&V assessment showed that Harris established a strong basis for good program management practices for Release 1.B. American Systems did identify, however, certain weaknesses that could lead to schedule risk and cost overrun for Release 1.C if not addressed soon. Those weaknesses include:

- insufficient use of earned value analysis;
- lack of an Integrated Baseline Review (IBR);
- incomplete adherence to risk management program;
- risks associated with testing;
- lack of system capabilities documentation; and
- insufficient Configuration Management Plan.

Subsequent to issuance of our draft report, GPO made significant changes to the FDsys program to include assuming program control of FDsys. However, our original findings and recommendations are still applicable, and GPO management has appropriately responded based on the new plan for the FDsys program. This report includes 14 recommendations to strengthen management of the FDsys program, and management's response to those recommendations. Our evaluation of management's response has been incorporated into the body of the report and is included in its entirety in Appendix A. We consider management's actual and proposed corrective actions responsive to each of the recommendations. We are closing three recommendations (numbers 6, 8, and 14) upon issuance of this report. The remaining 11 recommendations will remain open for reporting purposes until the agreed-to corrective actions are completed. The status of each recommendation upon issuance of this report is included in Appendix B. Please notify us when actions have been completed on the remaining open recommendations.

Insufficient Use of Earned Value Analysis

Release 1.B cost and schedule overruns are having a major impact on the schedule and planned functionality for Release 1.C. While overruns could be caused by a variety of problems, they can be potentially avoided or lessened in Release 1.C through the more active use of Earned Value (EV)[4] analysis by Harris. Earned Value Management (EVM) is used to track the project's technical performance (accomplishment of planned work), schedule performance, and cost performance. If used effectively, EVM should provide an early warning of FDsys project performance problems while time is available for corrective action. EVM should also improve definition of the project scope, prevent scope creep, communicate objective progress to FDsys stakeholders, and keep the project team focused on achieving progress.

The Schedule Performance Index (SPI)[5] Harris reported for January through July 2007 showed that the program was behind schedule.[6] Similarly, the Cost Performance Index

[4] Earned Value is calculated as the percent work complete times the sum of all the budget values established for the work to be performed on the project.

[5] An SPI is a measure of schedule efficiency on a project. The index is the ratio of EV to planned value. An SPI equal to or greater than one indicates that the project is ahead of schedule, while a value of less than one indicates that the project is behind schedule.

(CPI)[7] Harris reported for the same time period showed that the program was running over budget.[8] Although there are a number of potential causes for such deviations, the monthly reports and program reviews during that time do not indicate the plan of actions taken for getting the program back on schedule and within budget.

A best practice for standard program management is to provide either a summary report, stoplight-style chart of key program management indicators and program areas, or both. American Systems determined that Harris does provide that type of stoplight chart. In EV standard practice however, SPI and CPI are typically flagged as "yellow" when they are between .9 and .95 and "red" when under .9. While Harris does follow such a threshold for reporting, best practices requires that a plan to get the program back to "green" should be provided whenever an indicator is "yellow" or "red." Harris did not provide such plans for FDsys.

Harris also did not conduct an EV variance analysis at the control account[9] level. A best practice for program management is to require variance analysis at the control account level whenever a cost or schedule variance greater than 10 percent exists (although the program usually sets the thresholds). Variance analysis typically requires explanation for the variance and a plan of action to remediate the variance. Such analysis provides detailed insight into which parts of the program are leading to problems. The Harris Program Management Plan and Command Media[10] outline how that analysis should be done for Harris programs. However, no variance analyses were accomplished at the control account level during at least the last four months.

Lack of Integrated Baseline Review for Release 1.B

One potential reason for the cost and schedule overruns for Release 1.B was that the overall program plan as initially defined was unrealistic in terms of the cost to perform the work or the time needed to complete the work. While American Systems did not do a backward-looking schedule analysis for Release 1.B, they did inquire about the measures that the GPO FDsys Program Management Office (PMO) took for ensuring that the plan was realistic in terms of cost and schedule.

[6] The SPI for January through July 2007 was 0.87, 0.88, 0.80, 1.13, 0.88, 0.84, and 0.79 respectively, with an overall SPI for the program under 0.95 for the entire period.

[7] A CPI is a measure of cost efficiency on a project. The index is the ratio of EV to actual cost of work performed. A value equal to or greater than one indicates the cost to complete the work is less than planned. A value of less than one indicates the cost to complete the work is more than planned.

