U. S. GOVERNMENT PRINTING OFFICE ■ OFFICE OF INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

APRIL 1, 2011 THROUGH SEPTEMBER 30, 2011

GPO U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

THE U.S. GOVERNMENT PRINTING OFFICE

For well over a century, the U.S. Government Printing Office (GPO) has fulfilled the needs of the Federal Government for information products and distributing those products to the public. GPO is the Federal Government's primary resource for gathering, cataloging, producing, providing, authenticating, and preserving published U.S. Government information in all its forms. GPO also produces and distributes information products and services for each of the three branches of Government.

Under the Federal Depository Library Program, GPO distributes a wide range of Government publications in print and online to more than 1,250 public, academic, law, and other libraries across the country. In addition to distributing publications through that library system, GPO provides access to official Federal Government information through public sales and other programs, and—most prominently—by posting more than a quarter of a million titles online through GPO Access (www.gpoaccess.gov).

Today approximately 97 percent of Federal Government documents begin as digital products and are published directly to the Internet. Such an evolution of creating and disseminating information challenges GPO, but it has met those challenges by transforming itself from primarily a print format entity to an agency ready, willing, and able to deliver from a digital platform a high volume of information to a multitude of customers.

Although a transition to digital technology changes the way products and services are created and offered, GPO strives to continually satisfy the requirements of Government and accomplish its mission of *Keeping America Informed*.

THE OFFICE OF INSPECTOR GENERAL

The Office of Inspector General (OIG) was created by the GPO Inspector General Act of 1988—title II of Public Law 100-504 (October 18, 1988) (GPO IG Act). The OIG at GPO is dedicated to acting as an agent of positive change—changes that help GPO improve its efficiency and effectiveness as the Agency undertakes an era of unprecedented transformation. Through evaluation of GPO's system of internal controls, the OIG recommends policies, processes, and procedures that help prevent and detect fraud, waste, abuse, and mismanagement. The OIG also recommends policies that promote economy, efficiency, and effectiveness in GPO programs and operations.

The OIG informs the Public Printer and Congress about problems and deficiencies as well as any positive developments relating to GPO's administration and operation. To accomplish those responsibilities, the OIG conducts audits, assessments, investigations, inspections, and other reviews.

TABLE OF CONTENTS

MESSAGE FROM THE INSPECTOR GENERAL

This Semiannual Report to the Congress covers the activities of the GPO Office of Inspector General for the period of April 1, 2011 through September 30, 2011.

With the current budget environment, all eyes are on federal agencies to tighten the efficiency of their operations and identify potential areas for spending cuts. The OIG FY 2012 budget request reflects a 14% decrease from its previous budget. In the last six months the GPO OIG has lost five employees. These vacant positions are very critical and essential for carrying out the functions, duties, and responsibilities of the Office of Inspector General. These positions should be filled quickly upon the approval of the FY 2012 budget.

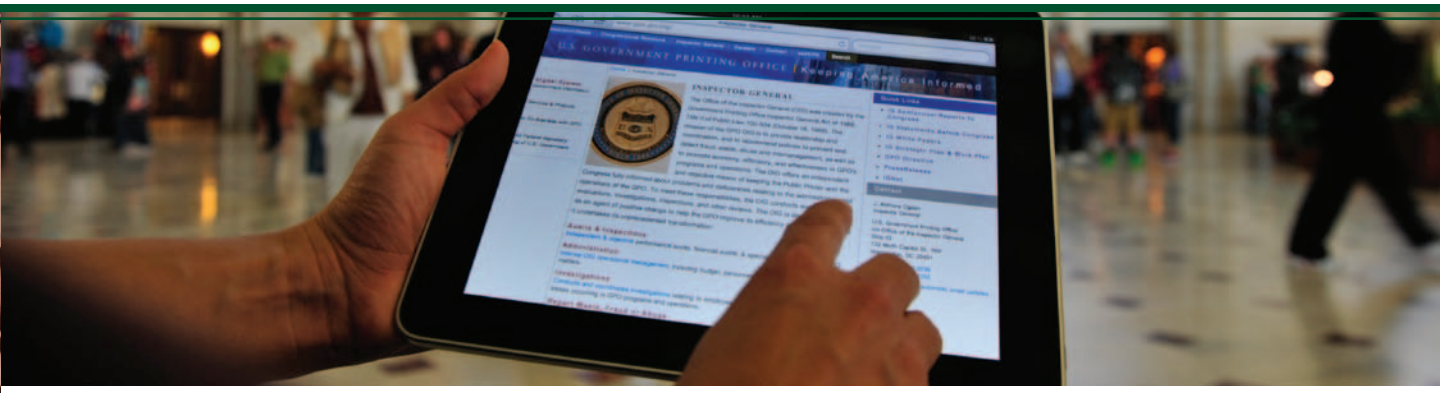
During this reporting period the Office of Audits and Inspections (OAI) and the Office of Investigations (OI) have continued to function in a professional, efficient, and responsible manner. Highlights of their efforts demonstrate the energies expended to make the GPO even better by identifying fraud, waste, abuse, and mismanagement. The IG's office is staffed with highly motivated professionals dedicated to their profession and for which I have had the pleasure to work with.

This will be my first and last semi-annual report as Inspector General for the Government Printing Office. It has been an honor and privilege to have served the staff of the OIG, the GPO, and the American public in this capacity. I am very proud for this opportunity and leave with the knowledge of having attempted to be fair with all concerned. I leave knowing the OIG staff will continue to meet its statutory obligations as an independent and objective force to promote the economy, efficiency, and effectiveness and to seek and identify fraud, waste, abuse, and mismanagement at the Government Printing Office.

Rodolfo Ramirez Jr.,
Inspector General


GOVERNMENT PRINTING OFFICE

HIGHLIGHTS OF THIS SEMIANNUAL REPORT



The Office of Audits and Inspections (OAI) issued two reports during this reporting period. Those reports included an audit of the agency's oversight of the Federal Digital System's (FDsys) master integrator contract as well as our annual report assessing GPO's Public Key Infrastructure (PKI) services. OAI also continued to oversee the Independent Verification and Validation (IV&V) efforts related to implementation of the Federal Digital System (FDsys) and the annual audit of GPO's financial statement.

OAI's significant accomplishments during this reporting period include the following:

- An audit of GPO's oversight of the Federal Digital System's (FDsys) Master Integrator (MI) contract showed that GPO did not implement key requirements of its Materials Management Acquisition Regulation (MMAR)—the Agency's primary guide for conducting procurements as well as other applicable criteria—in administering the contract. Specifically, the audit identified that GPO management did not (1) adequately oversee the contract, to include making effective use of a Contracting Officer's Technical Representative (COTR), to ensure that the contractor performed according to contract requirements, (2) protect the Agency's interest upon the initial indication of potential non-performance by the contractor, and (3) require adequate supporting documentation for contractor invoices before authorizing payment.
- Issued the results of an annual review conducted under contract by an Independent Public Accountant (IPA) on GPO's PKI services. GPO's PKI ensures the highest level of protection for electronic information that travels over ordinary, nonsecure networks. The IPA issued an unqualified opinion that management's assertion related to the adequacy and effectiveness of controls over its Certification Authority (CA) operations is, in all material respects, fairly stated.

The Office of Investigations (OI) opened ten investigations and 28 complaints for preliminary investigation, while closing 14 investigations and 32 complaints. At the end of this reporting period, OI had 21 ongoing investigations and two complaints. Sixteen investigations and 16 complaints were referred to GPO management for information or appropriate action.

More than 60 percent of the ongoing investigations involve allegations of procurement fraud. That number reflects continuing OI efforts to identify and investigate contract and financial fraud within GPO. This past reporting period, as a result of referrals from OI, GPO debarred two entities from doing business with the Agency.

The Department of Justice (DOJ) continues to work with OI on ongoing investigations into allegations of false statements, false claims, and collusive bidding. In furtherance of those investigations and others, the IG issued one subpoena for documents this reporting period.

OI's significant accomplishments during this reporting period include:

- One subject in an ongoing criminal investigation is seeking a plea agreement to one count of making false statements.
- OI initiated one Management Implication Report regarding the non-verification of shipping documentation by the GPO Finance and Administration Division, prior to GPO paying vendors for their services.

Personnel Update

During this reporting period, Vera Garrant joined OAI as a Supervisory Auditor. Vera comes to the OIG from the Department of Defense OIG where she was a Technical Specialist. Vera has over 27 years of Federal audit experience with several agencies, including the Internal Revenue Service, the Defense Contract Audit Agency, the Department of Health and Human Services OIG, and the National Aeronautics and Space Administration OIG. She is a graduate of New Hampshire College and is a Certified Public Accountant.

GPO MANAGEMENT CHALLENGES

The Government Performance and Results Act (GPRA) Modernization Act of 2010 defines major management challenge as "programs or management functions, within . . . agencies, that have greater vulnerability to waste, fraud, abuse, and mismanagement where a failure to perform well could seriously affect the ability of an agency or the Government to achieve its mission or goals." With this new definition, we update the list of management challenges we believe are critical for the Agency to address.

1. CUSTOMER SERVICE

To achieve its objectives as a 21st Century information processing and dissemination operation, GPO management must maintain the appropriate focus, staffing, and alignment with the Agency's Strategic Vision. The Agency recently updated the goals of its Strategic Plan. Its first goal is "It's All About the Customer"—to "understand, anticipate and meet the needs" of its customers. The Agency's second goal is to promote a more open and transparent Government by working with its customers in disseminating information through the use of all available technology. The culture and focus of customer service efforts must reflect a new way of thinking, and customers should come to GPO because they want—not because they must. Transformation of the traditional GPO customer relationship requires a continuing evolution toward what the Agency has called "world-class customer service."

