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

SEMIANNUAL REPORT TO CONGRESS

October 1, 2009 to March 31, 2010

U.S. GOVERNMENT PRINTING OFFICE

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 GPO OIG 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

Security is always excessive until it's not enough.

— Robbie Sinclair,
Head of Security,
Country Energy,
NSW Australia

I am pleased to present this Semiannual Report to Congress, which covers the activities of the GPO Office of Inspector General for the period October 1, 2009 through March 31, 2010.

Of particular importance during this reporting period was our work on security issues. The Office of Audits and Inspections (OAI) finalized an audit of the security of the e-Passport components supply chain. GPO is the sole producer of blank e-Passports to the Department of State. As further noted in the OAI section, the audit identified that the e-Passport supply chain security process was largely informal and GPO offices with overlapping responsibility should have been coordinating their work efforts rather than working autonomously.

Such an informal and uncoordinated process led to, among other things, insufficient security audits of critical e-Passport suppliers, lack of contractual control over subcontractors providing critical e-Passport components, and lack of contractor security plans or security-related requirements for some suppliers. We will monitor management's plan to implement necessary internal controls over the supply chain to ensure the security of e-Passport production.

In addition, the Office of Investigations investigated the loss of 18 laptop computers from an agency storage area. We were unable, however, to determine the disposition of these laptops due to the lack of security and inventory control over these materials. As a result, an audit is underway that will focus on security of agency property and management controls.

In this report, we also update the most significant management challenges facing the Agency. We note that human capital operations and management remains a critical challenge to the Agency. We are hopeful that the ongoing reorganization and focus on customer-driven solutions will bring about much needed change and direction. As noted previously, commitment by GPO senior management should bring about significant operational improvement.

The GPO OIG remains committed to quality, integrity, accountability, and transparency as we continue to fulfill our mission and goals. I encourage you to visit our website (www.gpo.gov/oig) and, to keep informed of OIG activities, please sign up to receive automatic email updates.

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

HIGHLIGHTS OF THIS SEMIANNUAL REPORT

The *Office of Audits and Inspections* (OAI) issued six new audit and assessment reports. Those 6 reports contained 45 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency. OAI issued a supply chain security audit of the Agency's e-Passport production activities. OAI continued to oversee the Independent Verification and Validation (IV&V) efforts related to implementation of the Federal Digital System (FDsys) and the annual audit of GPO's financial statement.

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

- Completed an audit report assessing the adequacy of GPO's security over its e-Passport components. The audit identified that the e-Passport supply chain security process was largely informal and that different GPO offices with overlapping responsibility related to e-Passport production or security should have been coordinating their work rather than working autonomously, which would have ensured proper security protocols over critical e-Passport component suppliers. Such an informal and uncoordinated process led to insufficient security audits of critical e-Passport suppliers, lack of contractual control over subcontractors providing e-Passport components, lack of contractor security plans or security-related requirements, and lack of required contract file documentation for some suppliers. Management concurred with our recommendations, which were designed to strengthen the security of the e-Passport supply chain.
- Completed our oversight responsibilities with respect to GPO's annual financial statement audit for which the Agency again received an unqualified opinion from the Independent Public Accounting (IPA) firm of KPMG, LLP.
- Completed an assessment of GPO's compliance with the Federal Information Security Management Act (FISMA), finding that although the Agency has made some progress in complying with FISMA, additional improvements are needed.
- Completed an assessment of GPO's network vulnerability management finding that the Agency implemented a robust and effective

program that identifies and circumvents common internal and external network threats.

- Issued two quarterly IV&V reports on the FDsys and made recommendations designed to strengthen program management, particularly technical risks associated with risk management and configuration management for future FDsys releases.

The *Office of Investigations* (OI) opened 10 full investigations and 26 complaints for preliminary investigation, while closing 15 investigations and 28 complaints (8 of which were closed with no action). At the end of this reporting period, the OI has 33 ongoing investigations and 22 open complaints. Additionally, seven investigations resulted in referrals to GPO management for potential administrative action, and eight complaints were referred to GPO management or other agencies.

Of the open complaints and investigations, 31 involve allegations of procurement fraud, demonstrating increased OI efforts in addressing procurement and financial fraud vulnerability within GPO. This heightened increase in procurement fraud cases is just one of the results of OI efforts to engage and educate management, Print Procurement officials, and other acquisitions employees.

Several ongoing investigations are being conducted in coordination with the Department of Justice, including its Antitrust Division. As part of the investigations, the Inspector General (IG) issued 12 subpoenas for documents this reporting period.