[8] The CPI for January through July 2007 was 0.67, 0.76, 0.94, 0.95, 0.84, 0.75, and 0.91, with an overall CPI for the program of 0.94.

[9] A control account is a project management control point for cost summarization, schedule and milestone control, variance analysis and reporting, responsibility assignment, scope control, and corrective action planning. The Control Account Manager is the person responsible for managing the control account, including reporting EV data.

[10] Command Media is Harris documentation describing its quality management system and standards for system development and program management.

A best practice for program management within Government programs the size of FDsys is to perform an Integrated Baseline Review (IBR) that will help ensure the cost and schedule plan is reasonable and achievable. The goal of an IBR is to determine if the technical work can be performed within the available schedule and budget. Clarification No. 6 amended the GPO Statement of Work for Harris, which amends Section C 3.9 to include the possibility for EVM IBRs. The Harris Program Management Plan Revision 1, Section 6.3 requires an IBR for each release. No IBR was held for Release 1.B.

Risk Management Program Not Completely Followed

American Systems found that the FDsys risk management program has well-established risk management plans and procedures that can help Harris identify and mitigate program risks before they become issues. The current Risk Management Plan calls for at least monthly risk review board meetings. However, there is no evidence that risk review board meetings were held during August or September 2007.

The risk database, a repository for risk tracking, has not been updated by Harris since June 12, 2007. Because of the extent of re-planning for Release 1.C, the FDsys PMO and Harris conducted a joint Independent Risk Assessment early in August of 2007 that identified a number of potential issues and risks to the program. Those results should be recast into forward-looking risks for Release 1.C and entered in the risk review process as outlined in the Risk Management Plan.

Risks Associated With Design Validation Testing

A risk exists that the Design Validation Test (DVT) conducted during Release 1.C could take longer than expected or might be ineffective because the requirements management process is not clearly defined, especially as it relates to testing. While Configuration Management (CM) and the Configuration Control Board (CCB) control the requirements baseline for the text of the requirements and release to which the requirements are allocated, the remainder of the requirements attributes (for example, test cases) are not. Although we would not expect that the CCB control the requirements, they should have a well-defined process. That process is not documented. More importantly, no clearly defined linkage exists between the requirements database (held in DOORS), the Program Tracking Report (PTR) tool (ClearQuest), and the testing tool. Although maintained manually, a process for maintaining the link should be defined so the three areas are traceable.

The program decided not to perform DVT on Release 1.B. As a result, the test program was not established during Release 1.B and did not have the opportunity to mature its plans and processes. Thus, formal test plans for DVT, the User Acceptance Test (UAT), and Beta testing were not developed to the level of rigor Release 1.C requires. A secondary effect is that GPO is not certain which requirements were successfully implemented in Release 1.B. Therefore, testing could take longer than expected because Release 1.C depends on the foundation of Release 1.B.

Lack of System Capabilities Documentation

During the initial analysis of the FDsys program, American Systems was unable to find adequate documentation of the detailed capabilities that the system would provide in meeting GPO business needs. Although high-level capabilities statements exist, the next level of detail (at the business process level) would provide for a common understanding of the functionality the system will provide. The Concept of Operations document was not updated and does not delineate functionality by release. Some use cases and workflows exist, but they are not combined to provide a comprehensive view of the capabilities provided in Release 1.C. Further, the use cases and workflows are not consistently linked to the requirements. As a result, GPO is potentially at risk that a system will be developed that meets technical requirements but not expectations from a business and stakeholder perspective.

Insufficient Configuration Management Plan

Harris has sole responsibility for the development and implementation of the Configuration Management Plan. The configuration management practices Harris uses were planned and established for the entire FDsys program, with a current focus on Release 1.B. The FDsys Configuration Management Plan does reference and can be mapped to the Harris Configuration Management Manual. This initial document is sufficient for the purpose of the initial phase of the FDsys program. However, the overall content of the document does not contain or reference specific configuration management standards that the Harris Configuration Management Manual specifies.

One possible explanation for the lack of specific standards may be as the Configuration Management Plan indicates, in Paragraph 1.1, that the "CM Plan describes the framework for the application of configuration and data management disciplines at the system, software, and data levels," and as a framework does not specifically reference the configuration management standards in the Harris Configuration Management Manual. Secondly, Paragraph 2.2 indicates that "the following Harris internal documents are applicable to the FDsys Program," with one of those documents being the Harris Configuration Management Manual. Although it is not our intention to see the entire Harris Configuration Management Manual repeated in the FDsys Configuration Management Plan, best practice dictates that the FDsys Configuration Management Plan should reference the configuration management standards in the Harris Configuration Management Manual. Harris does appear to be following the processes described in the plan.