Congress has previously introduced various bills to reduce or eliminate printing of the *Congressional Record* and bills or resolutions as cost-saving measures. The winner of the President's 2010 SAVE Award [Securing Americans' Value and Efficiency Award] suggested that GPO cease printing and mailing of thousands of copies of the *Federal Register* because most customers use the online version. During this challenging fiscal time, more than ever GPO customers will be looking for cost-effective products. This

GPO'S TOP 10 MANAGEMENT CHALLENGES

1. Customer Service.
2. Human Capital Operations and Management.
3. Federal Digital System.
4. Information Technology Security Management.
5. Acquisitions and Print Procurement.
6. Continuity of Operations.
7. Internal Controls.
8. Protection of Sensitive Information.
9. Financial Management and Performance.
10. Sustainable Environmental Stewardship.

presents an opportunity for GPO to continuously evolve and provide customers with cost-effective services and technologically advanced methods of information dissemination.

One continuing challenge for GPO in providing "world-class customer service" is customer agency billing and payments. Since 2001, GPO has relied in large part on the Department of Treasury's Intragovernmental Payment and Collection (IPAC), an electronic Internet-based collection and payment system for Federal agencies, to bill customer agencies for printing services. In the normal order and billing process, GPO first receives a request from a customer agency for printing and/or binding on a Standard Form (SF)-1, "Request for Printing and Binding." GPO awards a contract to a vendor/contractor to provide the printing. The print job is then delivered to the customer agency, and, after paying the contractor, GPO prepares the IPAC transaction documents to charge the agency. At the end of each month, GPO personnel access IPAC and retrieve the total costs due. IPAC transactions immediately affect GPO's revolving fund and the customer agency's respective accounts in the U.S. Treasury.

In 2004, the OIG reviewed the emerging issue of "chargebacks" by customer agencies, that is, agencies taking back funds electronically through IPAC from GPO's Revolving Fund. In FY 2004, the level of chargebacks exceeded $24 million. Our review found that incorrect customer billing code information, lack of purchase order documentation available to the agencies, and lax IPAC controls over chargebacks by customer agencies contributed to the problem. We specifically found that the "amount of staff time and resources expended—by both GPO and customer agencies—in performing duplicative activities, processes, or functions by having to re-charge agencies for appropriate costs is both inefficient and a waste of federal funds." Management accepted our recommendations to resolve these issues.

Unfortunately, the chargeback problem had not abated. In fact, as of March 2011, the IPAC chargeback balance exceeded $28 million. In April 2008, the IPAC chargeback balance was approximately $29 million. GPO management conducted a chargeback analysis during this reporting period. Based on at least seven previous studies or reviews on this issue (including our 2004 report), GPO management found that chargebacks are a "symptom of numerous process breakdowns," including incorrect order and billing information, inadequate and ineffective communication both inside the Agency on how to resolve this issue and outside with customers on how to provide correct order and billing information.[1]

One troubling finding is that GPO frequently double-bills customer agencies and "no root cause has been discovered." Such practices, the management analysis found, "impacts GPO's ability to provide effective customer service . . . and damages relationships with customer agencies."

The management analysis provides a general framework on how to move forward to tackle the chargebacks issue both in the short-term and long-term. The OIG asked KPMG, the independent financial statement auditor, to once again review this issue as part of the fiscal year 2011 financial statement audit. In addition, GPO management formed a multi-disciplined team to address the chargeback issue. As of September 2011, the team has successfully reduced the chargeback balance by approximately $9 million.

2. HUMAN CAPITAL OPERATIONS AND MANAGEMENT

The issues facing Human Capital (HC) operations and management at GPO have been identified as a significant management challenge for several semiannual

[1] An April 2007 GPO survey of agency customers found that almost 46 percent of customers were "dissatisfied" with GPO's billing process.

reporting periods. HC operations are at the heart of effectively accomplishing an agency's mission. In essence, HC provides services necessary to recruit, hire, develop, and retain the most precious and important source of productivity—the employees.

The Government Accountability Office (GAO) identified four critical areas related to Strategic HC Management that the OIG believes are relevant to GPO:

- *Leadership*. Top leadership must provide committed and inspired attention needed to address human capital transformation issues.
- *Strategic Human Capital Planning*. HC planning efforts must be fully integrated with mission and critical program goals.
- *Acquiring, Developing, and Recruiting Talent*. Agencies need to augment strategies to recruit, hire, develop, and retain talent.
- *Results-oriented Organizational Cultures*. Organizational cultures must promote high performance and accountability, empower and include employees in setting and accomplishing programmatic goals, and develop and maintain inclusive and diverse workforces reflective of all segments of society.[2]

HC has implemented a reorganization plan and added new staff to address the four areas that GAO cites to transform HC operations and management. During a previous reporting period, the Office of Personnel Management (OPM) issued audit findings about GPO's delegated competitive examining (DE) operations. OPM found that while most of the DE operations are being conducted compliantly, a "lack of a viable accountability system" contributed to two illegal appointments and resulted "in inconsistent operations as well as inefficiencies."

Among the significant findings of the OPM audit were that GPO (1) did not have a fully functioning accountability system that ensures efficient and compliant DE operations; (2) had significant problems in transaction processing, particularly regarding the critical "on-boarding process" that establishes new hires; (3) lacks consistent updated guidance concerning DE processes; (4) used HC Specialists in DE

work before completing certification training, which is prohibited by the Interagency DE Agreement with OPM; and (5) did not use annual trend data regarding opportunities to hire veterans, or the results of annual self-audits to improve program operations.

HC management acknowledged problems with timeliness and accuracy in its operations, particularly the time it takes from position announcement to on-boarding and transaction processing. HC management is addressing those issues, in part, through implementation of EmpowHR, an electronic system of HC processing, and by establishing employee performance goals that emphasize accuracy, timeliness, and customer service. We believe that for HC to successfully transform to a high-performing business unit, it must produce a change in its culture to achieve "results-oriented, customer-focused, and collaborative" HC solutions.

We also believe that the Agency faces challenges in effectively managing its workforce during a time when fiscal austerity and lean operations will be of paramount importance to the Agency. Our ongoing audit of payroll operations uncovered a significant level of overtime pay and employees on Leave Without Pay (LWOP) and Absent Without Leave (AWOL). In FY 2009, GPO expended $9.5 million in overtime pay and almost $11 million during FY 2010. Those totals amount to almost 4 percent of total payroll in FY 2009 and 4.6 percent in FY 2010. In addition, the number of employees on LWOP for significant periods of time remained high during both FY 2009

[2] GAO Report GAO-09-632T, http://www.gao.gov/new.items/d09632t.pdf.

and FY 2010. For example, in FY 2010, 413 employees were on LWOP for a total of 56,715 hours, or 7,089 days. A high number of employees were also listed as AWOL during the past two fiscal years: 114 in FY 2009 for a total of 5,983 hours and 83 in FY 2010 for a total of 4,804 hours.

As part of our payroll audit, the results of which we expect to issue during the next reporting period, we will be looking at the reasons for elevated levels of overtime, LWOP, and AWOL and making recommendations on how to effectively manage and decrease these labor costs and the resulting loss of productivity.

3. FEDERAL DIGITAL SYSTEM

The Federal Digital System (FDsys) was originally designed to be a comprehensive information life-cycle management system that will ingest, preserve, provide access to, and deliver content from the three branches of the Federal Government. The system is envisioned as a comprehensive, systematic, and dynamic means of preserving electronic content free from dependence on specific hardware and/or software. Because FDsys replaces GPO Access as the Agency's official information management system for electronic Government documents, the Agency must ensure that the system is robust, effective, and provides as much functionality as the increasing demands of electronic Government information require.[3]

FDsys has three major subsystems: the content management subsystem, the content preservation subsystem (accessible to GPO internal users only), and the access subsystem for public content access and dissemination. A multi-year, multi-release integration effort is being used to design, procure, develop, integrate, and deploy selected technologies and components of FDsys.

The OIG is responsible for Independent Verification & Validation (IV&V) work associated with developing and implementing FDsys. Under the supervision and direction of the OIG, American Systems conducts independent programmatic and technical evaluations of the FDsys program to verify whether system implementation is consistent with the FDsys project and cost plan and meets GPO

[3] In June 1994, GPO launched GPO Access, which provides online access to information from all three branches of the Federal Government.

requirements. Additionally, IV&V monitors development and program management practices and processes to anticipate potential issues and validates its findings through quarterly reports.

Background

The FDsys program has undergone substantial changes since its inception. During the fall of 2007, the schedule and scope for the first release was changed significantly and a final release with a reduced scope was planned for late 2008. In early 2008, GPO implemented a reorganization of the program with respect to Government and contractor participation and responsibilities, and implemented a new design for FDsys. The GPO FDsys Program Management Office (PMO) assumed the role of the Master Integrator previously held by a contractor. The PMO also assumed the responsibility for designing and managing system development. The original Master Integrator contractor and other contractors were assigned system development roles under the overall guidance of the PMO.

In January 2009, GPO deployed a public beta version of the FDsys access subsystem, containing 8 of the 55 data collections in the GPO Access system. The content management and content preservation subsystems, supporting the Internal Service Provider, Congressional Publishing Specialist, Preservation Specialist, and Report user roles, was released in late March 2009. Since deployment, the PMO has continued to update/upgrade the beta system and correct deficiencies identified during testing. In September 2010, the PMO announced that Release 1 was complete. However, while all coding and development was complete, several tasks remained outstanding, including completion of a Continuity of Operations (COOP) Instance and completion of a number of testing activities, including performance testing. In December 2010, the Public Printer announced that FDsys was the "official system of record" for GPO, three and one-half years later than originally planned.

