



U. S. GOVERNMENT PRINTING OFFICE • OFFICE OF INSPECTOR GENERAL
SEMIANNUAL REPORT TO CONGRESS

April 1, 2010, through September 30, 2010

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 more than half of all 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 will 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.



CONTENTS

MESSAGE FROM THE INSPECTOR GENERAL	3
HIGHLIGHTS OF THIS SEMIANNUAL REPORT	5
OIG MANAGEMENT INITIATIVES	6
PERSONNEL UPDATES	7
COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY	8
REVIEW OF LEGISLATION AND REGULATIONS	8
 GPO MANAGEMENT CHALLENGES	 9
 OFFICE OF AUDITS AND INSPECTIONS	 21
A. Summary of Audit and Inspection Activity	21
B. Financial Statement Audit	21
C. Audit and Inspection Reports	22
D. Ongoing Work	24
E. Status of Open Recommendations	24
 OFFICE OF INVESTIGATIONS	 31
A. Summary of Investigative Activity	31
B. Types of Cases	32
C. Summary of Investigative Accomplishments	32
D. Other Significant Activities	36
 APPENDICES	 37
A. Glossary and Acronyms	37
B. Inspector General Act Reporting Requirements	40
C. Statistical Reports	41
Table C-1: Audit Reports with Questioned and Unsupported Costs	41
Table C-2: Audit Reports with Recommendations That Funds Be Put to Better Use	42
Table C-3: List of Audit and Inspection Reports Issued During Reporting Period	43
Table C-4: Investigations Case Summary	44
Table C-5: Investigations Productivity Summary	46
D. Peer Review Results	47



MESSAGE FROM THE INSPECTOR GENERAL

This Semiannual Report to Congress covers the activities of the GPO Office of Inspector General for the period April 1, 2010 through September 30, 2010.

During this reporting period, our Office of Audits and Inspections continued its oversight activities of the implementation of the Federal Digital System (FDsys), as well as the Public Key Infrastructure, which supports critical, digital agency functions. The OAI notes 48 open recommendations from previous reporting periods requiring management's attention.

The Office of Investigations continues to see growth in the area of contract and procurement fraud, as well as employee misconduct cases. Currently, the OI has 50 active complaints and investigations in progress, a significant increase over the last reporting period. In order to meet the increasing demands from the burgeoning case load, the OI will welcome two new special agents at the beginning of FY 11.

We continue to evaluate critical issues facing GPO, and have updated the most significant management challenges, accordingly. Human capital operations and management continues as a critical challenge to the Agency. We remain hopeful that a renewed focus on customer-driven solutions and results will bring about much needed change and direction. Additionally, we note critical developments with Security and Intelligent Documents that will warrant additional oversight efforts by this office.

As the GPO OIG remains committed to quality and accountability, we continue our own process improvement efforts. As we move into the next fiscal year, the OIG will undergo peer reviews of our Audit and Investigative functions, as well as an internal review of OIG operations and procedures. Being mindful of improving our own operations will only enable the OIG to better fulfill its mission and goals.

For more information, please visit our website (www.gpo.gov/oig) and, to keep informed of OIG activities, please sign up to receive automatic email updates.

A handwritten signature in black ink, reading "J. Anthony Ogden". The signature is written in a cursive, flowing style.

J. Anthony Ogden
Inspector General
U.S. Government Printing Office





HIGHLIGHTS OF THIS SEMIANNUAL REPORT

*T*he Office of Audits and Inspections (OAI) issued three new reports during this reporting period. Those three reports included assessments related to the Independent Verification and Validation (IV&V) efforts of implementing the Federal Digital System (FDsys). We also issued an annual report assessing GPO's Public Key Infrastructure (PKI) services.

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

- Continued to oversee the efforts of American Systems as it conducted IV&V for the public release of FDsys. We issued two quarterly reports this period providing observations and concerns on the program's technical, schedule, and cost risks as well as requirements traceability of those risks and the effectiveness of the program management processes in controlling risk avoidance.
- 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 8 investigations and 24 complaints for preliminary investigation, while closing 8 investigations and 29 complaints (10 of which were closed with no action). At the end of this reporting period, OI had 33 ongoing investigations and 17 open complaints. Additionally, three investigations and nine complaints were referred to GPO management for potential administrative action.

Of the open complaints and investigations, 27 involve allegations of procurement fraud, which reflects increased OI efforts to address procurement and financial fraud vulnerability within GPO. The increase in procurement fraud cases is the result in part

of continued OI engagement with management, Print Procurement officials, and other acquisitions employees.

Several ongoing investigations are being conducted in coordination with the Department of Justice (DOJ), including its Antitrust Division. As part of those investigations, the IG issued four subpoenas for documents this reporting period.

OI's significant accomplishments during this reporting period include:

- As a result of an OI investigation substantiating that a contractor failed to comply with critical contract specifications regarding the security of personally identifiable information (PII), the contractor agreed to pay a \$25,000 settlement of U.S. penalty claims, without admitting wrongdoing or liability.
- The Agency terminated an employee as a result of an OI investigation into allegations the employee used or attempted to use her position for personal financial gain and benefit close friends.
- The Agency terminated another employee after OI determined that employee was convicted of a serious drug offense and initiated an investigation to determine if the employee was selling drugs on GPO property. The seriousness of the drug offense coupled with false statements the employee made to investigators formed the foundation of the successful administrative case against the employee.

OI continues investigations into allegations of false statements, false claims, and/or bid collusion by GPO print vendors. OI also has the assistance of the DOJ Antitrust Division, which continues to evaluate cases for possible criminal and/or civil action.

The Office of Administration/Legal Counsel (OALC) provides legal advice and counsel on issues arising during audits, inspections, and investigations, including opinions regarding legal accuracy and sufficiency of OIG reports. OALC manages administrative and management issues as well as congressional and media relations and requests for information. OALC reviews and edits audit, inspection, and investigative reports before the IG approves.

During this reporting period, OALC accomplished the following:

- Reviewed, edited, and approved four subpoenas; reviewed and edited three audit reports and five reports of investigation.
- Worked with the IG to develop agenda for OIG-wide retreat.
- Updated the OIG 3-year Strategic Plan for discussion with senior staff.
- Supported the IG in his role as the Chair of the Legislation Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE) in reviewing and analyzing proposed legislation affecting the IG community, soliciting comments, and drafting letters and informal comments for Members of Congress.
- Hired a law clerk for the summer who worked on a variety of legal research projects.
- Supported the procurement of an electronic case management system for OI.
- Organized a presentation on Whistleblower Protection Issues for members of the Council of Counsels to the Inspector General (CCIG).
- Acted on a variety of matters as the OIG liaison to the GPO General Counsel and the GPO Office of the Chief of Staff, including support with GPO litigation and personnel action matters.

OIG MANAGEMENT INITIATIVES

During this reporting period, the OIG held an office-wide retreat in June 2010 to discuss the vision, direction, and goals of the OIG as well as how to continue to enhance, improve, and measure the success of its operations. We have also drafted an updated, 3-year strategic plan. We continued to meet with various business units during the reporting period to determine high-risk areas for the Agency to better focus our resources.

During the upcoming reporting period we will work on refreshing our Web site and developing a formal communications plan with the Agency's Office of Communications to help educate GPO employees and other stakeholders about the role of the OIG,

employee rights, and the importance of reporting wrongdoing and cooperating with the OIG.

PERSONNEL UPDATE

During this reporting period, Patricia Bach and David Hilburg joined OAI as Senior Auditors. Patricia brings 25 years of audit and accounting experience to the OIG from the Department of Energy where she was a Senior Accountant. Patricia previously held auditor positions with the Department of Defense and the General Services Administration. She has a Bachelor of Science degree from the University of West Florida and is a Certified Public Accountant. David brings more than 6 years of audit experience from the U.S. Air Force Audit Agency where he was an Audit Manager. David has a bachelor's degree from Washington University and a Master of Science degree from the Colorado School of Mines.

On September 30, 2010, Debra Miller, the Assistant Inspector General for Investigations (AIGI), retired from federal government service. Debbie began her investigator career in 1977 with the Florida Auditor General's Office investigating welfare fraud. In 1982, she became a Special Agent with the Environmental Protection Agency's OIG where she worked in civil and criminal investigations. In that same year, Congress charged that the EPA had mishandled the \$1.6 billion toxic waste Superfund and demanded records from then EPA Administrator Anne Gorsuch. Gorsuch refused and became the first agency director in U.S. history to be cited for contempt of Congress. As a result of this scandal, Debbie was involved in highly sensitive investigations of alleged misconduct by an Assistant Administrator and a Regional Administrator, which led to their resignations and financial recoveries for the EPA.

After a brief stint as a Financial Investigator for Blue Cross and Blue Shield of Virginia, she moved to NASA's OIG where she worked until 1998 on sensitive and complex criminal and civil investigations. One significant achievement at NASA was her work as the lead agent on the investigation of the Hubble Space Telescope primary mirror flaw. That investigation resulted in a civil settlement of \$25 million



David Hilburg joined the OIG as Senior Auditor. Debra Miller, Assistant Inspector General for Investigations, retired after 27 years of federal service.

with the mirror manufacturer, at the time the largest recovery by the NASA OIG.