Another potential weakness is that the PMO does not have its own configuration management process. The lack of such a process increases the risk of the PMO not knowing which artifacts they control. By not taking formal ownership of the documents, code, and other program artifacts, the PMO cannot adequately control their content and status.

Configuration management is a critical function encompassing requirements management, code management, management of test processes and results, and change management in general. There must be some assurance that approved requirements changes from the CCB are accurately reflected in the DOORS requirements database. Proper maintenance and updating of the requirements database facilitates reporting and ensures that the requirements database contains approved changes traceable from the requirements database through the original PTR. Without stronger change management and requirements management practices, Release 1.C could incur both schedule and cost risk as a result of an increase in scope or missed requirements (i.e. longer development time and a shortened test phase, or both).

Lack of Detailed Transition Plans

Because Release 1.B is a pilot version of FDsys, detailed plans for certification and accreditation, training, and transition to operations were not developed. Without such plans, American Systems could not determine how prepared the FDsys PMO is for such activities in Release 1.C. Those activities are typically time consuming and require detailed planning.

Certification and accreditation are important activities that support risk management. The Federal Information Security Management Act (FISMA) requires that executive branch agencies follow system certification and accreditation guidelines the National Institute of Standards and Technology[11] publishes. As a legislative branch agency, GPO is not required to comply with FISMA. However, because of the services GPO provides, particularly those to agencies within the executive branch, the Agency has chosen to comply with the principles of FISMA. Additionally, lack of early planning for training and transitioning operations to GPO increases the risk that these activities will take longer than expected.

Recommendations

The GPO Chief Information Officer (CIO) should:

1. Require that Harris provide in its monthly reporting structure a plan based on the earned value analysis known as the "return to green plan(s)." The return to green plan is initiated when earned value metrics reach specified thresholds. Such plans will provide the Program Management Office with visibility into how problems are being addressed by the Program Management Office.

[11] National Institute of Standards and Technology Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," provides guidelines for certification and accreditation of information systems supporting the executive agencies of the Federal Government. Accreditation is the official management decision senior agency officials give to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Certification is the information and supporting evidence needed for accreditation. Certification and accreditation is developed during a detailed security review of an information system.

Management's Response. Concur. GPO has assumed program control of FDsys. GPO will require that Harris provide more detailed monthly reporting to include Earned Value Management System (EVMS) metrics that will be approved by GPO. The complete text of management's response is in Appendix A.

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. However, due to the recent change in the FDsys program structure, it is unclear how earned value data will be reported going forward. The IV&V team will continue to monitor the use of earned value metrics and return to green plans. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

2. Require monthly program review meetings that provide visibility into earned value data as well as technical progress. Those meetings will give the Program Management Office and other GPO management visibility into the schedule, cost, and technical status of the program.

Management's Response. Concur. GPO will conduct monthly program reviews (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

3. Require that Control Account Managers follow the Harris process and provide variance analysis required during the Release 1.C design and development stages.

Management's Response. Concur. The FDsys Contracting Officer's Technical Representative will monitor the program activity of Harris Control Account Managers to ensure their compliance with Harris' stated process. GPO will require Control Account Managers to provide variance analysis data consistent with any agreed upon EVMS metrics (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

4. Require completion of an Integrated Baseline Review for Release 1.C between 30 and 60 days after the program management baseline is accepted. Completion will provide mutual understanding of the elements that comprise the program baseline between Harris and the Program Management Office. Further, it will attempt to identify potential risks to the program and increase the confidence for all parties involved that the system can be delivered on time and within budget.

Management's Response. Concur. While management concluded that an Integrated Baseline Review (IBR) is not feasible at this point in the program, they will determine how best to apply an IBR to the new approach once a detailed program schedule has been created (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. Due to the recent change in program management, we agree that an IBR is not feasible at this time. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

5. Require execution of the Risk Management Plan as documented. Regular risk review board meetings should be conducted and the risk database should be updated accordingly with elements of risk discovered. The risk review board minutes should be published and made available to management in the Program Management Office.