Current OIG Concerns

Reduced Functionality. The declaration of FDsys as GPO's "official system of record" signified that all of the official versions of GPO content along with the source data resided in and was available in FDsys. Nevertheless, many of the services and functionality envisioned in Release 1, such as Library community requirements, have not been realized.

The initial requirements to be contained within Release 1 (for June 2007) totaled 1,835. When FDsys was declared GPO's official system of record in December 2010, the system contained approximately 1,171 requirements, which was substantially less functionality than originally anticipated.

The FDsys program is currently working on Release 2; however, much of the work to-date has not been the design and development of FDsys to original requirements; instead, the FDsys Program Management Office (PMO) has concentrated on outside agency requests for new Collections; further delaying the completion of FDsys as originally intended.

The FDsys program has reached a crossroads of sorts; requiring a decision on the future of the program. The extent of the FDsys design and development effort to the original requirements moving forward is unclear. Thus, it is unclear if FDsys will become the system it was originally envisioned to be. Factors that may influence that decision include the following:

- The FDsys program continues to work on outside government agency requests for new Collections resulting in the delay of design and development of FDsys based on documented requirements. The re-prioritization to accomplish this additional tasking continues to push the schedule out resulting in delayed functionality not only to FDsys but the stakeholder community.
- Anticipated funding for FDsys will be lower than previous levels which may require the program to scale back the capabilities and features of FDsys from what was originally envisioned.
- The FDsys program has decided not to implement requirements derivation processes (on original FDsys requirements) unless a new feature is added (to FDsys) that impacts those existing requirements. Development and testing of the original FDsys requirements could prove more difficult and result in additional errors.

- Over 400 Program Tracking Reports (PTRs) remain open with no definitive plan for working and closing them. The need to continually address this many problems will require diverting resources that could otherwise be used on further design and development of the original requirements.

Quality. Inconsistent and Incomplete Testing. A continuing concern for the FDsys program is the quality of the deployed system. Reliable testing is important to determine if FDsys can function appropriately and effectively as it receives more traffic from users. Though the testing effort has improved, it is maligned due to incomplete requirements and resource issues, including lack of time to thoroughly test the system as prescribed in the *FDsys Master Test Plan*. The pronouncement of FDsys as the system of record in December 2010 occurred prior to the completion of Release 1 testing.

Increased Costs. The total FDsys contract costs incurred as of the end of September 2011 was approximately $46 million (unaudited). Most of those costs were attributable to Release 1. The original contract to design and develop Release 1 was approximately $16 million. Substantial investments will continue to be required to complete the FDsys that was originally envisioned. Additionally, one of the goals of FDsys was to replace GPO Access. As this has taken longer than anticipated, it has necessitated the need for GPO Access to remain operational. Therefore, GPO is running GPO Access in parallel at a significant cost to the Agency. The Agency is now using GPO Access as an archive-only system.

Inadequate Program Management. The FDsys program does not consistently use proven and accepted standard program management practices. The PMO has not embraced techniques that would give the program more insight into progress, enabling better management and better opportunity for successful deployment within scope, cost, schedule, and quality goals. For example, while the PMO committed in response to an OIG recommendation to use Earned Value (EV) analysis to measure progress against cost and schedule, they have not done so. If used effectively, EV can provide an early warning of project performance problems while time is available for corrective action.

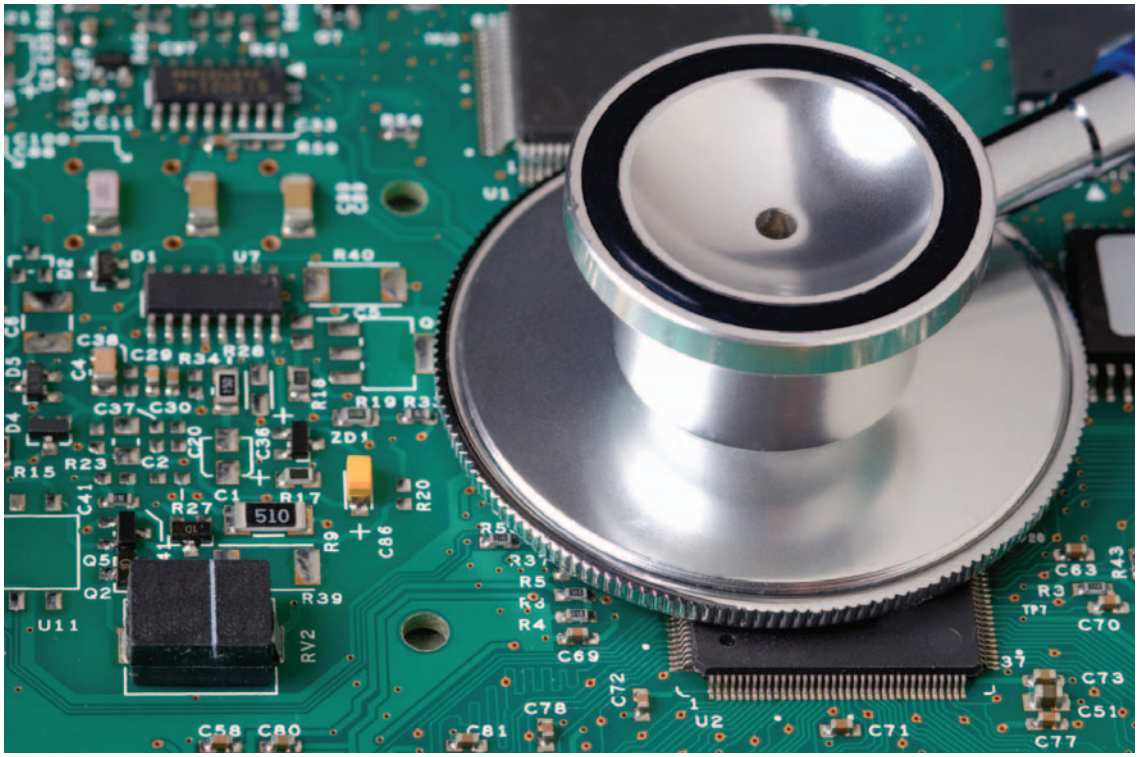
Transition Planning. As the FDsys moves forward, a growing concern is the status of the transition effort that is required for retirement of GPO Access. The *Transition Master Plan* containing required tasks and activities for retiring GPO Access has not been maintained since its initial development in January 2011. Therefore, it is unclear what work has been accomplished and what work remains to be done.

While continuing to have concerns regarding implementation of FDsys, we do not want to imply that the FDsys program lacks effort or has failed to produce a viable product. The FDsys Release 1 has received praise and notoriety for its look, feel, and ease of use. The PMO has also dealt with external commitments/requests (for example, availability of bulk data) that have altered internal priorities and resulted in the delay of work on the development of all the capabilities envisioned for the release. In addition, the migration of data from GPO Access to FDsys has been an extremely difficult undertaking and required more time and resources than the PMO originally anticipated.

We continue to believe that the primary challenges for the FDsys program are in the areas of program management, system engineering leadership, technical direction, and an adequate test program for the FDsys system. The goal of our on-going IV&V efforts is to report key risks and issues to the PMO and management and provide value-added recommendations that will help mitigate risks.

4. INFORMATION TECHNOLOGY SECURITY MANAGEMENT

Because GPO provides services to executive branch agencies that must comply with the Federal Information Security Management Act (FISMA) of 2002, GPO chose to substantially comply with the principles of the Act. The purpose of FISMA is to improve information security at Government agencies and Government contractors. Complying with FISMA continues to present additional challenges for GPO, including protecting sensitive Agency systems, information, and data.



During FY 2007, the OIG conducted a baseline assessment of compliance with FISMA to identify any gaps and deficiencies in GPO's overall information security program, including critical systems. We completed a full FISMA assessment in FY 2009. The scope included evaluating GPO progress in complying with FISMA based on the 2007 assessment. Our most recent assessment noted that while GPO has made some progress in complying with FISMA, additional improvements are needed. During this reporting period, the Information Technology and Systems (IT&S) office continued to make progress in addressing recommendations made in our 2009 assessment.

The Federal Government is shifting its IT security strategy from periodic security reviews to continuously monitoring and remediating IT security vulnerabilities. In February 2010, the National Institute of Standards and Technology (NIST) published Special Publication 800-37 Revision 1; *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*. The publication transformed the traditional Certification and Accreditation (C&A) process, which required detailed audits and inventories of Federal agency information systems. While providing a baseline of security controls for information assets, the C&A process did not address the real-time nature of threats to information systems.

We plan to initiate our next assessment of GPO's compliance with FISMA in early 2012. Our assessment approach will integrate the new NIST risk management framework and include an evaluation of GPO's ability to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

5. ACQUISITIONS AND PRINT PROCUREMENT

Acquiring goods and services and procuring printing on behalf of the executive branch remain critical challenges as GPO strives to transform the Agency and meet the changing needs of its customers. During FY 2010, GPO procured goods and services

valued at more than $600 million, approximately two-thirds of the Agency's consolidated expenses. Given this financial vulnerability, we are concerned that GPO has not fully assessed its acquisition programs to identify critical performance and oversight issues.

In 2008, OMB issued guidance to executive branch agencies on conducting internal reviews of the acquisition function required under OMB Circular No. A-123. Although not required to follow those guidelines, GPO manages and oversees procurement and production of printing on behalf of its executive branch customers. We, therefore, believe GPO (and its customers) would benefit greatly from an internal review of Customer Services (formerly Print Procurement) and Acquisition Services.