In 1998, Debbie joined the Social Security Administration (SSA) OIG as a Regional Special Agent in Charge where she oversaw the administrative, operational, and management activities of three investigative field divisions. In 2003, Debbie became SSA OIG's Contract Fraud Program Manager to initiate and develop a contract fraud investigative program. In that capacity, she was the lead agent in a successful case prosecution against a former owner of a Maryland security firm, its former Chief Operating Officer, and a long-time General Service Administration employee. These individuals pled guilty in a bribery and tax evasion scheme involving federal security contracts worth more than \$130 million. The company provided armed and unarmed security guards for 18 Federal agencies at 120 installations in 32 States and territories. The case is the largest corruption case ever prosecuted in Maryland, in terms of the size of the contracts involved.

As the AIGI at GPO OIG, Debbie was critical in transforming the Office of Investigations. She started with a staff of three Special Agents and a caseload of

seven contract and procurement fraud cases. In two years, she grew the office to seven Special Agents, increased procurement fraud investigations more than 200%, and issued a variety of reports to GPO management to prevent procurement fraud and increase protection of sensitive information. She also developed fraud briefings for GPO staff and was successful in obtaining U.S. Marshal Services' Special Deputations for the OI's Special Agents.

Through it all, Debbie was able to successfully raise three beautiful children. She also worked tirelessly as a member of the Women in Federal Law Enforcement Association to promote work/life balance in the workplace. We wish Debbie the best in her next adventures.

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

On October 14, 2008, the IG Reform Act of 2008, Public Law 110-409, established the CIGIE. The CIGIE addresses integrity, economy, and effectiveness issues that transcend individual Government agencies and helps increase professionalism and the effectiveness of personnel by developing policies, standards, and approaches aiding in establishing a well-trained and highly skilled workforce in OIGs. The GPO OIG—along with other legislative branch OIGs—is a member of CIGIE.

The role of the CIGIE includes identifying, reviewing, and discussing areas of weakness and vulnerability in Federal programs and operations for fraud, waste, and abuse, and developing plans for coordinated Government-wide activities that address those problems and promote economy and efficiency in Federal programs and operations.

In May 2009, the IG at GPO was elected to serve a 2-year term as Chairman of the CIGIE Legislation Committee. The Legislation Committee provides to the IG community helpful and timely information about congressional initiatives. The Committee also solicits the IG community's views and concerns in response to congressional initiatives and requests, and presents views and recommendations to congressional entities and the Office of Management and Budget (OMB).

On behalf of the CIGIE Legislation Committee, the IG wrote letters and communicated with several congressional committees on various legislative matters affecting the IG community, most significantly to:

- Convey the views of the IG community on House of Representatives Bill 4983 (HR 4983), "Transparency in Government Act of 2010," which would place certain requirements on the IG community to review data for Federal agency awards.
- Convey the sense of the IG community regarding a requirement under Senate Bill 372 (S 372), "The Whistleblower Protection Enhancement Act of 2009," that IGs designate a Whistleblower Protection Ombudsman within their offices.

In addition to participating in CIGIE meetings and events, legislative branch IGs meet regularly to promote communication, cooperation, and coordination with one another on an informal basis. During this reporting period, the IGs of the Government Accountability Office (GAO) and Library of Congress hosted meetings in which the following issues were discussed and are undergoing consideration:

- Shared training opportunities for legislative branch OIG personnel.
- Cross-cutting legislative branch audits and inspections.
- Model performance criteria and standards.
- Ongoing discussions regarding legislative issues affecting the legislative branch OIG offices.

REVIEW OF LEGISLATION AND REGULATIONS

The OIG, in fulfilling its obligations under the IG Act, reviews existing and proposed legislation and regulations relating to programs and operations at GPO. It then reports in each semiannual report on the impact of legislation or regulations on the economy and efficiency of programs and operations administered or financed by GPO. The OIG will continue to assist the Agency in achieving its goals in that area.

During this reporting period, there were no legislative proposals relating to GPO programs and operations.



GPO MANAGEMENT CHALLENGES

In each Semiannual Report to Congress, the OIG identifies for management a list of issues most likely to hamper the Agency’s efforts if not addressed with elevated levels of attention and resources. In this report, we update the list of management challenges we believe are critical for the Agency to address.

1. Human Capital Operations and Management. The issues facing Human Capital (HC) operations and management at GPO were identified as a significant management challenge for several semiannual reporting periods. HC operations are at the heart of effectively accomplishing an agency’s mission. In essence, HC provides services necessary to acquire the most precious and important source of productivity—its employees.

In writing about the challenges of human capital in general, J. Christopher Mihm recently notes that “[d]riven by long-term fiscal constraints, changing demographics, evolving governance models, and other factors, the federal government is facing new and more complex challenges in the twenty-first century and federal agencies

GPO’S TOP 10 MANAGEMENT CHALLENGES

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

must transform their organizations to meet these challenges. **Strategic human capital management must be the centerpiece of any serious change in management strategy.**¹ In today's environment, successful HC operations are "results-oriented, customer-focused, and collaborative."²

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.³

We continue to be concerned that management has not placed enough emphasis on addressing the four areas that GAO cites to transform HC operations and management. During this reporting period, 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."

*In today's environment,
successful HC operations
are "results-oriented, customer-
focused, and collaborative."*

Among the significant findings of the OPM audit were that GPO (1) does not have a fully functioning accountability system that ensures efficient and compliant DE operations; (2) has significant problems in transaction processing, particularly regarding the critical on-boarding process that establishes new hires; (3) lacks consistent updated guidance addressing DE processes; (4) has used HC Specialists in DE work before completing certification training, which is prohibited by the Interagency DE Agreement with OPM; and (5) is not using annual trend data regarding opportunities to hire veterans, or the results of annual self-audits to improve program operations.

GPO HC management acknowledged problems with its transaction processing, particularly the on-boarding processes, with the OIG experiencing an 80-percent error rate. OPM recommended that GPO consider an outsourcing pilot of human resources services for the OIG, noting that as an independent organization, the GPO OIG is an ideal candidate because many other OIGs have outsourced their human resources services. With such a pilot, GPO could track efficiency, effectiveness, and cost of the outsourcing option to compare with its own HC operations. In response to the OPM recommendation and with the support of the Public Printer and Chief Management

Officer, the OIG proposed an Interagency Agreement with OPM for such services during fiscal year (FY) 2011.

In its response to OPM's audit, GPO HC management admits "the need for improvement in certain key areas regarding planning, documenting, and accountability" and indicates either planned or initiated actions for addressing required and recommended actions. We encourage management to undertake and complete any action necessary to address OPM's recommendations as quickly as possible. 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.

¹ "Human Capital: Federal workforce challenges in the Twenty-first Century," in Hannah S. Sistare, Myra Howze Shiple and Terry F. Buss, eds., *Innovations in Human Resource Management: Getting the Public's Work Done in the 21st Century* (New York: M.E. Sharpe, Inc., 2009), 13.

² *Id.*, 19.

³ GAO Report GAO-09-632T, <http://www.gao.gov/new.items/d09632t.pdf>.

We also believe that the Agency faces challenges in acquiring, developing, and retaining a diverse, qualified workforce with the right sets of skills for meeting both the Agency's needs today and in the future. In September 2008, we completed a congressionally requested audit of GPO's diversity programs, particularly those related to establishing a more diverse population in senior leadership positions. The audit revealed that while GPO voluntarily adopted several components for establishing a model Federal Government diversity program, improvements could be made toward enhancing diversity of the Agency's corps of senior-level employees. We recommended that the Public Printer adopt all or a combination of the leading practices that GAO recommends for establishing a model Federal Government program. During this reporting period, we closed those recommendations.

2. Information Technology Management and Security.

As GPO transforms to a highly efficient and secure multimedia digital environment, management of the Agency's information technology (IT) resources is critical. Acquisition, implementation, and sustainment of engineering issues associated with IT resources and the Information Technology and Systems (IT&S) Business Unit (including security issues) pose new management challenges.

Noteworthy challenges for IT&S include establishing and maintaining a top-level Enterprise Architecture as well as support for several significant initiatives, including FDsys, the e-Passport system, digital publication authentication using a PKI, information system management, implementation of the GPO Business Information System (GBIS) (an Oracle solution), and implementation of electronic human resources systems.

Legacy systems increasingly inhibit the Agency's ability to respond to customer needs and must be replaced. To create a plan that will help mitigate risks for aging legacy systems, IT&S analyzed legacy applications and their impact on business operations. As a result, IT&S recently completed a 5-year strategy for improving the level of system support and has begun executing the plan. The strategy they developed should guide the Agency



through implementation of new systems and retirement of the older legacy systems. FDsys, human resource systems, and GBIS releases are now operational. Additionally, in FY 2009, IT&S completed an Agency-wide rollout of an enhanced Time and Attendance application (WebTA).

The following areas are significant IT issues confronting the Agency:

a. Compliance with the Federal Information Security Management Act

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. Complying with FISMA presents additional challenges for IT&S, 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, IT&S continued to progress in addressing recommendations made in our 2009 assessment.