Management's Response. Concur. GPO will establish and maintain a risk review board process. The anticipated frequency of the board will be bi-weekly at first, evolving into monthly as the process matures (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

6. Require that Harris convert lessons learned from the independent risk assessment into risks elements and enter them into the risk management process for acceptance and possible remedy. Alternatively, the Program Management Office should hold an independent assessment focusing specifically on identifying risks associated with Release 1.C.

Management's Response. Concur. GPO is currently leveraging lessons learned material and will continue to do so with the re-constituted FDsys team to ensure that the program does not repeat past mistakes (see Appendix A).

Evaluation of Management's Response. Management's actions are responsive to the recommendation. This recommendation is resolved and dispositioned, and considered closed for reporting purposes.

7. Require clear establishment of expectations for testing Release 1.C. The Master Test Plan should provide the high-level guidance for the criteria for Government sell-off of requirements. The Design Validation Test plan should clearly identify test cases and the requirements verified. The User Acceptance Test and Beta Test Plans should address verification to some agreed-to criteria. Sufficient time should be provided in the schedule for Design Validation Test for Release 1.C because Release 1.B did not undergo formal testing.

Management's Response. Concur. GPO agreed that sufficient test plans are critical to FDsys success in light of the lack of formal Release 1.B testing. Therefore, GPO made the Master Test Plan and Design Validation Testing Plan deliverables to GPO from Harris on February 28, 2008. GPO will review these documents and incorporate them into a new Master Test Plan including User Acceptance Test and Beta plans (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

8. Consider developing a complete set of scenariōs that define GPO expectations for Release 1.C. The scenarios could be documented in a number of forms, including use cases, flow diagrams, English descriptions, or other business process languages. Scenarios would help ensure that expectations are defined and provide the Harris development team with a high-level description of the system. Furthermore, scenarios would provide a basis for User Acceptance Test and Beta testing. Because those tests are designed to ensure that the system meets its business and mission needs, scenarios would clearly define that need and establish the expectations for that testing. Ideally, the scenarios would link requirements for establishing traceability between requirements and capabilities.

Management's Response. Concur. The Program Management Office (PMO) has developed scenarios that define GPO expectations for Release 1.C. The PMO has developed descriptions of each system workflow and associated use case created for R1C2 and R1C3 (see Appendix A).

Evaluation of Management's Response. Management's actions are responsive to the recommendation. This recommendation is resolved and dispositioned, and considered closed for reporting purposes.

9. Require the development of a Requirements Management Plan (or at least a process that can be seen and monitored). Minimally, such a plan or process should establish the relationship between the requirements, Program Tracking Report, and testing tools. While it appears that the burden of requirements management falls mainly with the Harris systems engineering team, the change control process falls under the configuration management domain, that is, changes to the requirements baseline in DOORS cannot be updated unless the Configuration Control Board approves the change; therefore, the processes are inextricably joined. Requirements management processes should be included or referenced in the FDsys Configuration Management Plan.

Management's Response. Concur. GPO will control the requirements and will be responsible for establishing a process for requirements management. While final details have not been developed it is anticipated that this will include establishing an updated Configuration Management (CM) capability within the agency (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

10. Require that Harris schedule and carryout routine audits of the requirements database in DOORS to ensure timely and accurate updates that reflect only the changes the Configuration Control Board approved. Such a requirement should remedy the potential for scope increase as FDsys progresses to Release 1.C.

Management's Response. Concur. GPO agreed that a better requirements process must be developed. In assuming control of the requirements database, GPO will be in a better position to ensure that requirements changes are in line with program objectives. GPO or a contractor will conduct an audit after each program phase (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

11. Require that the FDsys Configuration Management Plan is more rigorous in both its specificity and in the implementation of the plan itself. The Configuration Management Plan should reference by name and number the configuration management standards cited in the Harris Configuration Management Manual to also include other pertinent documentation such as approved program directives and other related program processes currently known.

Management's Response. Concur. GPO agreed that the FDsys Configuration management Plan is insufficient. The PMO is now developing its own CM plan. Change requests will be submitted to GPO's Change Control Board (CCB). The CCB will perform programmatic and technical analysis and recommend either further analysis from the PMO or will forward the request through Harris' processes. GPO management is currently reviewing a draft document that establishes Configuration Management (CM) guidelines for GPO. The guidelines implement GPO instruction 705.30, Configuration Management Policy Statement. GPO's CM plan will manage the original contract, Conops, Requirements Baseline, Requirements Document, Technical Specs, and the Systems Architecture Design Document (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

12. Require that a Government Configuration Management Plan be established for FDsys. By having a Government plan, GPO could better control the deliverables of Harris and ensure that they are aware of the deliverable contents.