GPO also faces ongoing challenges with Agency contract management, as evidenced in part by our ongoing audit of FDSys contract administration and our continuing procurement fraud investigations. The rise in procurement fraud-related investigations and referrals by OI for suspension and debarment consideration further illustrate the need for greater contract oversight and contract officer training. During this reporting period, OI referred to management three complaints related to failures by contractors to follow the terms of GPO contracts. Through more efficient contract management and greater use of administrative contract remedies, GPO might have avoided the violations substantiated in those complaints. OI did not receive any formal response to those referrals.

Improving acquisitions by strengthening accountability, eliminating waste, improving performance, and targeting fraud and mismanagement are all necessary to protect the best interests of the taxpayers. In a time of budget cuts and constraints, GPO must do its part to effectively manage and protect procurement funds.

6. CONTINUITY OF OPERATIONS

GPO's ability to continue its mission essential functions during a disruption in operations continues to be a significant area of concern. GPO Directive 825.40, "Continuity of Operations Plan (COOP)," dated November 21, 2008, states that the agency established a COOP plan to provide for continuation of the Agency's essential functions and operations. The plan requires that activities be operational within 12 hours and that operations be sustained for up to 30 days. The Agency's essential functions are supporting the printing and electronic publishing requirements of Congress, production of the online *Federal Register* for the Office of the Federal Register, and blank passports for the Department of State.

The Agency has made considerable progress in relation to COOP actions and identified assorted risks and problems that it continues to work to resolve. During this reporting period, the Agency conducted its annual internal COOP exercise at the Laurel alternate facility. The results of that exercise will be reviewed during the next period. The Agency must continue to address those identified COOP risks and problems as it moves forward with establishing and ensuring that essential functions can continue during any COOP scenario.

7. INTERNAL CONTROLS

Effective internal controls over GPO programs and operations are critical to ensure that funds are used

for their intended purposes, programs achieve their goals and objectives, and GPO obtains the products and level of services for which it has contracted. To address this significant responsibility, GPO management establishes and maintains a system of internal controls for effective and efficient operations, reliable financial reporting, and compliance with laws and regulations. As the GAO notes in its *Standards of Internal Control in the Federal Government*, internal control "also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud." Almost all OIG audits include assessments of a program, activity, or function's control structure. Agency action to make internal controls the responsibility of all employees, but especially managers, must continue as a priority.

Although management recognizes the need for improving the internal control environment to successfully implement its strategic vision and planned future initiatives, Agency action is important because of implementation of Statement on Auditing Standards (SAS) No. 112, "Communicating Internal Control Related Matters Identified in an Audit." SAS No. 112 establishes standards and provides guidance on communicating matters related to an entity's internal control over financial reporting identified in a financial statement audit. The standard requires that the auditor communicate control deficiencies that are "significant deficiencies" and "material weaknesses."

KPMG is currently auditing the Agency's FY 2011 consolidated financial statements and assessing the status of FY 2010 findings that included significant deficiencies related to internal control over financial reporting. Those deficiencies included inadequate controls for the preparation, review, and approval of special journal entries; and processing and maintenance of human resource data. In addition, KPMG noted deficiencies in the design and/or operations of information technology (IT) general and application controls. KPMG did not consider any of those deficiencies to be material weaknesses. An evaluation of internal controls will continue to be an area of emphasis for all OIG audits.

8. PROTECTION OF SENSITIVE INFORMATION

After several recommendations from this office, GPO has begun to establish rules of conduct and appropriate administrative, technical, and physical safeguards that adequately identify and protect sensitive information. Failure to have such rules and safeguards could result in harm, embarrassment, inconvenience, or unfairness to individuals and GPO, including possible litigation. Of particular importance is the need to safeguard against and respond to any breach of personally identifiable information (PII), including personal information in both information systems and paper documents.

FISMA requires that each agency establish rules of conduct for persons involved with PII, establish safeguards for PII, and maintain accurate, relevant, timely, and complete PII information. As reported in OIG Report 07-09, "GPO Compliance with the Federal Information Security Management Act (FISMA)," dated September 27, 2007, and again in our FISMA Report 10-03 dated January 12, 2010, GPO is progressing with efforts to protect PII contained in information systems. GPO Directive 825.41, "Protection of Personally Identifiable Information," issued March 30, 2010, establishes a framework for protecting PII at GPO.

In response to recommendations included in a February 2009 Management Implication Report regarding the handling of PII, the Public Printer appointed a senior-level manager as Privacy Officer (PO). GPO also hired a new privacy program manager to help the PO implement GPO Directive 825.41. Our next FISMA assessment, which is scheduled to begin in early 2012, will evaluate GPO's implementation of GPO Directive 825.41 to protect sensitive information.

9. FINANCIAL MANAGEMENT AND PERFORMANCE

Over the years, financial management and performance has been identified by many agencies, including GPO, as a significant management challenge. Federal agencies continue to face challenges providing timely, accurate, and useful financial information and managing results. Better budget and performance integration has become even more critical for results-oriented management and efficient allocation of scarce resources among competing needs. OIG auditors and the contractors they oversee are vital in keeping the Federal Government's financial information and reporting transparent, valid, and useful to agency decision makers and other stakeholders.

GPO has completed migration of current business, operational, and financial systems, including associated work processes, to an integrated system of Oracle enterprise software and applications known as the Oracle E-Business Suite. This system is intended to provide GPO with integrated and flexible tools that support business growth and customer technology requirements for products and services.

The OIG continues to oversee the activities of KPMG, the IPA conducting the annual financial statement audit. KPMG expressed an unqualified opinion on GPO's FY 2010 financial statements, stating that the Agency's financial statements were fairly presented, in all material respects, in conformity with generally accepted accounting principles. Although GPO addressed previous material weaknesses, KPMG identified two significant deficiencies it did not consider material weaknesses: (1) financial reporting controls and (2) IT general and application controls. With respect to financial reporting controls, KPMG identified specific deficiencies concerning the recording of special journal entries in the wrong general ledger account and/or recorded in the wrong amount; and the use of a methodology that resulted in ineligible employees receiving goal sharing payments. KPMG also noted deficiencies in the reconciliation of annual leave balances, payment plans, and service computation dates.

Deficiencies with the design and/or operations of GPO's IT general and application controls were noted in security management, access controls, segregation of duties, configuration management, and contingency planning. Financial management and performance and the Agency's ability to provide timely, accurate, and useful financial information will continue to be a management concern. Each of the identified weaknesses and deficiencies will be followed up on as part of the FY 2011 financial audit, which is in progress.

Although not affecting the audit opinion, some issues continue to hamper the Agency with respect to financial management and performance. For example, as mentioned in the "Customer Service" management challenge, customer agency billing and payments continue to be an issue.

In January 2009, KPMG wrote in its management letter for the financial statement audit that internal controls over the IPAC billing process needed to be strengthened. KPMG observed that the major reason for the chargebacks was that GPO "is not gathering and/or validating key customer billing information" in the ordering process, which causes the agency being billed to reject the IPAC invoice. KPMG noted that the chargeback problem could "overstate accounts receivable in the consolidated financial statement" and also takes an inordinate amount of time and resources to investigate and resolve.

The Agency stated in its 2010 financial statements that GPO billed customers about $958 million for printing and binding services, including congressional services funded by appropriations, during FY 2010. The U.S. Department of the Treasury's

IPAC System was used to collect about $741.5 million, or 77.4 percent of this debt from customers. Additionally, about $77.4 million, or 8.1 percent of this debt, was collected from funds held in customer Printing and Binding Deposit Accounts maintained by GPO and another $17.2 million, or 1.8 percent, was collected through credit cards. Such electronic-based methods allow prompt collection of funds, rather than the more traditional methods of collection.

IPAC chargebacks, included in accounts receivable, totaled approximately $26.4 million at the end of FY 2010 and exceeded $28 million as of March 2011. During FY 2011, GPO management formed a team to collect the chargebacks from other Federal agencies. As a result, GPO has reduced the chargeback balance from the $26.4 million at FY 2010 yearend to about $17.5 million as of September 2011. The OIG intends to continue monitoring this issue during KPMG's audit of the FY 2011 financial statements.

10. SUSTAINABLE ENVIRONMENTAL STEWARDSHIP

As the largest industrial manufacturer in the District of Columbia, GPO has always faced challenges to become more environmentally sensitive.

We continue to urge adoption of principles consistent with sustainable environmental stewardship objectives. First, we encourage management and Congress to renew efforts to evaluate a new facility that would more appropriately meet Agency needs and be more energy efficient. A more energy efficient and environmentally conscious facility not only fits with the Agency's environmental stewardship initiative but also meets the environmental and economic objectives for Congress and the Administration.

We also continue to encourage management to promote and incorporate "green thinking" into all of its business processes through performance metrics, reward programs, and other means. For example, the OIG has recommended an integrated approach to green acquisition such as that espoused in Executive Order 13514, which sets sustainability goals for Federal agencies and focuses on making improvements in their environmental, energy, and economic performance. Although not required to adhere to the Executive Order, we believe that it is beneficial for management to adopt its tenets and develop written policies for purchasing environmentally sustainable goods and services, monitor compliance annually and fix shortcomings, and provide

training on making purchases that are environmentally sound and comply with the spirit of the order.

To meet those challenges, GPO should have a dedicated environmental executive who will address the issues across Agency business units and directly with officials in other legislative branch agencies.

We have included in our work plan a review of energy use at GPO to determine whether a comprehensive plan exists for implementing energy-related projects, as part of an overall plan that helps reduce emissions, energy consumption, and energy costs. We hope to begin the audit in the near future and look forward to working with Agency personnel in achieving a long-term and sustainable environmental stewardship program.