Looking forward, the potential changes to FISMA resulting from draft legislation before

Congress present IT&S with areas to monitor and incorporate into GPO's FISMA planning process.

b. Implementation of the Federal Digital System

The FDsys will 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. As of September 30, 2010, GPO expended approximately \$41 million (unaudited) to deploy FDsys Release 1, substantially exceeding the original planned cost of \$16 million.

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 IV&V work associated with developing and implementing FDsys. Under the supervision and direction of the OIG, American Systems conducts programmatic and technical evaluations of the FDsys program to determine whether system implementation is consistent with the FDsys project plan and cost plan and meets GPO requirements. Additionally, IV&V monitors development and program management practices and processes to anticipate potential issues. Specific IV&V tasks include:

Program Management – IV&V includes activities regarding the cost, schedule, and risk associated with development and implementation to evaluate overall program management effectiveness.

Technical – IV&V includes activities regarding the resources, system requirements, architecture and design documents, and other critical deliverables associated with FDsys development and implementation.

Testing – IV&V includes activities regarding the Master Test Plan and test efforts performed by the FDsys implementation team and the IT&S System Test Branch to verify adequacy and completeness of testing activities.

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.

During this reporting period, the PMO completed deployment of 6 post-Release 1 production builds. The builds nearly complete migration of data from the existing GPO Access system to FDsys, and implement resolutions of 281 software Program Tracking Reports (PTRs). The Continuity of Operations (COOP) capability, a critical step in the transition from GPO Access to FDsys as the "system of record," has not yet been implemented. However,

*As of September 30, 2010,
GPO expended approximately
\$41 million (unaudited) to deploy
FDsys Release 1, substantially
exceeding the original planned
cost of \$16 million.*



PMO documentation reflects substantial progress in terms of the design, development, and testing for both the Continuity of Access (COA) (to support the public users) and the full COOP.

Although the FDsys program continues to progress, a number of issues remain. Based on the information contained in the FDsys Release 1 Completion Plan dated October 1, 2010, the PMO completed the Final Sunset Release and deployed this Release to the Production System as scheduled on September 30, 2010. However, this does not mean that the PMO met their goal of sun-setting GPO Access and implementing FDsys as GPO's official system of record. The FDsys Release 1 Completion Plan has been modified twice since then. The latest version of the Plan indicates that the non-developmental activities that are required to sunset GPO Access were eighty-two percent complete with transition from GPO Access to FDsys planned for December 23, 2010. GPO continues to operate and maintain two systems. FDsys is still a beta system, and GPO Access continues as the official system of record.

A continuing concern for the FDsys program is the quality of the deployed system. While the testing effort is better and more rigorous, the test team is still identifying software problems before major production builds are deployed. These problems, documented as PTRs, describe errors/deficiencies in system operation and/or failures

to meet expected performance. As of September 30, 2010, nearly 600 PTRs created since the initial beta deployment of Release 1 (in March 2009) remain open and unresolved. The on-going need to address these PTRs consumes program resources and reduces PMO ability to develop and deploy new functionality.

This brief assessment does not mean to imply that the FDsys program lacks effort or has failed to produce a viable product. The FDsys Release 1 beta system 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.

The OIG continues to believe that the primary challenges for the FDsys program are in the areas of program management, system engineering leadership and 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 any risks.

3. Security and Intelligent Documents. As the Federal Government's leading provider of secure credentials and identity documents, GPO management regards Security and Intelligent Documents (SID) as a business unit best exemplifying the Agency's transformation toward high-technology production. Because of SID's growing strategic importance for the Agency's transformation efforts and its sensitive work in areas of national security, the OIG closely monitors management's efforts in developing formal, internal security controls of these products, and will continue to emphasize oversight of all SID operations and programs.

During this reporting period, SID manufactured more than 7.7 million electronic passports (e-Passport) for the Department of State. The Washington, D.C., facility produced more than 5.4 million passports, while the Secure Production Facility (SPF) located as a COOP site in Stennis, Mississippi, produced more than 2.3 million. During FY 2010, the total passport production volume for the Department of State was 13,275,300 passports.

SID continues to operate the Washington, D.C.-based Secure Credential Center (SCC), which supports the Department of Homeland Security's Customs and Border Protection (DHS/CBP) Trusted Traveler Programs (TTP).⁴ SID reports that the SCC produced 199,477 Trusted Traveler cards during FY 2010. During this reporting period, SCC also produced, personalized, and distributed for the Department of Health and Human Services Center for Medicare and Medicaid Service's (CMS) Medicare identification cards to citizens of Puerto Rico. Rather than producing blank e-Passports, which do not entail the "personalization" of the credential with a citizen's personal information, the TTP and CMS programs entail the use of PII by GPO to produce identity cards.

⁴ TTPs provide expedited travel for preapproved, low-risk travelers through dedicated lanes and kiosks by providing those travelers secure identification cards.

*GPO management regards
Security and Intelligent
Documents (SID) as a business unit
best exemplifying the Agency's
transformation toward
high-technology production.*

The OIG is in the process of finalizing an audit of GPO's secure personalization system (SECAPS) IT security controls. SECAPS is the baseline for personalization operations that supports various GPO customer identity card programs, including TTP and CMS. Because SECAPS handles PII, the OIG placed particular audit emphasis on security controls over PII. The audit included a security evaluation of SECAPS physical controls, system interconnections and transmission of PII, operating systems and database systems supporting SECAPS, and purging PII. The OIG expects to issue the report in November 2010.

In 2005, the OIG recommended that GPO adopt International Organization for Standardization (ISO) 9000 standards for passport production.⁵ Standards help promote best practices for management systems and occupational health and safety in a production environment. In July 2010, the SPF at Stennis and SID personnel successfully completed required audits, making the facility ISO 9001-certified. This globally recognized certification is a significant accomplishment. According to SID, the Washington, D.C., secure

facilities and SID personnel are also on schedule to be ISO 9001-certified in November 2010. SID is also working to complete a library of standard operating procedures that will lay the foundation for future Occupational Health and Safety Assessment Series (OHSAS) 18001 certification.⁶

⁵ The International Organization for Standardization, or ISO, is the world's largest developer and publisher of international standards. ISO 9000 family of standards represents an international consensus on good quality management practices. It consists of standards and guidelines relating to quality management systems and related supporting standards.

⁶ OHSAS 18001 is an Occupation Health and Safety Assessment Series for health and safety management systems. It is intended to help an organization control occupational health and safety risks. It was developed in response to widespread demand for a recognized standard against which to be certified and assessed.



SID also reports continuation of 5S audits at both plant locations. 5S is a methodology intended to improve efficiencies in manufacturing process flows, equipment use and placement, and environmental housekeeping standards. SID also continues its work to complete the certification process for SCC to become a GSA-qualified secure card graphical personalization facility. Such a certification will allow SCC to handle, personalize, and distribute Homeland Security Presidential Directive 12 (HSPD-12) cards. The audits for certification were completed as planned in May 2010, and GSA should complete its assessment in November 2010. This certification will allow the SCC to more comprehensively serve Federal Government organizations in the area of secure credentials.

SID is developing a capability to manufacture secure blank card bodies through the procurement of card lamination and punch equipment and technologies that will result in more secure and controlled card production as well as lower costs and better service to GPO's agency customers. In September 2010, SID took delivery of card lamination and punch equipment as well as the process of installation and development of standard operating procedures. Operator training is underway. SID should be able to manufacture secure blank card bodies during FY 2011.

SID is also establishing a Secure Credential Testing Laboratory that will conduct regular performance, durability, and quality tests of passports and credential products. The Secure Credential Testing Laboratory is expected to be operational

in FY 2011. Eliminating costly third party commercial test laboratory expenses for required product evaluations, the laboratory will also provide an environment of greater governmental control and security. The secure facilities are under construction, equipment has been ordered, and personnel are being trained to support this crucial secure product-testing environment.

In cooperation with the Department of State's Bureau of Consular Affairs, the Agency issued a Request for Proposal in June 2010 for procurement of e-Covers used in manufacturing U.S. Passports. The proposed e-Covers will be compatible with existing GPO manufacturing and Department of State passport personalization processes, and must meet various external applicable requirements and standards, including those of the International Civil Aviation Organization (ICAO) and ISOs.

4. Internal Controls. 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.

Our audits continue to identify issues related to internal controls. For example, the OIG issued an audit report during the last reporting period that discusses internal controls associated with the security of GPO's e-Passport supply chain. As part of that audit, we determined whether GPO had formal documented policies, procedures, techniques, or mechanisms in place to implement a security process for its e-Passport supply chain and whether an organizational structure was in place that clearly defines key areas of authority, responsibility, and appropriate lines of reporting for e-Passport supply chain security. The audit revealed that a control deficiency existed because GPO did not have a formal, Agency-wide process for ensuring security for the e-Passport supply chain, as basic Federal Government internal control standards require.

The annual financial statement audit also addresses internal control issues and provides management with recommendations for corrective actions. 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.” During the FY 2009 financial statement audit, KPMG, LLP, (KPMG) identified two significant internal control deficiencies it did not consider material weaknesses. The significant deficiencies KPMG identified were related to (1) financial reporting controls, and (2) IT general and application controls. The deficiencies will be followed up on during the FY 2010 financial statement audit, which is ongoing. An evaluation of internal controls continues an area of emphasis for all OIG audits.