Among OI's significant accomplishments during this reporting period include:

- Investigated allegations that a GPO employee used or attempted to use her position for personal financial gain and benefit close friends. As part of this investigation, OI staff worked jointly with the Department of Justice Public Integrity Section, and management proposed terminating the employee.
- Investigated disposition of 18 laptop/portable computers identified as missing from an Information Technology and Systems (IT&S) Division storage area at the GPO headquarters building. We reported to management that as a result of a lack of security and inventory controls in IT&S, OI was unable to determine the final disposition of 18 missing laptops. The findings of the investigation were referred to OAI, which initiated an audit of IT&S property management protocols.
- As a result of a previously reported OI investigation, which found that GPO employees failed to provide truthful information during an administrative investigation conducted by GPO Human Capital Office, three employees retired after receiving notice of termination and the fourth received a 30-day suspension and demotion.

OI continues investigations into allegations of false statements, false claims, and/or bid collusion by GPO print vendors. OI has the assistance of the Department of Justice Antitrust Division, which continues to evaluate the 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 often reviews and edits audit, inspection, and investigative reports before the IG approves.

During this reporting period, OALC accomplished the following:

- Reviewed, edited, and approved 12 subpoenas.
- Developed a Memorandum of Understanding with GPO's IT&S to establish policies about access to and security of OIG digital information on GPO servers.
- Developed an internal administrative policy for streamlining and formalizing administrative procedures.
- Drafted an information security policy for discussion to be completed and finalized during the next reporting period.
- Began the internal process for an update of the OIG's strategic plan.
- Provided support to the IG in his capacity as Chairman of the Legislation Committee of the Council

of Inspectors General on Integrity and Efficiency (CIGIE).

- Received an award from the Council of Counsels to the Inspector General (CCIG) for exemplary service to the CCIG Website Working Group.
- Acted on a variety of matters as the OIG liaison to the GPO General Counsel, including support with GPO litigation and personnel action matters and the GPO Chief of Staff's office.

OIG MANAGEMENT INITIATIVES

During this reporting period, senior managers began work on updating the OIG 3-year strategic plan. An office-wide retreat in June 2010 is planned where managers and employees will discuss the vision, direction, and goals of the OIG and how to continue to enhance, improve, and measure the success of its operations. The OIG was also featured in the GPO publication, *Typeline*, which is a quarterly magazine issued to all GPO employees. The *Typeline* article discussed the role and work of the OIG through personal interviews with an investigator, Elisabeth Heller, and an auditor, Karl Allen. The OIG will continue to work on a communications strategy for reaching as many GPO employees as possible to educate them 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, Rebecca Sharek joined OAI as a supervisory auditor. Rebecca brings 15 years of audit experience to the OIG from the National Aeronautics and Space Administration (NASA). While at NASA, Rebecca was a Program Manager in the OIG, where she supervised a variety of audits related to the Manned Spaceflight Program and Safety and Mission Assurance. She also worked as the Audit Liaison and Business Systems Manager at the John F. Kennedy Space Center. Rebecca is a Certified Internal Auditor and graduated from Rollins College in Florida. She has a Master's Degree in Business Administration from the University of Central Florida.

Elisabeth Heller, special agent, and Karl Allen, supervisory auditor, were featured in the GPO employee publication *Typeline*. Rebecca Sharek joined the OIG as a supervisory auditor.

COUNCIL OF INSPECTORS GENERAL FOR INTEGRITY AND EFFICIENCY

On October 14, 2008, the Inspector General 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 develop 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 engaged in communications with several congressional committees on various legislative matters affecting the IG community, most significantly to:

- Express support for IG subpoena authority that includes attendance and testimony of non-Federal agency witnesses to aid audits and investigations that may be hampered by lack of cooperation of private contractors, grantees, former employees, and other third parties.
- Convey the results of a CIGIE survey conducted to assess 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.

Legislative branch IGs continued to meet quarterly in response to a Senate Appropriations Committee request that the IGs throughout the legislative branch communicate, cooperate, and coordinate with one another on an informal basis. The meetings continue to improve communications and contact between the legislative branch IGs. During this reporting period, the Inspector General for the U.S. Capitol Police hosted the meeting. Some issues discussed and under ongoing consideration include:

- Shared training opportunities for legislative branch OIG personnel.
- Cross-cutting legislative branch audits and inspections to include concerns regarding agency protection of personally identifiable information (PII).
- Joint efforts to improve environmental conditions and reduce costs.
- Development of consistent OIG privacy protection policies.
- 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 makes recommendations 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. In an effort to assist the Agency in achieving its goals, we continue to play an active role in that area.