OFFICE OF AUDITS AND INSPECTIONS

OAI conducts independent and objective performance and financial audits relating to GPO operations and programs, and oversees the annual financial statement audit conducted by an IPA. OAI also conducts short-term inspections and assessments of GPO activities, which generally focus on issues limited in scope and time. Audits are performed in accordance with generally accepted government auditing standards that the Comptroller General of the United States issues. When requested, OAI provides accounting and auditing assistance for both civil and criminal investigations. OAI refers to OI for investigative consideration any irregularities or suspicious conduct detected during audits, inspections, or assessments.

A. SUMMARY OF AUDIT AND INSPECTION ACTIVITY

During this reporting period, OAI issued two new reports. The OAI also completed a peer review of the Peace Corps OIG's audit function. OAI also continued its work with management to close open recommendations carried over from previous reporting periods. GPO management has made significant progress in closing open audit and assessment recommendations. As a result, as of September 30, 2011, a total of 27 recommendations from previous reporting periods remain open.

B. FINANCIAL STATEMENT AUDIT

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG is conducting the FY 2011 audit under a multiyear contract for which OAI serves as the Contracting Officer's Technical Representative (COTR). The oversight provided ensures that the audit complies with Government Audit Standards. OAI also assists with facilitating the external auditor's work as well as reviewing the work performed. In addition, OAI provides administrative support to KPMG auditors and coordinates the audit with GPO management.

KPMG previously issued an unqualified opinion on GPO's FY 2010 financial statements, stating that the Agency's financial statements were fairly presented, in all material respects, and in conformity with generally accepted accounting principles. KPMG identified three significant deficiencies, which it did not consider to be material weaknesses. Those deficiencies were controls over special journal entries, control over human resource data, and IT general and application controls. KPMG did not disclose any instances of noncompliance with certain provisions of laws, regulations, and other matters required to be reported under Government Audit Standards.

During this reporting period, KPMG began work on the FY 2011 audit of GPO's consolidated financial statements.

C. AUDIT AND INSPECTION REPORTS

1. Audit Report 11-07 (Issued August 19, 2011)

http://www.gpo.gov/pdfs/ig/audits/11-07_Final-RptAuditFDsysMICont_08-19-11.pdf

GPO Oversight of the Federal Digital System Master Integrator Contract

In 2004, as part of its mission of Keeping America Informed, GPO embarked on the Federal Digital System (FDsys) project to replace *GPO Access* as an improved means of providing public access to electronic documents for all three branches of the Federal Government. GPO awarded the FDsys Master Integrator (MI) contract to Harris Corporation Government Communication Systems Division of Melbourne, Florida (Harris). As MI, Harris was required to design, develop, and then integrate the various FDsys components, technology, and applications. Initially, GPO planned for the basic FDsys functionality to be operational by July 2007, at a cost of $16 million.

Because of GPO dissatisfaction with Harris' performance, in April 2008, the Agency issued a contract modification which reduced the scope of work for Harris and transferred MI responsibilities to GPO's FDsys Program Management Office (PMO). GPO assigned Harris other lesser system development roles under the overall guidance of the FDsys PMO. The reorganization moved the PMO to the Office of Information Technology and Systems (IT&S) within the organization of GPO's Chief Information Officer (CIO). In addition, the PMO replaced the Harris design for FDsys with a new design strategy that included the predominant use of commercial-off-the-shelf software. With the new modification and decreased Harris responsibilities, contract costs increased from an initial planned cost of $16 million to more than $21 million. GPO did not retain Harris when the contract's period-of-performance ended in December 2008. Subsequently, on December 21, 2010, GPO announced FDsys as its official Web site (www.fdsys.gov) for disseminating electronic Government information, three years behind schedule, with less functionality than originally planned, and a total program cost of $44.4 million.

The OIG performed an audit of the Agency's oversight of the FDsys MI contract to determine whether GPO effectively administered the contract with Harris Corporation. The audit showed that GPO did not implement key requirements of its Materials Management Acquisition Regulation (MMAR)—the Agency's primary guide for conducting procurements as well as other applicable criteria—in administering its contract with Harris as the MI for FDsys. Specifically, the audit identified that GPO management did not:

- adequately oversee the contract, to include making effective use of a Contracting Officer's Technical Representative (COTR), to ensure that Harris performed according to contract requirements;
- protect GPO's interest upon the initial indication of potential non-performance by Harris Corporation; and
- require adequate supporting documentation for contractor invoices before authorizing payment.

As a result, GPO paid Harris more than $5 million in excess of the original contract price for significantly less work than the contract initially required and for potential non-performance. In addition, because management did not obtain adequate supporting documentation for invoices Harris submitted, the Agency potentially paid for costs that were unallowable and unreasonable.

We recommended that GPO develop written policy on administering acquisitions that include statements about the composition, roles, responsibilities, and training requirements of acquisition teams; procedures for conducting contractor oversight including developing quality assurance surveillance plans; incorporating the use of COTRs in the acquisition process; taking appropriate action to protect GPO's interest in the case of potential contractor non-performance; and maintaining complete contract files. A recommendation was also made to modify Agency training courses on project management to include composition of the acquisition team and their roles in project management, use of formal project documents in successful project management such as a project plan, acquisition plan, and project charter; and techniques for effective oversight of outside contractors in project management. Management concurred with each of the recommendations and has planned responsive corrective actions.

2. Assessment Report 11-08 (Issued September 30, 2011)

http://www.gpo.gov/pdfs/ig/audits/11-08_FinalReportGPOPKICertificationAuthority_09-29-11.pdf

Assessment of GPO's Public Key Infrastructure Certification Authority–Attestation Report

GPO implemented a PKI to support its "born digital and published to the web" methodology to meet GPO customer expectations of being official and authentic. The GPO PKI also directly supports GPO's mission related to electronic information dissemination and e-Government. The GPO Certification Authority (CA) issues, signs, and manages the public key certificates in secure facilities based in Washington, D.C. The GPO PKI is cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification provisions require that the GPO PKI undergo an annual compliance review.

To satisfy this compliance requirement, the OIG tasked Ernst & Young to conduct a WebTrust assessment of its CA. The assessment, for the period of July 1, 2010, through June 30, 2011, was conducted in accordance with the American Institute of Certified Public Accountants (AICPA) WebTrust Principles and Criteria for Certificate Authorities and Statement on Standards for Attestation Engagements (SSAE) Number 10. The assessment represents an evaluation of whether GPO's assertion related to the adequacy

and effectiveness of controls over its CA operations is fairly stated based on underlying principles and evaluation criteria.

The scope of the assessment included the following entities involved with operating the GPO CA:

- CA policies and procedures;
- Registration authorities;
- CA and repository; and
- CA supporting systems, databases, and PKI facilities.

The assessment also measured the GPO CA's compliance with reporting requirements of the Federal Public Key Infrastructure Policy Authority.

As a result of work performed, Ernst & Young issued two Attestation Reports which express their unqualified opinion that (1) GPO management's assertion related to the adequacy and effectiveness of controls over its CA operations is, in all material respects, fairly stated based on the AICPA WebTrust for Certification Authorities Criteria, and (2) GPO management's assertion related to its CA operations compliance with the requirements of the FPKIPA is fairly stated in all material respects. E&Y also issued a Letter of Supplementary Information to address additional FPKIPA reporting requirements.

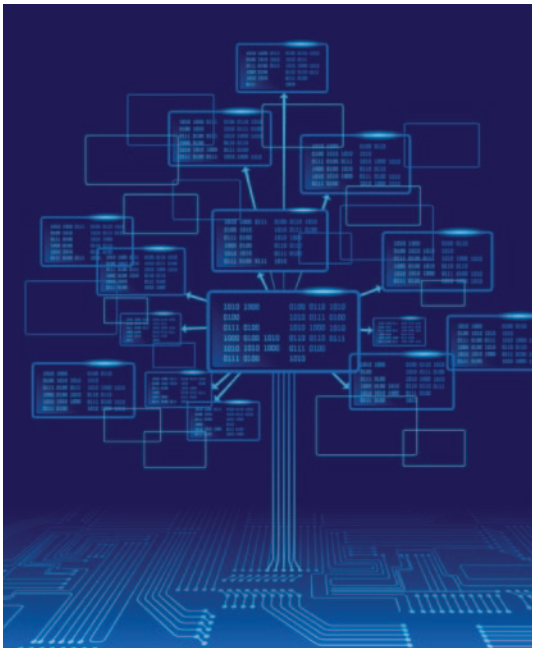
D. STATUS OF OPEN RECOMMENDATIONS

Management officials made progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. For the 27 recommendations still open, a summary of the findings and recommendations, along with the status of actions for implementing the recommendation and OIG comments, follow.

1. Assessment Report 09-01 (Issued November 4, 2008)

http://www.gpo.gov/pdfs/ig/audits/09-01.pdf

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability



FINDING

The OIG contracted with American Systems, a company with significant experience in the realm of IV&V for Federal civilian and Defense Agencies, to conduct IV&V for the first public release of FDsys. As part of its contract, the contractor is assessing the state of program management, technical and testing plans, and other efforts related to this public release. The contractor is required 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 process in controlling risk. During the period the report covers, GPO launched a public beta version of FDsys containing a limited number of collections. This fourth quarterly report provides an overview of the key risks and issues identified by the FDsys IV&V team from April through June 2008, including security requirements and risk management.

RECOMMENDATION

The OIG made five recommendations to management intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

One recommendation remains open for which management continues to work on implementing corrective actions.

2. Assessment Report 09-03 (Issued December 24, 2008)

http://www.gpo.gov/pdfs/ig/audits/09-03.pdf

Federal Digital System (FDsys) Independent Verification and Validation (IV&V)–Fifth Quarter Report on Risk Management, Issues, and Traceability

FINDING

This fifth quarterly report provides an overview of the key risks and issues identified by the FDsys IV&V team from July through September 2008, including those related to the FDsys detail design and system integration testing as well as technical, schedule, and cost risks the program faces.