Internal control “also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud.”

5. Protection of Sensitive Information. GPO has had 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 PII, including PII in both information systems and paper documents. In accordance with OMB Memorandum 06-15 and OMB Memorandum 07-16, executive branch agencies must implement policies and procedures that protect and respond to a breach of PII as far back as the middle of 2007.

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) during the last reporting period. The primary duty for the PO is to implement Directive 825.41. The PO will also review PII in each of the Agency’s business units, reduce PII to the minimum necessary, develop a schedule for periodic review of PII, establish a plan to eliminate the unnecessary collection and use of social security numbers, and establish an incident response plan to handle breaches of PII. The OIG is monitoring implementation of GPO Directive 825.41 to ensure that safeguards are in place, implemented, and followed.

During this reporting period, GPO hired a new privacy program manager (PPM) to help the PO implement GPO Directive 825.41. The PPM has met with various GPO Business Units, identified what PII is at GPO, where it is located, and how it is safeguarded. The PPM established a Privacy Incident Response Team and incident handling timeline so that GPO can respond appropriately to any privacy related incident. In addition, each Business Unit has designated a Privacy Point of Contact who will work closely with the PPM to ensure that any existing or new projects adhere to GPO’s privacy protection policies. The PPM is working with GPO University to develop a training curriculum for all GPO employees and contractors on their responsibilities for protecting PII and complying with established guidelines.

Finally, the Agency issued new, updated forms for Agency customers—the SF-1 Binding and

Requisition Form and the GPO 4044 (Simplified Purchase Agreement Work Order)—that will now require that customers indicate whether documents are classified, sensitive but unclassified (SBU), or contain PII. The forms were revised, in part, in response to the OIG’s recommendations to improve GPO processes concerning handling classified and sensitive but unclassified materials, in addition to other instances regarding the handling of PII. We applaud the agency for moving forward with these efforts to address PII protection at GPO.

6. Acquisitions and Print Procurement. As with other Federal agencies, GPO faces challenges in its acquisition functions. Acquiring goods and services, especially those necessary to transform the Agency and provide services to its Federal customers in an efficient, effective, accountable, and environmentally conscious manner, is essential. With more than \$650 million in acquisitions during FY 2009, we remain concerned that the Agency has not devoted the resources necessary for conducting an independent assessment of acquisition services that will identify gaps in effective performance and implement a plan for resolving critical issues, as the Services Acquisition Reform Act of 2003 and OMB guidelines require.

During 2009, OMB provided guidelines to executive branch agencies requiring that they conduct internal reviews of the acquisition function required under OMB Circular No. A-123. OMB used the GAO “Framework for Assessing the Acquisition Function at Federal Agencies” as the standard assessment approach.⁷ Although GPO is not required to follow OMB guidelines in that area, we believe that the Agency would greatly benefit from a review of its Acquisition Services. Although the Public Printer announced in his June 7, 2010, letter to Congress that such an independent assessment would be completed by the end of this reporting period, the OIG has not yet received the assessment report.

We are also concerned about other specific issues regarding Agency contract administration, as evidenced in part by our recent audit of the



security of the e-Passport supply chain and other ongoing audits. As our audit of the e-Passport supply chain revealed, of the 10 significant e-Passport supplier contracts reviewed, 5 lacked critical information that the Agency’s Materials Management Acquisition Regulation (MMAR) requires. Such contract file information is critical to the OIG so we can review and investigate Agency contracting actions and administration. Acquisition Services should comply with the MMAR by properly documenting contract files.

Additionally, we identified that a significant number of e-Passport supplier contracts did not contain security-related requirements or language that would have given the Agency the right to review, authorize the subcontracting of, and inspect the operations of companies that provide critical components for the e-Passport. Acquisition Services should work with the Office of General Counsel and SID to ensure that all contracts related to e-Passports, and other sensitive identity products, include the appropriate language about proper security plans and oversight rights.

Finally, we note that the Improper Payments Elimination Improvement Act was signed into law

⁷ GAO Report GAO-05-218G, September 2005, <http://www.gao.gov/new.items/d05218g.pdf>.

on July 22, 2010. That 2010 Act amends the Improper Payments Information Act of 2002 by requiring that executive branch agencies periodically identify and review programs and activities susceptible to significant improper payments and report on any actions to reduce or recover improper payments in accordance with guidance OMB plans to issue. Although GPO is not covered by law, we urge management to undertake this type of review so that it can develop actions that will reduce or recover any improper payments. We expect to review efforts by the Agency in this area in the future.

7. 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 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. The new 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 2009 financial statements, stating that the Agency's financial statements were fairly presented, in all material respects, and in conformity with generally accepted accounting principles. Although GPO addressed previous material weaknesses, KPMG identified two significant deficiencies it did not consider material weaknesses, including (1)

financial reporting controls, and (2) IT general and application controls.⁸

With respect to financial reporting controls, KPMG identified specific deficiencies concerning review and reporting of general property, plant, and equipment; certain reconciliation controls; and controls over compilation of statement of cash flows. Deficiencies with the design and/or operations of GPO's IT general and application controls were noted in security management, access controls, 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 2010 financial audit, which is in progress.

8. Continuity of Operations. GPO's ability to continue its mission essential functions of congressional printing and publishing, production of the *Federal Register*, and production of blank passport books for the Department of State during a disruption in operations continues to be a significant area of concern. A power loss incident in 2009, which directly affected production of the *Congressional Record*, brought the COOP issue to the forefront and underscored the critical nature of the Agency's ability to continue essential functions during a disruption of operations. A public-facing server outage in 2009 also raised issues concerning the capability of GPO to maintain communications with external stakeholders and employees during a COOP event to include Web-based content as well as e-mail.

The Agency continues with the necessary steps for enhancing its COOP posture, including planning and conducting exercises with scenarios that test alternate production facilities and procedures for

⁸ A significant deficiency is defined as a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

notifying essential personnel. Accomplishments during the last reporting period included an Executive Offices COOP exercise in February 2010. The exercise was the first involving executive leadership and some support units, and included relocating to a non-GPO facility for strategy and decision-making. The primary goal of the exercise was to familiarize the appropriate personnel with the procedures and situation of working out of a non-GPO building to manage the first phase of a COOP event. Although all of the goals were demonstrated, there were areas needing improvement and recommendations made for further improving the Agency's COOP posture. These areas will be further tested as part of the Agency's COOP plans for FY 2011.

9. Strategic Vision and 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 Strategic Vision. 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 state-of-the-art customer relations management.

In line with its Strategic Vision, GPO previously reorganized several business units to better serve its Government customers. Such a realignment of business units was initiated to help streamline processes, strengthen customer relationships, and develop new sales opportunities. GPO should continue its efforts to enhance business development and customer service and measure their level of success to ensure a culture of continuous improvement.

Nevertheless, after almost 6 years, the Agency's Strategic Vision, which was issued on December 4, 2004, and included a Business Plan from FY 2005 through 2009, is itself in need of review and updating. The Agency should review its transformational efforts thus far to measure its accomplishments, its shortcomings, and its renewed vision for the future. Senior management developed a draft update to the Agency's Strategic Vision in May 2010 that included nine strategic goals, which included

creating a culture of customer service, support of the Administration's initiative on transparency, and a collaborative approach to fiscal responsibility. As of the end of this reporting period, management has not provided the OIG with an update to the Agency's Strategic Vision.

10. Sustainable Environmental Stewardship. As the largest industrial manufacturer in the District of Columbia, GPO has always faced challenges to become more environmentally sensitive. The Public Printer has made central to his administration "the call to sustainable environmental stewardship" and to attempt to be green in virtually every step of the printing process. Previously, the Public Printer outlined a plan that would help GPO become more efficient and make better use of resources under its control. More recently, the Public Printer noted that a future based on environmental sustainability is more than simply going green, but rather "it means expanding our digital operations and making changes in paper, inks, equipment configurations, and energy sources so that we can support our customers in Congress, Federal agencies, and



the public in a more efficient and environmentally responsible way.”

We reported in our previous semiannual report that GPO was printing the *Congressional Record* on paper comprised of 100-percent post-consumer waste. GPO is also printing the *Federal Register* on 100-percent post-consumer waste paper. And progress continues on other initiatives, including moving from Web offset presses to digital equipment, developing a chemical inventory management system, and reducing landfill waste.

We continue to encourage management and Congress to renew their 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 encourage management to promote and incorporate green thinking into all business processes through performance metrics, reward programs, and other means. For example, the OIG urges an integrated approach to green acquisition. In October 2009, the President issued Executive Order 13514, which sets sustainability goals for Federal agencies and focuses on making improvements in their environmental, energy, and economic performance. In particular, the Executive Order advances sustainable acquisition by ensuring that 95 percent of new contract actions including task and delivery orders for products and services (with the exception of acquisition of weapon systems) are energy-efficient (such as Energy Star or Federal Energy Management Program designated), water-efficient, bio-based, environmentally preferable (for example, Electronic Product Environmental Assessment Tool certified), non-ozone depleting, contain recycled content, or are non-toxic or less-toxic alternatives, where such products and services meet an agency’s performance requirements.

We continue to encourage management and Congress to renew their efforts to evaluate a new facility that would more appropriately meet Agency needs and be more energy efficient.