Although there were no legislative proposals relating to GPO programs and operations, the OIG reviewed and provided comments on a proposed Directive to protect PII.

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 have refreshed the list of management challenges that 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 OIG semiannual reporting periods. HC operations are at the heart of effectively accomplishing an agency's mission. In essence, HC provides the services necessary to acquire the most precious and important source of productivity—its employees.

Indeed, writing about the challenges of human capital, J. Christopher Mihm recently noted 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]

The Government Accountability Office (GAO) has identified four critical areas related to Strategic HC Management 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]

Based on our own experience as clients of HC, a recent investigation of a HC employee and the results of recent internal and external HC reviews, we are concerned that management has not placed enough emphasis on addressing these four areas to transform HC operations and management. First, we noted previously that the Office of Personnel Management (OPM) completed an HC Management Review of GPO in late 2008. The objectives of the review were to determine whether GPO adhered to merit systems principles as well as complied with applicable laws and regulations. OPM also assessed the Agency's efficiency and effectiveness in administering HC and human resources management programs and systems.

Among the significant findings of the OPM evaluation were that GPO (1) did not finalize its long-term strategic goals and objectives, (2) did not conduct a workforce analysis identifying its mission-critical occupations and competencies, (3) had no indication that the existing HC function had the capacity and data structure needed to partner strategically with managers to conduct workforce analysis and planning, and (4) did not assess its organizational, occupational, and individual needs or evaluate the training offered to determine how well it meets short- and long-range program needs. While management did not fully agree with the OPM findings, the Agency did indicate that it has either planned or initiated actions addressing the recommendations. We encourage management to undertake and complete all actions necessary to address these recommendations.

We also believe that the Agency faces challenges in acquiring, developing, and retaining a diverse, qualified workforce with the right skill sets 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 in the report that the Public Printer adopt all or a combination of the leading practices that the GAO recommends for establishing a model Federal Government program. GPO management agreed with our recommendations.

As of this reporting period, however, we are not able to close the recommendations in the report and urge that GPO management, once again, provide a comprehensive plan for addressing implementation of the recommendations. In addition, as previously noted, although the Agency has begun training management on "EEO and Discriminatory Harassment," comprehensive diversity training for managers and employees at GPO is still needed.

[1] "Human Capital: Federal workforce challenges in the Twenty-first Century," in Hannah S. Sistare, Myra Howze Shiplett 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. at 19.
[3] GAO Report GAO-09-632T, http://www.gao.gov/new.items/d09632t.pdf.

We are also concerned that HC operations are hampered by a broken culture. As a result, in part, of issues the OIG raised regarding processing new OIG employees since August of 2008, management tasked its Organizational Architects (OAs) with conducting an HC operations review. Among other things, the focus was to assess HC operations and procedures for processing new employees as well as within-grade increases. OA found that more than 50 percent of personnel processed through HC at GPO in Fiscal Year (FY) 2009 experienced errors. The review noted a lack of ownership, responsibility, and accountability for those errors as significant problems. The review also noted a lack of means for measuring accuracy and performance incentives focusing on speed rather than accuracy. According to the review, the culture in HC allows for "blaming, finger pointing and ultimately mistakes," which has resulted in "extremely" low HC employee morale.

In response to the OA review, management is working closely with OPM to restructure HC operations. For HC to successfully transform to a high-performing business unit, the restructuring must not, however, be simply a re-shuffling of the chairs but actually produce a change in the HC culture to achieve "results-oriented, customer-focused, and collaborative" HC solutions.

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

Noteworthy challenges for IT&S include establishing a top-level Enterprise Architecture and support for several significant initiatives, including FDsys, the e-Passport system, digital publication authentication using a Public Key Infrastructure (PKI), information system management, implementation of the GPO's 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 initiated an analysis of legacy applications and their impact on business operations. 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 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. Many of the weaknesses identified during the FY 2007 baseline assessment still exist.

Looking forward, the potential changes to FISMA resulting from draft legislation currently before Congress present IT&S with areas to monitor and incorporate into GPO's FISMA planning process.

b. Implementation of the Federal Digital System

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. FDsys has three major subsystems: the content management subsystem and 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 will design, procure, develop, integrate, and deploy select technologies and components of FDsys.