Management's Response. Concur. GPO management is currently reviewing a draft document that establishes CM guidelines for GPO. The guidelines implement GPO instruction 705.30. CM will apply to all systems, subsystems, and components of the GPO IT infrastructure, including Commercial-Off-The-Shelf, Commercially Available Software systems, and custom engineered systems. FDsys will follow GPO CM guidelines, which will provide a measure of the effectiveness of the contractor deliverables (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

13. Require development of and early review of detailed Release 1.C plans for transition to operations, training, and certification and accreditation. Early review ensuring that plans are complete and comprehensive is essential for a successful public deployment. Once plans are established, the FDsys Program Management Office should perform a schedule analysis to ensure sufficient time is provided for these activities.

Management's Response. Concur. GPO has been participating in a number of activities in support of a successful transition and public deployment. System documentation is being developed to support the entire lifecycle of system operations (see Appendix A).

Evaluation of Management's Response. Management's planned actions are responsive to the recommendation. The recommendation is resolved, but will remain undispositioned and open for reporting purposes until corrective actions are completed.

14. Consider hiring an experienced Government program manager for the FDsys program. Ideally, the individual should have experience managing programs similar to the size and nature of the FDsys.

Management's Response. Concur. GPO agreed that an experienced program manager is needed to support the FDsys program. In September of 2006 the Office of the Chief Technical Officer attempted to hire an experienced program manager for FDsys at the GS-15 level. The resulting candidates were interviewed and deemed not suitable for the program. Meanwhile, GPO's program staff has obtained significant experience from the FDsys program and others being run through the Program Office. GPO intends to restructure the Program Management Office with one of the current associate directors assuming the role of FDsys Program Manager (see Appendix A).

Evaluation of Management's Response. Management's actions are responsive to the recommendation. IV&V will continue to monitor the overall effectiveness of FDsys program management. This recommendation is resolved and dispositioned, and considered closed for reporting purposes upon issuance of the final report.

If you have questions concerning this assessment 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

Kevin J. Carson
Assistant Inspector General for Audits and Inspections

cc:
Chief of Staff
Chief Management Officer
Chief Technology Officer

Appendix A. Management's Response

IT&S Response to:
OIG Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – First Quarter Observations and Recommendations

February 16, 2008

Introduction

The GPO Office of the Inspector General (OIG) issued a report to GPO's Chief Information Officer (CIO) detailing its findings and recommendations derived from an assessment of Harris Corporation's program management practices used in the development of GPO's FDsys Release 1.B, pilot system covering the time period of July to September 2007. Within this assessment entitled OIG Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – First Quarter Observations and Recommendations, The OIG provided a list of fourteen (14) recommendations for improvements in managing the implementation of FDsys Release 1.C.

This document is the GPO Information Technology and Systems (IT&S) response to the OIG recommendations contained in that assessment Report. Please note that there have been significant changes in the program since the report was issued, and the initial responses were crafted. IT&S responses will carry one of three designations: 1) old Plan: This is the response by IT&S prior to the change in program responsibility; 2) new Plan: This is the response by IT&S after the change in program responsibility; 3) old and new Plan: The response covers either approach to program responsibility.

OIG Recommendations and IT&S Response

The results of the IV&V assessment Report indicated, as was expected by GPO management, several areas for improvement. The IT&S response to each of the OIG recommendations is shown below.

OIG Recommendation #01:
Require that Harris provide in its monthly reporting structure a plan based on the earned value analysis known as the "return to green plan(s)." The return to green plan is initiated when earned value metrics reach specified thresholds. Such plans will provide the Program Management Office with visibility into how problems are being addressed by the Program Management Office.

IT&S Response (old Plan):
Harris has agreed to provide GPO with more detailed monthly reporting to include jointly developed earned value management system (EVMS) metrics that will ultimately be approved by GPO. Based on the recommendation of the OIG, GPO will require that Harris include a "return to green" plan as part of the EVMS in order to systematically remedy budget/schedule deficiencies and mitigate program risks as they are identified. Additionally, these deficiencies along with proposed mitigation will be monitored as part of the Risk Management Plan.

IT&S Response (new Plan):

As an overall "return to green plan" GPO has assumed program control of FDsys. GPO will require that Harris provide more detailed monthly reporting to include EVMS metrics that will be approved by GPO.