Although not required to adhere to the Executive Order, we urge that management 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. These and other stewardship initiatives will require a top-to-bottom and bottom-to-top commitment. Employee empowerment and training will be absolutely necessary for the Agency to achieve its goals and sustain them.

We noted in our previous report that GPO’s environmental executive recommended to the OIG issues to explore with the GPO legislative branch counterparts. Those recommendations include the following:

- consolidating waste-hauling contracts to obtain a more favorable rate for recycled goods as well as ensure that each agency can participate in recycling efforts.
- consolidating standard goods purchasing, such as cafeteria supplies, cleaning chemicals, and paper (in all its forms), to reduce cost and ensure each agency is using the “greenest” products available.
- sharing service contracts to achieve economies of scale and uniformity throughout the legislative branch agencies.

The legislative branch OIGs have reviewed the issues and are exploring crosscutting review opportunities. We again encourage that management address those issues directly with officials in other legislative branch agencies.

We 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 look forward to working with Agency personnel in achieving a long-term and sustainable environmental stewardship program.



OFFICE OF AUDITS AND INSPECTIONS

As the IG Act requires, OAI conducts independent and objective performance and financial audits relating to GPO operations and programs, and oversees the annual financial statement audit an IPA firm conducts. OAI also conducts short-term inspections and assessments of GPO activities, which generally focus on issues limited in scope and time. OIG 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 three new reports. OAI also continued its work with management to close open recommendations carried over from previous reporting periods. As of September 30, 2010, a total of 48 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 2010 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. OIG oversight of KPMG, as differentiated from an audit in accordance with Government Audit Standards,

is not intended to enable us to express, and therefore we do not express, an opinion on GPO's financial statements, the effectiveness of internal controls, or compliance with laws and regulations.

KPMG previously issued an unqualified opinion on GPO's FY 2009 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 two significant deficiencies, which it did not consider to material weaknesses. Those deficiencies were: (1) financial reporting controls and (2) IT general and application controls.

During this reporting period, KPMG began work on the audit of GPO's 2010 consolidated financial statements.

C. AUDIT AND INSPECTION REPORTS

1. Assessment Report 10-07 (Issued June 18, 2010)

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

The FDsys program is intended to modernize the information collection, processing, and dissemination capabilities GPO performs for the three branches of the Federal Government. During this reporting period, the OIG continued to oversee the efforts of American Systems as it conducted IV&V for the public release of FDsys. As part of its contract with the OIG, American Systems is assessing the state of program management, technical and testing plans, and other efforts related to the rollout of Release 1. The contract requires that American Systems issue to the OIG a quarterly Risk Management, Issues, and Traceability Report, providing observations and recommendations on the program's technical, schedule, and cost risks as well as requirements traceability of those risks and the effectiveness of the program management processes in controlling risk avoidance.

This eleventh quarterly report covers the period from January 1, 2010, through April 6, 2010. Although IV&V did not identify any new technical, cost, or

schedule risks, the report discusses issues and concerns addressed in previous quarterly reports. The issues and concerns were already encompassed by open recommendations provided to the PMO in previous IV&V Quarterly Reports.

2. Assessment Report 10-08 (Issued September 16, 2010)

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

The twelfth quarterly report on FDsys covers the period from April 7, 2010, through July 30, 2010. The period covered for this report was extended from June 30 to July 30 in order to include responses from the FDsys PMO to the OIG's request for information related to the first public FDsys Program Review. During this period, IV&V did not identify any new technical, cost, or schedule risks. As a result, we did not make any new recommendations. The report does, however, discuss several issues worth noting as the PMO implements the remaining efforts to complete Release 1. For example, IV&V identified that:

- As of July 28, 2010, the PMO identified a total of 155 Program Tracking Reports (PTRs) that need resolving to complete Release 1 and sunset GPO Access. Resolving those 155 PTRs would result in at least 565 remaining open in various states (for example, Submitted, In Analysis, In Work) when FDsys replaces GPO Access as GPO's electronic system of record.
- Seventy-four system requirements that are "Not Implemented" were assigned the status "Need for Release 1 Completion." Of the 74 requirements, 26 also had associated PTRs. Of the 26 requirements, 18 appear to have been implemented because their associated PTRs were resolved. The other eight requirements in this group were linked to PTRs but not included in a July 28, 2010, list of critical PTRs that must be fixed to sunset GPO Access. Thus, it was not clear whether the PMO intended to resolve these eight as part of the FDsys Release 1 product targeted for the end of FY 2010.
- The other 48 requirements "Not Implemented" with a status of "Need for Release 1 Completion"

had not been assigned to PTRs. Since the Release 1 Completion schedule did not contain a specific task to resolve them, it is unknown if their fixes had already been or would be implemented in the Release 1 time frame.

- The PMO has made substantial progress toward completion of Release 1. The schedule, which is being maintained on a weekly basis, indicates that the Release 1 effort is 58-percent complete. However, the schedule also indicates that significant efforts, specifically those related to the final verification of the system, are incomplete.

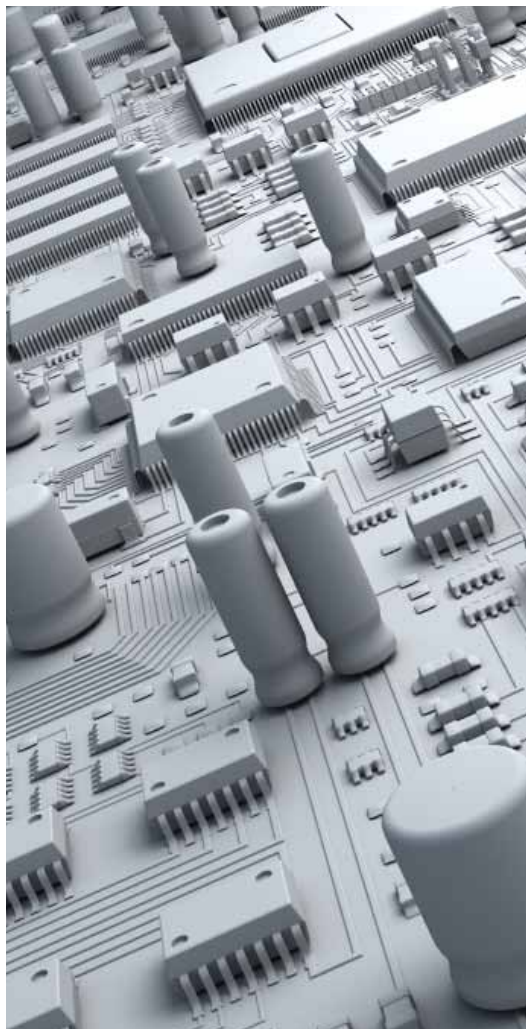
Recommendations provided to the PMO, which address the concerns identified, were provided by IV&V in earlier Quarterly Reports.

3. Assessment Report 10-09 (Issued September 20, 2010)

WebTrust 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, 2009, through June 30, 2010, 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
- CA supporting systems, databases, and PKI facilities

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

As a result of work performed, Ernst & Young issued an attestation report expressing its unqualified

opinion that management's assertion related to the adequacy and effectiveness of controls over its CA operations was, in all material respects, fairly stated based on the AICPA WebTrust for CA Criteria.

D. ONGOING WORK

OAI has several audits and assessments ongoing whose results should be published during the next reporting period. Those assignments include:

- An audit of GPO's Administration of the FDSys Master Integrator Contract will determine whether GPO effectively administered the contract. The audit will specifically determine whether GPO adhered to the Materials Management Acquisition Regulation and other applicable laws, rules, regulations, and guidance related to (1) contract award; (2) monitoring of contract performance; (3) contract modifications; (4) verification of costs incurred; and (5) contract closeout.
- An audit of the GPO Express Program will evaluate management controls over the program, including whether (1) GPO Express cards were adequately controlled and issued, (2) contract terms between FedEx Kinkos and GPO were complied with, and (3) revenues reflected program activity.
- An audit of Control and Accountability of Laptop Computers will determine whether (1) GPO could account for all Agency laptop purchases and (2) controls were in place to prevent the theft or loss of laptops.
- An audit of the GPO Ethics Program will determine whether (1) GPO complied with applicable Federal ethics guidance, and (2) the ethics program at GPO was consistent with Federal Government best practices.
- Senior management requested that the OIG assess compliance of GPO's payroll operations with applicable laws, rules, and regulations. The audit will determine whether GPO complied with applicable guidance related to the (1) request and approval of Leave Without Pay (LWOP); (2) request, approval, calculation, and administration of advanced annual leave; (3) request, approval, calculation, and administration of daily and weekly overtime;

(4) calculation and administration of bi-weekly and annual earnings limits and salary caps; and (5) calculation, payment, and administration of the GPO Goal Sharing Program.

- An audit of the Secure Card Personalization System's (SECAPS) IT Security Controls will determine whether a requisite level of IT security controls was applied to help ensure data integrity, data confidentiality, and system availability.

E. STATUS OF OPEN RECOMMENDATIONS

Management officials made progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. For the 48 recommendations still open, a summary of the findings and recommendations, along with the status of actions for implementing the recommendation and OIG comments, follows.