The OIG is responsible for the IV&V work associated with developing and implementing FDsys. We contracted with American Systems to conduct programmatic and technical evaluations of the FDsys Program and determine whether system implementation complies with the FDsys project plan and cost plan as well as meets GPO requirements. The IV&V effort also monitors development and program management practices and processes to anticipate potential issues.

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 from the contractor the role of Master Integrator. The PMO also assumed 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, which employed 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, were released in late March of 2009. Since deployment, the PMO has updated and upgraded the beta system and corrected deficiencies identified during testing.

During this reporting period, the PMO completed the deployment of several post-Release 1 production builds. Despite these deployments, however, FDsys Release 1 is still not complete and close to 4 years have elapsed since inception of the Program in August 2006. The beta system contains less than half (only 25) of the GPO Access Collections. Both GPO Access and FDsys must be operational to ensure that all GPO content is available to the public. The Continuity of Operations (COOP) capability, a critical step in the transition from GPO Access to FDsys as the "system of record," is not yet implemented.

In addition, as of February 28, 2010, GPO expended $36.5 million (unaudited) to deploy Release 1, substantially exceeding the original planned cost of $16 million. This expenditure has yet to produce a final version of Release 1, and a beta version of the release contains considerably less functionality in terms of the system requirements than originally planned.

A complete IV&V assessment of the quality of the FDsys Program 6 months into FY 2010 remains difficult at this time, but several concerns should be highlighted. First, although the Program has met its initial goal of fielding a beta system, the PMO is still having difficulty closing out Release 1. Recently, the PMO published an initial Release 1 Completion Plan, delineating high-level milestones required for the "sunsetting" of GPO Access and the establishment of FDsys as the GPO system of record. Although the plan is a good start, if the PMO fails to effectively manage the plan in areas such as tracking costs, schedule, and resources, the overall goal of completing Release 1 by the end of FY 2010 may not be achieved.

Another concern is the apparent change in the criteria the PMO previously identified as a prerequisite for "sunsetting" GPO Access. This criteria included the availability of a full COOP capability. According to the Release 1 Completion Plan, this capability will not be initially available. Instead, the PMO intends to create a Continuity of Access (COA) Instance until the entire COOP effort can be completed. The COA concept is scheduled to be operational August 2010. The most recent completion date for a full COOP capability is December 2010.

A more troublesome concern for the FDsys Program is the quality of the deployed system. While the testing effort has improved and become more rigorous, the test team continues to identify numerous software problems prior to deployment of major production builds. The problems, documented as Problem Tracking Reports (PTRs), describe errors or deficiencies in system operation and failures to meet expected performance. With each deployment the number of PTRs has grown, and hundreds of PTRs remain open. The ongoing need to resolve and close the PTRs consumes program resources and reduces PMO ability to develop and deploy new functionality.

This brief assessment does not mean to imply that the Program lacks effort or has failed to produce a viable product. The FDsys beta system has received praise for its look, feel, and ease of use. The PMO has also dealt with external commitments and requests (for example, availability of bulk data) that have altered the internal priorities and resulted in the delay of work on development of the capabilities envisioned for FDsys. The OIG believes that the primary challenges for the FDsys Program are in the areas of program management, system engineering leadership, and technical direction as well as 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 those risks.

c. Other Challenges

On August 23, 2009, GPO's Persistent Uniform Resource Locator (PURL)[4] server failed, causing significant downtime for Federal depository libraries across the United States in disseminating U.S. Government information. Surprisingly, no backup plan existed, and IT&S could not provide the necessary software application support for the rebuild process. As a result, GPO ended up outsourcing the

[4] PURLs are Web addresses that act as permanent identifiers for changing Web infrastructure. PURLs are persistent because once established, a PURL does not change although a Web page may change.

building of a "bridge of stability" for the current system. Ultimately, we believe that FDsys will address persistent identification of content requirements, but at present there is no timeline to complete this transition.

As a result of the server failure, we initiated an inspection to determine what caused the server to fail, why no backup capability was available, and why IT&S could not support the rebuild process. The results of our inspection could identify lessons learned to help prevent similar incidents from occurring. We expect to issue a report during the next reporting period.

3. Security and Intelligent Documents. As the Federal Government's leading provider of secure credentials and identity documents, Security and Intelligent Documents (SID) is a business unit that management believes best exemplifies the Agency's transformation toward high-technology production. During this reporting period, SID reported successful manufacturing for the Department of State of more than 5.5 million electronic passports (e-Passport). The Washington, D.C., facility produced more than 3.7 million passports while the Secure Production Facility (SPF) located at a COOP site in Stennis, Mississippi, produced more than 1.8 million passports. The FY 2010 production target volume for the Department of State is a total of 11 million passports.