RECOMMENDATION

The OIG made ten recommendations to management intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with six of the recommendations, partially concurred with one, and nonconcurred with three. Management proposed responsive corrective actions to six of the recommendations. Although we disagreed with management's position on the remaining four recommendations, we accepted management's proposed alternative corrective actions.

OIG COMMENTS

One recommendation remains open. Management continues to take responsive actions to implement the remaining recommendation.

3. Assessment Report 09-07 (Issued March 20, 2009)

http://www.gpo.gov/pdfs/ig/audits/09-07_sep.pdf

Federal Digital System (FDsys) Independent Verification and Validation (IV&V)–Sixth Quarter Report on Risk Management, Issues, and Traceability

FINDING

This sixth quarterly report provides an overview of the key risks and issues identified by the FDsys IV&V team from October 2008 through January 9, 2009, including security, and the state of program activities required for deployment, as well as technical, schedule, and cost risks.

RECOMMENDATION

The OIG made four recommendations intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

One recommendation remains open. Management continues to take responsive actions to implement the open recommendation.

4. Assessment Report 09-12 (Issued September 30, 2009)

http://www.gpo.gov/pdfs/ig/audits/09-12_sep.pdf

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Seventh Quarter Report on Risk Management, Issues, and Traceability

FINDING

This seventh quarterly report for the period January 1, 2009, through May 8, 2009, identifies critical technical, schedule, and cost risks for the FDsys Program. The report provides a high-level overview of the key risks and issues that IV&V identified during the reporting period. The report also discusses IV&V assessments covering FDsys security and the state of program activities required for deployment performed over the same time period.

RECOMMENDATION

The OIG made 25 recommendations designed to strengthen FDsys program management, particularly for future FDsys releases.

MANAGEMENT COMMENTS

Management generally concurred with all recommendations, with the exception of one, and proposed responsive corrective actions for each.

OIG COMMENTS

Two recommendations remain open for which the OIG and IV&V continue to monitor the status of their implementation.

5. Assessment Report 10-01 (Issued December 2, 2009)

http://www.gpo.gov/pdfs/ig/audits/10-01_Final-RptFDsysIVQtr9.pdf

Federal Digital System (FDsys) Independent Verification and Validation – Ninth Quarter Report on Risk Management, Issues, and Traceability

FINDING

This ninth quarterly report for the period July 1, 2009, through September 30, 2009, identifies critical technical, schedule, and cost risks for the FDsys Program. The report provides a high-level overview of the key risks and issues that IV&V identified during the reporting period. The report also discusses IV&V assessments covering FDsys security and the state of program activities required for deployment performed over the same time period.

RECOMMENDATION

The OIG made 11 recommendations to management designed to strengthen FDsys management.

MANAGEMENT COMMENTS

Management generally concurred with the recommendations and has either taken or proposed responsive corrective actions.

OIG COMMENTS

Two recommendations remain open for which the OIG and IV&V continue to monitor the status of their implementation.

6. Assessment Report 10-03 (Issued January 12, 2010)

GPO's Compliance with the Federal Information Security Management Act

FINDING

FISMA requires that each executive branch agency develop, document, and implement an agency-wide program for providing information security for the

information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Although a legislative branch agency, GPO recognizes the need to be FISMA compliant because of the services it provides, including services to executive branch agencies.

In FY 2007, the OIG contracted with a consulting firm to perform a baseline assessment of GPO's FISMA compliance and to evaluate the design and effectiveness of the controls over GPO's information security program, policies, and practices. We completed a full FISMA assessment in FY 2009. The assessment was performed using the most recent applicable FISMA requirements and guidelines published by OMB and NIST. Significant emphasis was placed on evaluating the GPO systems used for providing services to client agencies. The OIG issued a sensitive report concluding that GPO made some progress in complying with FISMA, but that additional improvements are needed. In addition, many of the weaknesses identified during the FY 2007 baseline assessment still exist.

RECOMMENDATION

The OIG made a total of 21 recommendations, which, if implemented, will help further move GPO toward FISMA compliance.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

Management continues to work with the OIG to implement corrective actions on the remaining ten open recommendations.

7. Audit Report 11-01 (Issued December 16, 2010)

Government Printing Office's Ethics Program

FINDING

An agency's ethics program is the formalized means by which senior management can educate and enlighten agency employees and prevent or detect employee misconduct and violations of ethics regulations. An effective ethics program inspires employees not only to comply with ethics regulations, but also fulfill the highest ideals of public service and provide the public with full faith and confidence that the agency's mission, programs, and functions are fair and impartial.

An audit of the Agency's ethics program was performed to determine whether GPO complied with applicable Federal ethics guidance and the ethics program at GPO was consistent with Federal Government best practices. Although it did not identify specific instances of ethics violations or noncompliance, the audit did find that GPO did not have an established ethics program consistent with Federal Government best practices.

RECOMMENDATION

The OIG made two recommendations, which, if implemented, should improve the Agency's ethics program and, in turn, the Agency's overall ethical culture.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

Management continues to work with the OIG to implement corrective actions on the two open recommendations.

8. Audit Report 11-02 (Issued December 6, 2010)

Control and Accountability of Laptop Computers

FINDING

Government-issued notebook or laptop computers are at risk of loss and theft because of their high value, portability, and ease of concealment. Because of their ability to store large amounts of data, lost or stolen laptops also create a risk of exposing PII and sensitive Government information. The inability to account for laptops has been prevalent throughout the Federal Government, and the GPO has experienced instances of missing laptops.

The audit found that based on our testing of a statistical sample of laptops issued to personnel between 2005 and 2009, we estimated with 99-percent confidence that GPO could not account for between 150 and 213 laptops. The purchase price value of the missing laptops was between $331,500 and $470,730. Agency management could not provide an explanation as to the location of the missing laptops. The audit further showed that GPO could not account for the laptops in part because management did not establish standard operating procedures to implement written policies on property control and accountability for laptops. In addition, internal controls within GPO for preventing the loss of laptops need improvement as evidenced by the inability of the Agency to produce reports of either acquisition or disposition of laptops, or to account for laptops from purchase to final disposition. GPO also did not meet its objectives outlined in GPO Instruction 705.29, "IT End User Asset Management,", November 5, 2005, for maintaining a centralized end user asset management program that verifies duplicative purchases are not made, and gathers information for disaster recovery planning.

RECOMMENDATION

The OIG made a total of seven recommendations, which if implemented, should help improve control and accountability over the Agency's laptop computers.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

Management continues to work with the OIG to implement corrective actions on the seven open recommendations.

9. Audit Report 11-06 (Issued March 31, 2011)

Secure Card Personalization System Information Technology Security Controls

FINDING

GPO provides personalized smartcards and identity cards for customers throughout the Federal Government. The Secure Card Personalization System (SECAPS) is the automated system used for producing the cards. SECAPS was developed

Table of Open Recommendations

AUDIT	NUMBER OF OPEN RECOMMENDATIONS	NUMBER OF MONTHS OPEN
09-01 Federal Digital System (FDsys) Independent Verification and Validation (IV&V)–Fourth Quarter Report on Risk Management, Issues, and Traceability	1	34
09-03 FDsys IV&V–Fifth Quarter Report on Risk Management, Issues, and Traceability	1	33
09-07 FDsys IV&V–Sixth Quarter Report on Risk Management, Issues, and Traceability	1	30
09-12 Federal Digital System (FDsys) Independent Verification and Validation (IV&V)–Seventh Quarter Report on Risk Management, Issues, and Traceability	2	24
10-01 FDsys IV&V–Ninth Quarter Report on Risk Management, Issues, and Traceability	2	21
10-03 GPO's Compliance With the Federal Information Security Management Act	10	20
11-01 GPO's Ethics Program	2	9
11-02 Control and Accountability of Laptop Computers	7	9
11-06 Secure Card Personalization System Information Technology Security Controls	1	6

by GPO through a contract with General Dynamics Information Technology and designed to create personalized embossed identity cards, Homeland Security Presidential Directive No. 12 (HSPD-12) compliant smartcards, and high-frequency radio frequency identification cards. GPO produces cards for the Department of Homeland Security's Customs and Border Protection's Trusted Traveler Program and for the Center for Medicare and Medicaid Services in the Department of Health and Human Services.

We issued a sensitive report that identifies opportunities to strengthen IT security controls and further reduce the potential risk of system compromise.

RECOMMENDATION

The OIG made a total of three recommendations, which if implemented, should help strengthen IT

security controls and further reduce the potential risk of system compromise.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

Management continues to work with the OIG to implement corrective actions on the one remaining open recommendation.

OFFICE OF INVESTIGATIONS

OI receives and evaluates complaints and conducts investigations related to fraud, waste, and abuse in GPO programs and operations. OI remains focused on procurement fraud investigations, but also investigates allegations of bribery, false statements, theft, and other employee and contractor misconduct.

Investigations that substantiate violations of Federal law, GPO Directives, or contract terms/specifications may result in administrative sanctions, civil action, or criminal prosecution. Such actions can include employee terminations, contractor debarments, and court-imposed prison terms, probation, fines, or restitution. OI may also issue Management Implication Reports to the Agency that detail systemic problems or vulnerabilities and offer recommendations on how to correct them.

OI conducts investigations at all GPO locations, including its 15 Regional Printing Procurement Offices and potentially thousands of contract print vendors nationwide. It maintains a close relationship with GPO Security Services and the Uniform Police Branch to coordinate law enforcement efforts impacting GPO. Liaison is also maintained with DOJ, the OIG community, and other law enforcement agencies and organizations.