1. Assessment Report 06-02 (Issued March 28, 2006)

GPO Network Vulnerability Assessment

FINDING

Although GPO has many enterprise network controls in place, improvements that will strengthen the network security posture are needed. During internal testing, we noted several vulnerabilities requiring strengthening of controls. However, no critical vulnerabilities were identified during external testing. Although unclassified, we consider the results of the assessment sensitive and, therefore, limited discussion of its findings.

RECOMMENDATION

The OIG made four recommendations that should strengthen internal controls associated with the GPO enterprise network. Those recommendations should reduce the risk of compromise to GPO data and systems.

MANAGEMENT COMMENTS

Management concurred with each recommendation and initiated corrective action.

OIG COMMENTS

One recommendation made in this report remains open. Implementation of corrective action is still ongoing.



2. Assessment Report 08–12 (Issued September 30, 2008)

Assessment of GPO's Transition Planning for Internet Protocol Version 6 (IPv6)

FINDING

The OIG assessed Agency planning for transition from Internet Protocol version 4 (IPv4) to version 6 (IPv6). Internet routing protocols are used to exchange information across the Internet. Protocols are standards that define how computer data are formatted and received by other computers. IPv6 is a developing Internet protocol that provides benefits such as more Internet addresses, higher qualities of service, and better authentication, data integrity, and data confidentiality. The OIG assessment identified that GPO plans to transition to IPv6 as part of a broad acquisition plan that will update its IT infrastructure. The Agency has not finalized target dates for the updates. The OIG believes that the planned transition is an effective long-term approach. In the short term, however, GPO should consider implementing the minimum IPv6 requirements, which should ensure that resources such as FDSys are capable of ingesting information from IPv6 sources.

RECOMMENDATION

The OIG made two recommendations to management that would enhance planning for the IPv6 transition.

MANAGEMENT COMMENTS

Management concurred with each recommendation and has either taken or planned to take responsive corrective actions.

OIG COMMENTS

One recommendation remains open. The recommendation remains open pending completion of GPO's ongoing infrastructure refresh.

3. Assessment Report 09–01 (Issued November 4, 2008)

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 this 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

Two recommendations remain open. Management continues to work on implementing corrective actions for the three open recommendations.

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

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 10 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

Three recommendations remain open. Management continues to take responsive actions to implement the three open recommendations.

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

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

Three recommendations remain open. Management continues to take responsive actions to implement the three open recommendations.

6. Assessment Report 09–12
(Issued September 30, 2009)

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 each recommendation with the exception of one and proposed responsive corrective actions for each.

OIG COMMENTS

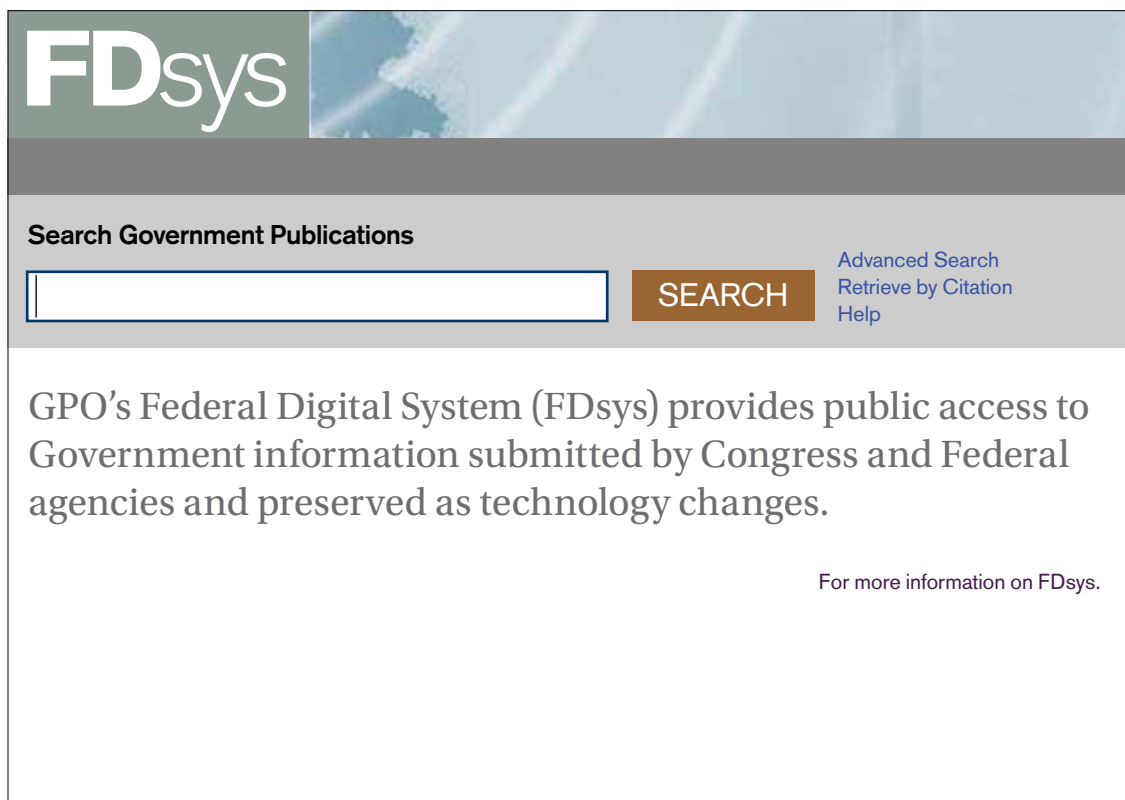
A total of 17 recommendations remain open. The OIG and IV&V continue to monitor the status of their implementation.

7. Assessment Report 10–01
(Issued December 2, 2009)

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



FDsys

Search Government Publications

SEARCH

[Advanced Search](#)
[Retrieve by Citation](#)
[Help](#)

GPO's Federal Digital System (FDsys) provides public access to Government information submitted by Congress and Federal agencies and preserved as technology changes.

For more information on FDsys.

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 a total of 11 recommendations.

MANAGEMENT COMMENTS

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

OIG COMMENTS

Four recommendations remain open. The OIG and IV&V continue to monitor the status of their implementation.

8. 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 the National Institute of Standards and Technology. 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

GPO 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 14 open recommendations.

9. Assessment Report 10–05 (Issued March 24, 2010)

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

FINDING

The tenth quarterly report identifies a number of technical risks associated with FDsys development practices, system engineering, COOP, existing PTRs, and the FDsys test program. American Systems identified schedule and cost risks associated with these technical risks.

Table of Open Recommendations

AUDIT	NUMBER OF OPEN RECOMMENDATIONS	NUMBER OF MONTHS OPEN
06–02 GPO Network Vulnerability Assessment	1	54
08–12 Assessment of GPO’s Transition Planning for Internet Protocol Version 6 (IPv6)	1	24
09–01 Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability	2	22
09–03 FDsys IV&V – Fifth Quarter Report on Risk Management, Issues, and Traceability	3	21
09–07 FDsys IV&V – Sixth Quarter Report on Risk Management, Issues, and Traceability	3	18
09–12 Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Seventh Quarter Report on Risk Management, Issues, and Traceability	17	12
10–01 FDsys IV&V – Ninth Quarter Report on Risk Management, Issues, and Traceability	4	9
10–03 GPO’s Compliance With the Federal Information Security Management Act	14	8
10–05 10–01 FDsys IV&V – Tenth Quarter Report on Risk Management, Issues, and Traceability	3	6

RECOMMENDATION

A total of six recommendations were made to management and were designed to mitigate risks and strengthen overall management of the FDsys program.

MANAGEMENT COMMENTS

Two of the report’s recommendations were subsequently closed as a result of the FDsys program’s decision to transition to an open-ended development effort with objectives (for example, new functionality) that will be defined by stakeholder

inputs and PMO requirements. As a result, those two recommendations were no longer considered applicable as a result of the change in development approach because the PMO does not intend to define a final system and completion date. Of the remaining four recommendations, three were unresolved because of inadequate proposed actions by management.

OIG COMMENTS

Three recommendations remain open as of the end of this reporting period.



OFFICE OF INVESTIGATIONS

OI conducts and coordinates investigative activity related to fraud, waste, and abuse in GPO programs and operations. While concentrating our efforts and resources on major fraud investigations, the activities investigated can include possible wrongdoing by GPO contractors, employees, program participants, and others who commit crimes against GPO.

Investigations that uncover violations of Federal law or GPO rules or regulations may result in administrative sanctions, civil action, and/or criminal prosecution. Prosecutions may result in court-imposed prison terms, probation, fines, or restitution. OI may also issue Management Implication Reports (MIRs), which detail investigative findings that warrant management's prompt attention.

OI is responsible for investigations at all GPO locations, including its 15 Regional Printing Procurement Offices (RPPOs) nationwide. OI also maintains a liaison with the GPO Security Services and Uniform Police Branch to coordinate efforts impacting law enforcement programs. Liaison is also maintained with DOJ, the OIG community, and other investigative agencies and organizations.

A. SUMMARY OF INVESTIGATIVE ACTIVITY

At the end of last reporting period, 22 complaints were open. OI opened 24 new complaint files this period, 10 complaints were converted to full investigations, and 10 were closed after preliminary review with no action. Additionally, nine complaints were referred to GPO management. At the end of the reporting period, 17 complaints remained open.