<u>OIG Recommendation #02:</u>
Require monthly program review meetings that provide visibility into earned value data as well as technical progress. Those meetings will give the Program Management Office and other GPO management visibility into the schedule, cost, and technical status of the program.

IT&S Response (old Plan):
Monthly program review meetings have been instituted, and the latest one was held on January 23, 2008. As part of the EVMS implementation, emphasis on earned value data will be a part of subsequent meetings. Review of "return to green" plans will also be incorporated as a part of the meetings.

IT&S Response (new Plan):

GPO will conduct monthly program reviews.

<u>OIG Recommendation #03:</u>
Require that Control Account Managers follow the Harris process and provide variance analysis required during the Release 1.C design and development stages.

IT&S Response (old and new Plan):
The FDsys COTR will monitor the program activity of Harris Control Account Managers (CAMs) to ensure their compliance with Harris' stated process. Likewise, GPO will require CAMs to provide variance analysis data consistent with any agreed upon EVMS metrics as reference in the above response to OIG Recommendation #01.

OIG Recommendation #04:

Require completion of an Integrated Baseline Review for Release 1.C between 30 and 60 days after the program management baseline is accepted. Completion will provide mutual understanding of the elements that comprise the program baseline between Harris and the Program Management Office. Further, it will attempt to identify potential risks to the program and increase the confidence for all parties involved that the system can be delivered on time and within budget.

IT&S Response (old Plan):

Harris has proposed a revised budget, schedule, and work breakdown structure (WBS) (submitted to GPO on January 11, 2008). Together, these elements would comprise a new performance measurement baseline (PMB). Once the terms of a replan are agreed upon, GPO will conduct an Integrated Baseline Review (IBR) within 60 days of the new agreement. The scope of the IBR will likely be limited to one or two key accounts rather than a full IBR. The IBR will encompass some of the previously referenced activities including an analysis of the PMB and CAM interviews to examine EVMS reporting methods with variance analysis.

IT&S Response (new Plan):

At this point in the program, GPO has concluded that an IBR is not feasible. GPO will determine how best to apply an IBR to the new approach once we have had an opportunity to create a detailed program schedule

OIG Recommendation #05:

Require execution of the Risk Management Plan as documented. Regular risk review board meetings should be conducted and the risk database should be updated accordingly with elements of risk discovered. The risk review board minutes should be published and made available to management in the Program Management Office.

IT&S Response (old Plan):

IT&S concurs with the IG's findings. A new Project Engineer has begun on the program and the risk management plan was discussed at the January Program Review. Since then a risk management process meeting was held to discuss the resumption of the process. The risk database has also been revisited as part of this effort.

IT&S Response (new Plan):

GPO intends to establish and maintain a risk review board (RRB) process. The anticipated frequency of RRB will be bi weekly at first, evolving into monthly as the process matures.

OIG Recommendation #06:

Require that Harris convert lessons learned from the independent risk assessment into risks elements and enter them into the risk management process for acceptance and possible remedy. Alternatively, the Program Management Office should hold an independent assessment focusing specifically on identifying risks associated with Release 1.C.

IT&S Response (old Plan):

IT&S agrees, and since 1B, there have been numerous lessons learned discussions and no documentation of risk assessment. However, the incorporation of these lessons learned into the risk management process has been requested by the PMO.

IT&S Response (new Plan):

GPO is currently leveraging the lessons learned material in the establishment of the new program plans. GPO will continue to analyze and close out on items previously raised by Harris corporation and in parallel conduct a new Lessons Learned session with the re-constitued FDsys team. These items will be actioned, where possible, to ensure that the program does not repeat past mistakes.

OIG Recommendation #07:

Require clear establishment of expectations for testing Release 1.C. The Master Test Plan should provide the high-level guidance for the criteria for Government sell-off of requirements. The Design Validation Test plan should clearly identify test cases and the requirements verified. The User Acceptance Test and Beta Test Plans should address verification to some agreed-to criteria. Sufficient time should be provided in the schedule for Design Validation Test for Release 1.C because Release 1.B did not undergo formal testing.