A. SUMMARY OF INVESTIGATIVE ACTIVITY

At the end of last reporting period, 32 complaints were open. OI opened 28 new complaint files, of which 10 were opened into full investigations. Additionally, 19 complaints were closed with no action, 16 were referred to other law enforcement organizations, and 13 were referred to management. At the end of the reporting period, two complaints were open.

At the end of last reporting period, 31 investigations were open. During this reporting period, 10 investigations were opened and 20 were closed. Sixteen of the closed investigations were referred to management, and one was closed with the Agency having taken action.

During the last six months, OI made eight presentations to DOJ officials. Those presentations resulted in one criminal acceptance and one civil acceptance. OI continues to work with DOJ on several ongoing investigations.

The IG issued one subpoena to further ongoing criminal, civil, and administrative investigations. Documents requested included financial records, bid preparations, production records, and agreements among contractors and/or affiliated companies.

B. TYPES OF CASES

Procurement Fraud

OI continues to focus its investigative resources on identifying and investigating procurement fraud. The investigations focus on contractor and GPO employee misconduct that adversely impacts the contracting process. Violations include false statements, false claims, product substitution, collusive bidding, bribery, kickbacks, and financial conflicts of interest. In FY 2010, GPO procured more than $600 million in goods and services through contracting. That figure includes at least $450 million in contracts awarded to print contractors selected from a pool of over 15,000 of pre-qualified vendors. OI recognizes print procurement as a significant risk area and procurement fraud investigations represent more than 60 percent of the OI case inventory. Including allegations in complaint status, OI has 24 open procurement investigations.

The OI frequently receives allegations of contractor misconduct that result in minimal financial loss to GPO. DOJ often declines these cases for civil and criminal prosecution because they do not meet the financial thresholds necessary to justify involving an Assistant U.S. Attorney. To encourage the use of administrative action against this type of misconduct, the OI increased suspension and debarment referrals from only one in FY2010 to ten in FY2011. Because of those referrals, GPO debarred 12 subjects in FY11—three times the number debarred in the last two fiscal years.

Workers' Compensation Fraud

OI also investigates GPO employees who allegedly submit false claims or make false statements to receive workers' compensation benefits. Investigations may result in criminal prosecutions, civil recoveries, or administrative action levied against employees by GPO or the Department of Labor. OI has three ongoing investigation involving allegations of workers' compensation fraud.

Employee Misconduct

OI routinely investigates allegations of employee criminal and administrative misconduct. Allegations can be violations of Federal and local laws or failures to follow GPO Directives. Penalties for employee misconduct range from verbal counseling to termination and/or criminal prosecution. OI has two open complaints and three full investigations involving alleged employee misconduct.

Proactive Initiatives

While conducting reactive investigations, OI may identify business units, programs, and/or procurements that are vulnerable to fraud. In those instances, OI may open proactive initiatives to identify whether fraud or other criminal activity has in fact occurred. The findings of proactive initiatives result in Management Implication Reports or spin-off investigations of procurement fraud, employee misconduct, or other types of violations. During the last reporting period, OI opened a proactive initiative to identify worker's compensation fraud.

Other Investigations

OI conducts other types of investigations that do not fall into one of the previous categories. Examples of those types of investigations include unauthorized use or access to GPO systems, and requests for information or assistance from outside entities.

C. SUMMARY OF INVESTIGATIVE ACCOMPLISHMENTS

Criminal and Civil Cases

OI continues an investigation of allegations of false statements, false claims, forgery, or bid collusion by GPO print vendors. One subject pled guilty to one count of false statements and was sentenced to three years probation, six months house arrest, and a $2,000 dollar fine. OI has the assistance of the DOJ Civil Division, which is in the process of evaluating the case.

Internal Administrative Cases

OI referred to management the findings of an investigation into allegations a GPO employee received over $2,100 in unauthorized travel reimbursements via the Government Travel Card and Government Purchase Card Programs. The investigation revealed management approved unauthorized travel expense reimbursement for charges made to the employee's Government Purchase card, thereby paying for the same charges twice. GPO has since instituted vendor charge code limitations to its Government Purchase Cards and is seeking full restitution from the former employee.

OI referred to the GPO, Office of General Counsel; GPO management; and the Department of Labor (DOL), Office of Worker's Compensation Program (OWCP), Regional Director, the findings of an investigation into allegations a GPO employee had employment outside of the GPO while receiving Worker's Compensation benefits. The investigation revealed the employee had outside employment while receiving OWCP benefits and made false statements on the documents they submitted to receive the benefits. Determination of administrative action is pending.

External Administrative Cases

As previously reported, OI referred to the Office of General Counsel for consideration of suspension/debarment the findings of an investigation into allegations that a GPO contractor submitted a fraudulent shipping receipt and invoice to GPO for payment. The investigation revealed the company falsified Bills of Ladings to received GPO payment prior to the actual shipping date of the products contracted. During this reporting period, the contractor and company were debarred from doing business with GPO beginning August 15, 2011, and ending August 14, 2014.

OI referred to the Office of General Counsel, for consideration of suspension and debarment, the findings of the following seven investigations:

- OI investigation established that a GPO contractor submitted false claims to GPO for payment on a contract. The contractor fabricated shipping receipts at dollar amounts higher than the actual shipping costs accrued by the contractor. The contractor then submitted the fabricated shipping receipts to GPO in order to receive payment.
- OI investigation established that a GPO contractor who had a history of compliance issues with GPO, had in fact started to use the name of another GPO contractor (with their permission) when bidding on GPO solicitations. The contractor did this in order to still receive GPO contract considerations from GPO. This referral for suspension and debarment applied to both contractors involved.
- OI investigation established that a GPO contractor pre-billed and submitted false shipping documentation to GPO for payment. In part the contractor admitted to fabricating shipping documents in order to make it appear he sent materials before the "due-by" date when in reality he shipped the materials after the "due-by" date. The contractor stated he did this in order to preserve his performance record with GPO as to not affect his chances of receiving future contracts.

- OI investigation established a contractor registered five fictitious companies with GPO and misrepresented their production capability to garner contracts. Subsequently, two of the five companies were awarded a total of 229 GPO contracts valued at $538,546 dollars.
- OI investigation established a contractor violated GPO Certificate of Independent Price Determination Policy by simultaneous bidding for two family-run businesses. This resulted in over 370 GPO print contracts, to include bids placed fraudulently, through a deceased owner's contractor account, which resulted in the awarded of 17 contracts valued at $4,061. The contractor acknowledged understanding GPO's policy and admitted to violating those requirements.
- OI investigation and analysis of documents received via IG Subpoena disclosed a contractor failed to meet contract specifications for five print contracts awarded by GPO. The contractor certified that all contract requirements were met and billed GPO for the full amount. One contract was terminated for default and the total loss to GPO for all contracts was estimated between $11,900 and $16,000.
- OI investigation established a contractor created a "Front" company to circumvent adverse GPO action related to the contractor's poor contract performance and compliance issues. In addition, the contract also admitted to falsifying shipping documentation in order to receive early payment.

D. MANAGEMENT IMPLICATION REPORTS

As previously reported, OI issued a Management Implication Report in November 2010 summarizing concerns and offering recommendations to improve supervisory controls, employee accountability, safety and productivity, and efficient use of human resources in Plant Operations. An OI investigation in part found that Plant Operations management had no general accountability for their second and third shift employees; some supervisors knew that employees frequently were AWOL, but took no disciplinary action against them; and the second and third shifts are potentially overstaffed, creating the opportunity for employee misconduct.

In June 2011, management responded to the MIR and concurred with all recommendations. Management further indicated they took or intend to take the following actions to address OI's recommendations:

- Plant Operations established rating criteria for frontline supervisors that focus on operational performance.
- The Press Division implemented policies and instructions for assigning employees to equipment. Plant Operations changed its policy document to reflect that "Supervisors will be held accountable for their employees' whereabouts."
- The Technical Manager of Strategic Planning and Analysis has been and will continue to capture overtime hours and study equipment utilization.

Also as previously report, OI issued an MIR in December 2010, summarizing serious lapses in management of GPO surplus property and offering recommendations to improve the sufficiency of and adherence to GPO Directives. An OI investigation in part found that GPO officials failed to comply with a requirement to report incidents of lost, stolen, or missing property to the Uniform Police Branch; GPO property was disposed of without proper documentation; and GPO Directives pertaining to property disposition either did not exist or needed revision.

In June 2011, management responded to the MIR and concurred with all recommendations. Management further indicated they intend to take the following actions to address OI's recommendations:

The OI recommended that management:

- Management directed the Managing Director of Plant Operations to develop written procedures and performance standards that hold Property Managers accountable for all improperly disposed property under their control.
- Management directed the Director of Quality Assurance to work with the Managing Director of Plant Operations to formalize in writing a donation and bidding process for disposing of surplus property items.
- Management directed the Director of Quality Assurance to work with the Managing Director of Plant Operations to revise and consolidate existing GPO Directives to address all outdated, inaccurate, and duplicated information.

APPENDICES

APPENDIX A

Glossary And Acronyms

Glossary

Allowable Cost–A cost necessary and reasonable for the proper and efficient administration of a program or activity.

Change in Management Decision–An approved change in the originally agreed-upon corrective action necessary to resolve an IG recommendation.

Disallowed Cost–A questionable cost arising from an IG audit or inspection that management decides should not be charged to the Government.

Disposition–An action that occurs from management's full implementation of the agreed-upon corrective action and identification of monetary benefits achieved (subject to IG review and approval).

Final Management Decision–A decision rendered by the GPO Resolution Official when the IG and the responsible GPO manager are unable to agree on resolving a recommendation.

Finding–Statement of problem identified during an audit or inspection typically having a condition, cause, and effect.

Follow-up–The process that ensures prompt and responsive action once resolution is reached on an IG recommendation.