At the end of the last reporting period, 33 investigations were open. During this reporting period, eight investigations were closed, and eight investigations were opened. Three of the closed investigations were referred to GPO management for potential administrative action. At the end of the reporting period, 33 investigations were ongoing.

During this reporting period, OI made nine presentations to DOJ officials. These presentations resulted in five criminal declinations,

one criminal acceptance, and one civil acceptance. Decisions by DOJ officials are pending on the remaining two.

Four IG subpoenas were issued during this period. Documents requested included financial records, bid preparations, and agreements among contractors and/or affiliated companies.

B. TYPES OF CASES

Procurement Fraud

OI is responsible for identifying and investigating wrongdoing by GPO contractors or employees during the administration of GPO contracts. Violations can include false statements, false claims, product substitution, collusive bidding, bribery, kickbacks, and financial conflicts of interest. In FY 2009, GPO procured more than \$675 million in goods and services through contracting. With such vulnerability in mind, OI has continued to develop investigations in the area of procurement fraud. The inventory of procurement fraud complaints/investigations represents more than 50 percent of our active caseload. Including allegations in complaint status, OI has 26 open procurement matters.

The inventory of procurement fraud complaints/investigations represents more than 50 percent of our active caseload.

Workers' Compensation Fraud

OI investigates GPO employees who allegedly submit false claims or make false statements to receive workers' compensation benefits. We are working on five investigative matters (complaints and investigations) involving possible fraudulent claims for workers' compensation. Two of those cases are being worked jointly with the Office of Inspector General for the Department of Labor.

Employee Misconduct

OI investigates allegations involving GPO employee misconduct. Allegations generally include false statements, theft of Government property or funds, assaults, misuse of Government computers, drug violations, gambling, and travel voucher fraud. OI has seven open investigations and three preliminary complaints involving alleged employee misconduct.

Other Investigations

OI conducts other types of investigations that do not fall into one of the categories above. Examples of such investigations include unauthorized use/access to GPO systems and requests for investigations by outside entities. OI has nine open investigative matters involving allegations of those types.

C. SUMMARY OF INVESTIGATIVE ACCOMPLISHMENTS

Criminal and Civil Cases

- As previously reported, an OI investigation found evidence that a GPO printing contractor failed to comply with critical contract specifications and submitted at least 10 invoices to GPO. Under GPO contract terms, Publication 310.2, Clause 24(b), submission of any invoice for work completed under a GPO contract is a certification that the work was completed in accordance with contract terms. The case was accepted for action by DOJ and on June 7, 2010, and the contractor agreed to pay a \$25,000 settlement of U.S. penalty claims without admitting wrongdoing or liability. Final debarment action against the contractor is pending.
- OI continues an investigation into allegations of false statements, false claims, forgery, and/or bid collusion by GPO print vendors. OI has the assistance of the DOJ Antitrust Division, which is in the process of negotiating a criminal plea agreement with one of the subjects involved.
- OI continues an investigation of allegations relating to false statements and/or false claims to GPO. The DOJ Antitrust Division is evaluating this case for possible criminal and/or civil action.
- As previously reported, an investigation of a printing contractor determined GPO paid more than \$175,000 after the company submitted delivery receipts and invoices for payment, but the contractor failed to perform according to specifications and did not deliver all products. Although DOJ previously declined the

case for criminal prosecution, the case was accepted this reporting period for civil resolution. Coordination is ongoing with DOJ.

- We previously reported that an OI investigation of overbilling by a GPO print contractor was accepted for potential civil action by DOJ. The investigation determined that from February 2002 until February 2004 the president of the company overbilled GPO approximately \$499,000. During this reporting period, the supporting civil Assistant U.S. Attorney submitted a motion for default judgment. Final adjudication is pending.

Internal Administrative Cases

- As previously reported, OI investigated allegations that a GPO employee used or attempted to use her position for personal financial gain and to benefit close friends. This joint investigation with the DOJ Public Integrity Section included numerous interviews, records reviews, and analysis by an independent subject matter expert. DOJ declined prosecution and the investigative results were referred to management, who terminated the employee.

- As previously reported, an OI investigation regarding the possible physical assault of a GPO contractor by a GPO employee was referred to agency management for administrative action. The conduct of the employee toward the contractor (captured on surveillance video) was deemed inappropriate, and the employee received a 3-day suspension.
- We previously reported that OI substantiated allegations that an employee was using GPO equipment to copy and sell digital video discs (DVDs) during work hours. DOJ declined the matter, and OI referred the case to management for action. The Agency considered the behavior inappropriate and imposed a 3-day suspension.
- OI investigated allegations that a GPO employee used a duplicate GPO identification badge to engage in time and attendance fraud. The employee attempted to gain access to GPO using an expired badge and when denied entry, produced a valid badge that had been brought to her by a co-worker. OI found that the employee did in fact have two badges and that on at least three



occasions she had a co-worker perform a Production Reporting for Operations, Budgeting, and Expenditures (PROBE) (a system used to record daily employee time and attendance) transaction with her valid badge 30 minutes before her arrival at work. When interviewed, the subject of this investigation initially provided false statements to the GPO Uniform Police Branch and OI. She ultimately confessed, however, after being confronted with the evidence. This case was declined by DOJ for prosecution and was referred to management for administrative action.

- OI investigated suspicions that a GPO employee was dealing drugs and had a firearm on GPO property. The investigation disclosed the employee had recently been convicted of drug and weapons-related offenses. Although the investigation did not substantiate that the employee had been dealing drugs on GPO property, the employee was dishonest with investigators when questioned about the circumstances of his drug arrest. As a result of the drug conviction and his lack of candor, the employee was terminated from his position with the GPO. The employee appealed the removal, but in September 2010, the Merit Systems Protection Board upheld the removal.
- An OI investigation of a GPO employee determined the individual, by her own admission, knowingly misused GPO's FedEx account to ship several private packages over the course of several years. The misconduct resulted in minimal loss to GPO and DOJ declined the case for prosecution. The investigation was subsequently referred to management who have proposed a 10-day suspension.
- OI investigated allegations that two GPO supervisors were unfairly and inequitably allocating overtime hours to themselves. The investigation did not find evidence supporting the allegations, but did determine the supervisors were working substantive overtime hours to complete work that could be accomplished by their subordinates. Specific findings were referred to management and to OAI for evaluation as part of an ongoing audit of the GPO payroll system.

External Administrative Cases

- OI referred to GPO management information discovered during an investigation of allegations that an individual was associated with several GPO print contractors and may have provided false information on vendor applications submitted to GPO. The investigation substantiated that although the individual was associated with the several GPO contractors, no evidence existed that the employee submitted multiple bids from multiple contractors on the same solicitation.
- OI also referred information to GPO management that an individual submitted two bids for the same contract under the names of two different contractors. The investigation determined that although neither contractor was awarded the job, the individual was associated with several GPO contractors. Further investigation did not identify any other instances where the individual submitted two or more bids for the same GPO solicitation.
- As a result of an investigation into allegations a company was acting as a broker for at least four print contractors in violation of GPO Contract Terms, OI referred information to GPO management. OI found the company attempted to broker at least one GPO contract; however, there was no evidence the company had ever been awarded any GPO contracts.
- Finally, OI referred to the GPO Office of General Counsel the findings of an investigation into allegations that a GPO contractor submitted invoices to GPO before shipping the finished product to the customer. The investigation substantiated that the contractor submitted a false invoice indicating that the product had been shipped, when in fact the materials were not shipped until almost 3 weeks later.

Miscellaneous Cases

- OI investigated allegations by a GPO employee that she was wrongfully arrested by the GPO Uniform Police Branch for assaulting another employee. The arrested employee further alleged that the arrest was



racially biased and handled in an unprofessional manner. The OI investigation found no evidence that the employee was wrongfully arrested. The Uniform Police Branch supervisor ordering the arrest discussed the arrest with superiors and they agreed with the supervisor's decision to arrest the employee for simple assault under D.C. Code § 22-404. Further, OI did not find any indication of racial bias. The findings of this investigation were also referred to Uniform Police Branch management, and it was recommended that the Uniform Police Branch and the Office of General Counsel work to expeditiously approve and implement General Orders and a Memorandum of Understanding with the Washington, D.C., Metropolitan Police Department. The OIG recommended that management in the Uniform Police Branch address any conflicts between branch supervisors and subordinate officers to foster professional behavior and clearly define a chain of command.

- OI investigated allegations that a former OIG employee ordered and distributed seven sets of honorary badges and credentials. OI became aware of the badges and credentials after being contacted by a law enforcement official who retrieved one during execution of a search warrant. The subject of the search warrant informed OI that he was asked by the former OIG employee to print some honorary credentials. OI conducted numerous interviews and was able to retrieve two more sets of honorary badges and credentials. The former employee was located in another state, but he was unwilling to cooperate with OI. Ultimately, OI determined the disposition of the remaining four sets of credentials, but because the former employee was unwilling to cooperate, it could not identify the individuals to whom the badges and credentials were given. DOJ declined the case for prosecution.