IT&S Response (old Plan):

Harris released the draft Master Test Plan to GPO for review in December 2007. The MTP was reviewed by PMO, IT Test Branch, and IV&V contractor personnel. Currently Harris is revising the MTP based on comments from these areas, and the expectation is that the final Plan will provide the necessary guidance for criteria for Government sell-off of requirements. The Design Validation Test Plan is still in development by Harris and will be shared with GPO and the IV&V contractors for review and comment prior to the R1C.2 Preliminary Design Review. The current R1C.2 schedule shows ~60 days for DVT testing (from SWIT completion through DVTRR). GPO will monitor testing progress to ensure the amount of time scheduled is sufficient to test and validate all requirements in R1C.2. GPO will control User Acceptance Testing and Beta Testing and will take the lead in determining verification criteria.

IT&S Response (new Plan):
GPO agrees that sufficient test plans are critical to FDsys success in light of the lack of formal R1B testing. Therefore, GPO has made the Master Test Plan (MTP) and Design Validation Test Plan (DVT) deliverables to GPO from Harris on 2/28/08. GPO will review this document and incorporate the content into a new MTP including UAT and Beta plans.

OIG Recommendation #08:
Consider developing a complete set of scenarios that define GPO expectations for Release 1.C. The scenarios could be documented in a number of forms, including use cases, flow diagrams, English descriptions, or other business process languages. Scenarios would help ensure that expectations are defined and provide the Harris development team with a high-level description of the system. Furthermore, scenarios would provide a basis for User Acceptance Test and Beta testing. Because those tests are designed to ensure that the system meets its business and mission needs, scenarios would clearly define that need and establish the expectations for that testing. Ideally, the scenarios would link requirements for establishing traceability between requirements and capabilities.

IT&S Response (old and new Plan):
The PMO has developed scenarios that define GPO expectations for Release 1.C.

The PMO has developed descriptions of each system workflow and associated use case created for R1C2 and R1C3. The actual use cases and workflows are documented within GPO's network storage at the following location: \SDS\Systems Engineering\Behavioral Model\1C Workflows and Use Cases. The following should be noted regarding this information:

1. The system workflows and use cases have NOT been done for R1C4. There are only placeholders.

2. There are many additional files within the workflow folders for 1C2 and 1C3. These are software workflows derived from BPM and tech memo activities and are not referenced in the attached spreadsheet.

OIG Recommendation #09:

Develop a Requirements Management Plan (or at least a process that can be seen and monitored). Minimally, such a plan or process should establish the relationship between the requirements, Program Tracking Report, and testing tools. While it appears that the burden of requirements management falls mainly with the Harris systems engineering team, the change control process falls under the configuration management domain, that is, changes to the requirements baseline in DOORS cannot be updated unless the FDsys Configuration Control Board approves the change; therefore, the processes are inextricably joined. Requirements management processes should be included or referenced in the FDsys Configuration Management Plan

IT&S Response (old Plan):

GPO will require Harris to include a requirements management plan in their FDsys Configuration Management Plan, to include, at minimum, a report outlining the relationship between requirements, Program Tracking Reports, and testing tools. GPO and Harris are working to conclude on the CM process and requirements change.

IT&S Response (new Plan):

GPO will control the requirements and will be responsible for establishing a process for requirements management. While final details have not been developed it is anticipated that this will include establishing updated CM capability within the agency.

OIG Recommendation #10:

Require that Harris schedule and carryout routine audits of the requirements database in DOORS to ensure timely and accurate updates that reflect only the changes the FDsys Configuration Control Board approved. Such a requirement should remedy the potential for scope increase as FDsys progresses to Release 1.C.

IT&S Response (old Plan):

GPO will require Harris to audit the DOORS database after each major program review (e.g., SRR, SDR, PDR, CDR) to ensure all requirements have been approved FDsys Configuration Control Board.

IT&S Response (new Plan):

GPO agrees that a better requirements process must be developed. In assuming control of the requirements database GPO will be in a better position to ensure that requirement changes made are in line with program objectives. GPO, or a contractor required to support this task, will conduct an audit after each program phase.

OIG Recommendation #11:
Require that the FDsys Configuration Management Plan is more rigorous in both its specificity and in the implementation of the plan itself. The Configuration Management Plan should reference by name and number the configuration management standards cited in the Harris Configuration Management Manual to also include other pertinent documentation such as approved program directives and other related program processes currently known.

IT&S Response (old and new Plan):
GPO agrees that the FDsys Configuration Management Plan is insufficient. The plan as defined and managed by Harris does not allow for adequate visibility by GPO into the manner in which FDsys documents and processes are being managed.