Funds Put To Better Use–An IG recommendation that funds could be used more efficiently if management took actions to implement and complete the audit or inspection recommendation.

Management Decision–An agreement between the IG and management on the actions taken or to be taken to resolve a recommendation. The agreement may include an agreed-upon dollar amount affecting the recommendation and an estimated completion date, unless all corrective action is completed by the time agreement is reached.

Management Implication Report–A report to management issued during or at the completion of an investigation identifying systemic problems or advising management of significant issues that require immediate attention.

Material Weakness–A significant deficiency, or combination of significant deficiencies that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

Questioned Cost–A cost the IG questions because of an alleged violation of a law, regulation,

contract, cooperative agreement, or other document governing the expenditure of funds; such cost is not supported by adequate documentation; or the expenditure of funds for the intended purposes was determined by the IG to be unnecessary or unreasonable.

Recommendation–Actions needed to correct or eliminate recurrence of the cause of the finding identified by the IG to take advantage of an opportunity.

Resolution–An agreement reached between the IG and management on the corrective action or upon rendering a final management decision by the GPO Resolution Official.

Resolution Official–The GPO Resolution Official is the Deputy Public Printer.

Resolved Audit/Inspection–A report containing recommendations that have all been resolved without exception, but have not yet been implemented.

Unsupported Costs–Questioned costs not supported by adequate documentation.

Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
C&A	Certification and Accreditation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CPS	Certification Practices Statement
COA	Continuity of Access
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
DE	Delegated Examining
DHS/CPB	Department of Homeland Security/ Customs and Border Patrol
FDsys	Federal Digital System
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GPO	U.S. Government Printing Office
IG	Inspector General
IPA	Independent Public Accountant
IT	Information Technology
IT&S	Information Technology and Systems
IV&V	Independent Verification and Validation
OALC	Office of Administration/Legal Counsel
OAI	Office of Audits and Inspections
OGC	Office of General Counsel
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	Personally Identifiable Information
PO	Privacy Officer
RPPO	Regional Printing Procurement Office

APPENDIX B

Inspector General Act Reporting Requirements

INSPECTOR GENERAL (IG) ACT CITATION	REQUIREMENT DEFINITION	CROSS-REFERENCE PAGE NUMBER(S)
Section 4(a)(2)	Review of Legislation and Regulations	N/A
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	7–22
Section 5(a)(2)	Recommendations for Corrective Actions	20–22
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	22–28
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	31–32
Section 5(a)(5)	Summary of Refusals to Provide Information	N/A
Sections 5(a)(6) and 5(a)(7)	OIG Audit and Inspection Reports Issued (includes total dollar values of Questioned Costs, Unsupported Costs, and Recommendations that Funds Be Put To Better Use)	20–22
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	37
Section 5(a)(9)	Statistical table showing the total number of audit reports and the dollar value of recommendations that funds be put to better use	38
Section 5(a)(10)	Summary of prior Audit and Inspection Reports issued for which no management decision has been made	N/A
Section 5(a)(11)	Description and explanation of significant revised management decision	N/A
Section 5(a)(12)	Significant management decision with which the IG is in disagreement	N/A

APPENDIX C

Statistical Reports

Table C–1: Audit Reports With Questioned and Unsupported Costs

DESCRIPTION	QUESTIONED COSTS	UNSUPPORTED COSTS	TOTAL
Reports for which no management decision made by beginning of reporting period	$0	$0	$0
Reports issued during reporting period	$0	$0	$0
Subtotals	$0	$0	$0
Reports for which a management decision made during reporting period			
1. Dollar value of disallowed costs	$0	$0	$0
2. Dollar value of allowed costs	$0	$0	$0
Reports for which no management decision made by end of reporting period	$0	$0	$0
Reports for which no management decision made within 6 months of issuance	$0	$0	$0

Table C–2: Audit Reports With Recommendations That Funds Be Put to Better Use

DESCRIPTION	NUMBER OF REPORTS	FUNDS PUT TO BETTER USE
Reports for which no management decision made by beginning of reporting period	0	$0
Reports issued during the reporting period	0	$0
Reports for which a management decision made during reporting period		
• Dollar value of recommendations agreed to by management	0	$0
• Dollar value of recommendations not agreed to by management	0	$0
Reports for which no management decision made by the end of the reporting period	0	$0
Report for which no management decision made within 6 months of issuance	0	$0

Table C–3: List of Audit and Inspection Reports Issued During Reporting Period

REPORTS	FUNDS PUT TO BETTER USE
Report on Audit of GPO Oversight of the Federal Digital System Master Integrator Contract (Audit Report 11-07, issued August 19, 2011)	$0
Report on Assessment of GPO's Public Key Infrastructure Certification Authority – Attestation Report (Assessment Report 11-08, issued September 30, 2011)	$0
Total	$0

Table C–4: Investigations Case Summary

Total New Hotline/Other Allegations Received during Reporting Period	28
Preliminary Investigations (Complaints) Closed to the File	32
Complaint Referrals to Other Agencies	16
Complaint Referrals to OAI	0
Investigations Opened by OI during Reporting Period	10
Investigations Open at Beginning of Reporting Period	31
Investigations Closed during Reporting Period	20
Investigations Open at End of Reporting Period	21
Referrals to GPO Management (Complaints and Investigations)	29

Current Open Investigations by Allegation	21	
Procurement Fraud	13	62%
Employee Misconduct	3	14%
Workers' Compensation Fraud	4	19%
Proactive Initiatives	1	5%
Other Investigations	0	0%

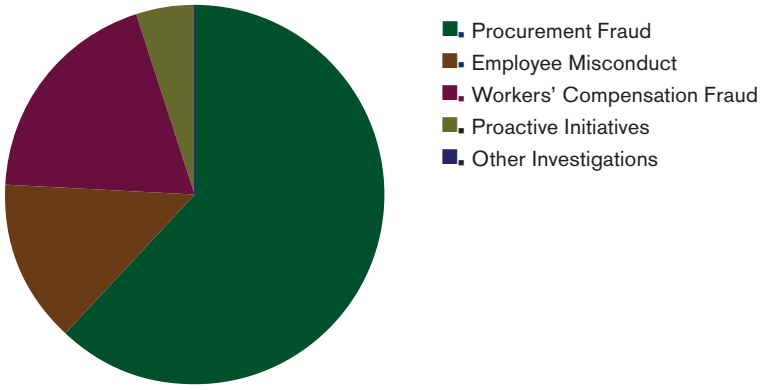


Table C–5: Investigations Productivity Summary

Arrests	0
Total Presentations to Prosecuting Authorities	8
Criminal Acceptances	1
Criminal Declinations	6
Indictments	0
Convictions	0
Guilty Pleas	0
Probation (months)	0
Jail Time (days)	0
Civil Restitutions	0
Civil Acceptances	1
Civil Agreements	0
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	0
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	
Contractor Debarments	2
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions	0
Proposed Employee Suspensions	3
Employee Terminations	0
Subpoenas	1

APPENDIX D–PEER REVIEW RESULTS

This appendix complies with Section 5(a)(14)-(16) of the IG Act of 1978, as amended.

A. PEER REVIEW OF THE AUDIT FUNCTION

Under generally accepted government auditing standards, OIG audit functions must have an external peer review at least every three years. The LOC OIG conducted a peer review of the GPO OIG audit function during this reporting period. On March 25, 2011, the LOC OIG issued its Peer Review Report of the GPO OIG audit function and found that the system of quality control for the audit function in effect for the two years ending September 30, 2010, was suitably designed and complied with, providing the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards. Federal audit organizations can receive a peer review rating of *pass, pass with deficiencies,* or *fail*. The GPO OIG received a peer review rating of pass. There are no outstanding recommendations from this peer review. The Peer Review Report is available on the GPO OIG Web site at http://www.gpo.gov/pdfs/ig/audits/GPO-AuditPeerReviewReport.pdf.

B. PEER REVIEW OF THE INVESTIGATION FUNCTION

Because it does not derive its statutory law enforcement power from Section 6(e) of the IG Act of 1978, as amended, the GPO OIG is not required to conduct an external peer review process of its investigative function. Nevertheless, the OIG voluntarily requests external peer reviews of its investigative function.

The National Science Foundation OIG conducted the peer review of the GPO OIG investigative function during this reporting period. On March 11, 2011, the National Science Foundation OIG issued its opinion and found that the system of internal safeguards and management procedures for the investigative function for the year ended 2010 complies with the quality standards established by the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency, the CIGIE, and the Attorney General guidelines. These safeguards and procedures provide reasonable assurance of conforming with professional standards in the conduct of its investigations. There are no outstanding recommendations from this peer review. The Peer Review Report is available on the GPO OIG Web site at http://www.gpo.gov/pdfs/ig/investigations/InvestigationsPeerReview.pdf.

C. PEER REVIEWS OF OTHER OIGS

The GPO OIG conducted a peer review of Peace Corps OIG's audit organization during this reporting period.

We conducted the peer review for the audit organization of the Peace Corps in effect for the year ended September 30, 2010 in accordance with generally accepted government auditing standards and guidelines established by the CIGIE. In our opinion, the system of quality control for the audit organization of the Peace Corps OIG was suitably designed and complied with to provide the Peace Corps OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Therefore, we issued a peer review report with a rating of "pass." As is customary, we also issued a letter that sets forth findings that were not considered to be of sufficient significance to affect our opinion expressed in our report.

U. S. GOVERNMENT PRINTING OFFICE ■ OFFICE OF INSPECTOR GENERAL

732 NORTH CAPITOL STREET, N.W. WASHINGTON, DC 20401

202-512-0039 ■ WWW.GPO.GOV/OIG ■ OIG HOTLINE 1-800-743-7574
GPOOIGHOTLINE@GPO.GOV