D. OTHER SIGNIFICANT ACTIVITIES

We continue other efforts to improve our abilities to detect, prevent, and investigate the loss of Government assets. The following summarizes other significant activities occurring in OI:

- Members of OI and OAI staff attended training on paper specifications and testing that the GPO Quality Control and Inventory Management Branch presented. The training focused on how paper is produced and how different types and specifications of paper are coded by the Joint Committee on Printing. Information was also presented about the various types of pulp used in producing paper. Special attention was given to the process by which recycled paper becomes post-consumer waste pulp, which is a required component in a significant percentage of the paper used in Federal printing. The training provided valuable information about ongoing product substitution investigations and potential joint OI/OAI initiatives.
- Personnel from OI and OAI also toured a de-inking and post-consumer waste pulp production facility. The tour provided in-depth exposure on

how post-consumer waste paper becomes pulp used as a component in the recycled paper used for Federal printing. The same OI and OAI personnel then visited a paper mill and witnessed first hand how a modern paper mill operates. The tour highlighted how paper mills alter production recipes to produce different paper types and specifications. This tour familiarized OI and OAI personnel with the paper manufacturing process and raw materials used.

- Special Agents in OI are Federal Criminal Investigators (general schedule job series 1811) and are designated as Special Police Officers by the Public Printer. This reporting period, all general schedule 1811 Criminal Investigators were granted special deputation by the U.S. Marshals Service. Over the last 2 years, OI has continued to develop an inventory of complex criminal and civil investigations requiring nationwide travel and frequent coordination with DOJ. The additional authority granted through special deputation will allow OI to independently investigate contractors throughout the United States and act as the lead agency when executing search and arrest warrants.

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	IPA	Independent Public Accountant
CA	Certification Authority	IPv6	Internet Protocol version 6
CIGIE	Council of Inspectors General on Integrity and Efficiency	IT	Information Technology
CMS	Center for Medicare and Medicaid Services	IT&S	Information Technology and Systems
CPS	Certification Practices Statement	IV&V	Independent Verification and Validation
COA	Continuity of Access	MIR	Management Implication Report
COOP	Continuity of Operations	OA	Organization Architects
COTR	Contracting Officer's Technical Representative	OALC	Office of Administration/Legal Counsel
DE	Delegated Examining	OAI	Office of Audits and Inspections
DHS/CPB	Department of Homeland Security/ Customs and Border Patrol	OGC	Office of General Counsel
FDsys	Federal Digital System	OI	Office of Investigations
FISMA	Federal Information Security Management Act	OIG	Office of Inspector General
FY	Fiscal Year	OMB	Office of Management and Budget
GAO	Government Accountability Office	OPM	Office of Personnel Management
GBIS	GPO's Business Information System	OWC	Office of Workers' Compensation
GPO	U.S. Government Printing Office	PII	Personally Identifiable Information
HSPD-12	Homeland Security Presidential Directive-12	PKI	Public Key Infrastructure
ICAO	International Civil Aviation Organization	PO	Privacy Officer
IG	Inspector General	PPPS	Passport Printing and Production System
IG ACT	GPO Inspector General Act, as amended	PTR	Problem Tracking Report
		RPPO	Regional Printing Procurement Office
		SAS	Statement on Auditing Standards
		SCC	Secure Credential Center
		SID	Security and Intelligent Documents
		SPF	Secure Production Facility
		TTP	Trusted Traveler Program

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	8
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	22–29
Section 5(a)(2)	Recommendations for Corrective Actions	22–29
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	24–29
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	32–35
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	22–24
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	41
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	42
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
48Section 5 (a) (14–16)	Peer Review Results	47–48

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
<hr/>		
Reports issued during the reporting period	0	\$0
<hr/>		
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
<hr/>		
Reports for which no management decision made by the end of the reporting period	0	\$0
<hr/>		
Report for which no management decision made within 6 months of issuance	0	\$0
<hr/>		

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

REPORTS	FUNDS PUT TO BETTER USE
Report on Federal Digital System (Fdsys) Independent Verification and Validation – Eleventh Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-07, issued June 18, 2010)	\$0
Report on Federal Digital System (Fdsys) Independent Verification and Validation – Twelfth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-08, issued September 16, 2010)	\$0
Report on WebTrust Assessment of GPO's Public Key Infrastructure Certification Authority – Attestation Report (Assessment Report 10-09, issued September 20, 2010)	\$0
Total	\$0

Table C-4: Investigations Case Summary

Total New Hotline/Other Allegations Received during Reporting Period	43
No Formal Investigative Action Required	6
Investigations Opened by OI during Reporting Period	8
Investigations Open at Beginning of Reporting Period	33
Investigations Closed during Reporting Period	8
Investigations Open at End of Reporting Period	33
Referrals to GPO Management	12
Referrals to Other Agencies	5
Referrals to OAI	2

Current Open Investigations by Allegation		
Procurement Fraud	20	61%
Employee Misconduct	7	21%
Workers' Compensation Fraud	3	9%
Other Investigations	2	9%

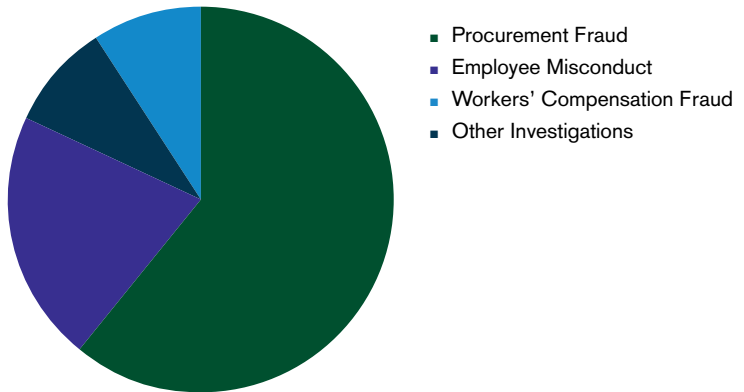


Table C-5: Investigations Productivity Summary

Arrests	0
Total Presentations to Prosecuting Authorities	9
Criminal Acceptances	1
Criminal Declinations	5
Indictments	0
Convictions	0
Guilty Pleas	0
Probation (months)	0
Jail Time (days)	0
Civil Restitutions	0
Civil Acceptances	1
Civil Agreements	1
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	0
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	12
Contractor Debarments	0
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions	5
Employee Terminations	1
Other Law Enforcement Agency Referrals	5

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

In November 30, 2006, the National Science Foundation (NSF) OIG issued a Peer Review Report of the GPO OIG audit function. The NSF OIG found that the system of quality control for the audit function at the GPO OIG in effect for the year ending March 31, 2006, met the requirements of the quality control standards established by the Comptroller General of the United States for a Federal Government audit organization and complied with during the year ending March 31, 2006, provided GPO with reasonable assurances of conforming with applicable auditing standards, policies, and procedures.

The NSF OIG recommended that GPO OIG request an interim peer review or conduct a comprehensive internal quality control review of its audit operations under its new audit policy and procedures manual (issued in July 2006), but due to inadequate resources, was not able to conduct a comprehensive internal quality control review. The GPO OIG audit function will undergo a peer review during this upcoming reporting period.

B. Peer Review of the Investigation Function

The GPO does not derive its statutory law enforcement power from Section 6(e) of the IG Act of 1978, as amended; therefore it is not required to undergo an external peer review of its investigation function. Nevertheless, the OIG voluntarily requests such external peer reviews.

The Farm Credit Administration (FCA) OIG conducted the last peer review of the GPO OIG investigation function and issued its opinion on June 1, 2005. The FCA OIG found that the system of internal safeguards and management procedures for the investigative function in effect for the period ending

February 5, 2005, was in full compliance with the quality standards established by the President's Council on Integrity and Efficiency (PCIE)/Executive Council on Integrity and Efficiency (ECIE). The safeguards and procedures provide reasonable assurance of conforming with professional standards in the conduct of its investigations. There are no outstanding recommendations from that peer review.

The GPO OIG investigation function will undergo a peer review during this upcoming reporting period.

C. External Peer Reviews

In 2008, the GPO OIG conducted two external peer reviews of the audit and investigative functions of the Board of Governors of the Federal Reserve System (Board) OIG. On March 31, 2008, the GPO OIG issued an Investigative Peer Review report. We found that the system of internal safeguards and management procedures for the investigative function of the Board OIG in effect for the period ended January 10, 2008, is in compliance with the quality standards established by the PCIE/ECIE, Special Deputation U.S. Marshal authority, or the Attorney General Guidelines for Office of Inspectors General with Statutory Law Enforcement Authority. These safeguards and procedures provide reasonable assurance of conforming with professional standards in the conduct of Board OIG investigations. No recommendations were issued in this report.

On September 4, 2008, the GPO OIG issued an Audit Peer Review report. We found that the quality control system for the audit function of the Board OIG in effect for the 18-month period ending March 31, 2008, met the requirements of the quality control standards established by the Comptroller General of the United States for a Federal Government audit organization and complied with during the year ending March 31, 2008, provided the Board OIG with reasonable assurances of conforming with applicable auditing standards, policies, and procedures. There are no outstanding recommendations from this peer review report.

U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

732 North Capitol Street, NW, Washington, D.C. 20401
202.512.0039 • www.gpo.gov/oig
OIG HOTLINE 1.800.743.7574 • gpoighotline@gpo.gov