The PMO is developing its own CM plan, parallel to Harris CM procedures (GPO must validate with the Harris CSWE and Program Manger that Harris CM procedures will be used), which will reference the CM standards in the Harris Configuration Management Manual. Change requests will be submitted to GPO's Change Control Board (CCB). The CCB will perform programmatic and technical analysis, and recommend either further analysis from the PMO or will forward the request through Harris' processes. GPO management is currently reviewing a draft document that establishes Configuration Management (CM) guidelines for GPO. The guidelines implement GPO instruction 705.30, Configuration Management Policy Statement.

GPO's CM plan will manage the original contract, Conops, Requirements Baseline, Requirements Document, Technical Specs (SFS, TDF, Tech Memos) and the SADD.

Harris has CM training scheduled shortly before CDR. The PMO has been invited to participate in the training, which will provide the opportunity for GPO to be more familiar with Harris CM practices and documentation and thus better able to judge the products of their CM protocols.

OIG Recommendation #12:
Establish a Government Configuration Management Plan for FDsys. By having a Government plan, GPO could better control the deliverables of Harris and ensure that they are aware of the deliverable contents.

IT&S Response (old and new Plan):
GPO management is currently reviewing a draft document that establishes Configuration Management (CM) guidelines for GPO. The guidelines implement GPO instruction 705.30, Configuration Management Policy Statement. The objective of CM is to create

an environment where the lifecycle of all information technology products, services, and infrastructure components, including relevant documentation, is managed in a controlled system. This discipline contributes to efficient planning, release, and implementation of changes to IT systems and services, and assures that relevant information is readily and consistently available to GPO decision makers.

CM will apply to all systems, subsystems, and components of the GPO IT infrastructure, including Commercial Off-The-Shelf (COTS), Commercially Available Software (CAS) systems, and custom engineered systems. CM control begins with system or change requests, progresses through baseline requirements documentation and implementation, continues through operation and modification, and ends with decommissioning of the system, subsystem, or components.

FDsys will follow GPO CM guidelines, which will provide a measure of the effectiveness of the contractor deliverables.

OIG Recommendation #13:

Require development of and early review of detailed Release 1.C plans for transition to operations, training, and certification and accreditation. Early review ensuring that plans are complete and comprehensive is essential for a successful public deployment. Once plans are established, the FDsys Program Management Office should perform a schedule analysis to ensure sufficient time is provided for these activities.

IT&S Response (old and new Plan):

GPO concurs with the OIG recommendation and has been participating in a number of activities in support of a successful transition and public deployment. Once deployment occurs, clearly defined roles, responsibilities, and documented processes will be in place for all IT personnel in order to manage and maintain the system. Developed training plans for IT personnel will be implemented, and appropriate staff will be giving specific duties in support of FDsys.

System documentation is being developed to support the entire lifecycle of system operations. Included in this are the FDsys Certification and Accreditation Plan (C&A Plan), System Security Plan, Self Assessment, Privacy Impact Assessment, and COOP. Once completed, all plans will go through the FDsys Change Control Board (CCB) process.

OIG Recommendation #14:

Consider hiring an experienced Government program manager for the FDsys program. Ideally, the individual should have experience managing programs similar to the size and nature of the FDsys.

IT&S Response (old and new Plan):
GPO agrees with the recommendation that an experienced program manager, dedicated to FDsys is needed to support the program. In September of 2006 the Office of the Chief Technical Officer (OCTO) attempted to hire an experienced program manager for FDsys at the GS 15 level (highest level allowed by Human Capitol).

We recruited through various organizations and media and the position was open to all sources, not just Government. The resulting candidates were interviewed and deemed not suitable for the program for a variety of reasons. In the meantime, GPO's program staff has obtained significant experience from the FDsys program and others being run through the Program Office. It is possible that a suitable candidate can be found either internally, or externally. GPO intends to restructure the Program Management Office with one of the current associate directors assuming the role of FDsys Program Manager.

Appendix B. Status of Recommendations

Recommendation No.	Resolved	Unresolved	Open/ECD*	Closed
1	X		9/30/2008	
2	X		9/30/2008	
3	X		9/30/2008	
4	X		9/30/2008	
5	X		9/30/2008	
6	X			X
7	X		9/30/2008	
8	X			X
9	X		9/302008	
10	X		9/30/2008	
11	X		9/30/2008	
12	X		9/30/2008	
13	X		9/30/2008	
14	X			X

*Estimated Completion Date