During this reporting period, the OIG issued a final audit report on the security of the e-Passport supply chain. This report is the latest product resulting from the OIG's continuing oversight of the e-Passport production process. As further noted in the OAI section, the audit identified that the e-Passport supply chain security process was largely informal and GPO offices with overlapping responsibility should have been coordinating their work efforts rather than working autonomously.

Such an informal and uncoordinated process led to insufficient security audits of critical e-Passport suppliers, lack of contractual control over subcontractors providing e-Passport components, lack of contractor security plans or security-related requirements and lack of required contract file documentation for some suppliers. Management concurred with our recommendations to strengthen the security of the e-Passport supply chain. We will monitor management's plan

to implement necessary internal controls over e-Passport supply chain security.

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).[5] SCC also produces, personalizes, and distributes the Department of Health and Human Services Center for Medicare and Medicaid Service's (CMS) Medicare identification cards to citizens of Puerto Rico. As opposed to blank e-Passport production, which does 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.

During this reporting period, the OIG began an audit of GPO's secure personalization system (SECAPS) information technology security controls. SECAPS is the baseline for personalization operations

[5] TTPs provide expedited travel for preapproved, low-risk travelers through dedicated lanes and kiosks by providing them secure identification cards.

that support various GPO customer identity card programs, including TTP and CMS. The audit will determine whether a requisite level of information technology security controls is being applied to help ensure data integrity, data confidentiality, and system availability. Because SECAPS handles PII, the OIG is placing particular audit emphasis on security controls over PII. The audit includes a security evaluation of SECAPS physical controls, system interconnections and the transmission of PII, operating systems and database systems supporting SECAPS, and purging of PII.

Standards promote industry best practices for occupational health and safety standards and programs in a production environment. SID reported the continuation of 5S audits at both plant locations. 5S is a series of defined steps and audits intended to improve efficiencies in manufacturing process flows, equipment usage and placement, and environmental housekeeping standards. According to SID, both locations (the District of Columbia and Stennis) continued to refine and formalize standard operating procedures used in the planned ISO 9000 audits and certification process.[6] Additionally, SID is working to complete a library of standard operating procedures that will underpin and lay the foundation for the OHSAS 18001 certification at a future date.[7]

SID reported that it also continues its work to complete the certification process for SCC to become a facility qualified to handle, personalize, and distribute Homeland Security Presidential Directive 12 (HSPD-12) cards. SID expects certification sometime during the next reporting period. Completion will allow SCC

to more comprehensively serve Federal Government organizations in the area of secure credentials. SID is also working to develop the 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.

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

Because of SID's growing strategic importance for the Agency's transformation efforts and its sensitive work in areas of national security, the OIG will closely monitor management's efforts in developing formal, internal security controls of these products and continue to emphasize oversight of production and transportation processes.

4. Internal Controls. GPO management establishes and maintains a system of internal controls for effective and efficient operations, reliable financial reporting,

[6] ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards. The 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.

[7] 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.

and compliance with laws and regulations. Almost all OIG audits include assessments of a program, activity, or function's control structure and the OIG has several ongoing audits that are assessing internal controls.

Of concern, however, is that our audits continue to identify issues related to internal controls. For example, we issued during this reporting period a report of an audit that reviewed and evaluated internal controls associated with the security of GPO's e-Passport supply chain. As part of that evaluation, 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 defined key areas of authority, responsibility, and appropriate lines of reporting for e-Passport supply chain security. We identified 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 recommended 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."

As further discussed in the OAI section, during the FY 2009 financial statement audit, KPMG identified two significant internal control deficiencies it did not consider material weaknesses. The significant deficiencies identified by KPMG were related to (1) financial reporting controls, and (2) information technology (IT) general and application controls. An evaluation of internal controls will continue to be an area of emphasis on all OIG audits.

5. Protection of Sensitive Information. GPO must establish rules of conduct and appropriate administrative, technical, and physical safeguards that will adequately identify and protect sensitive information. Failure to do so 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 the breach of PII. This includes PII contained in information systems as well as paper documents. In accordance with OMB Memoranda 06-15 and 07-16, executive branch agencies had to implement policies and procedures to protect and respond to the breach of PII as far back as the middle of 2007.

As noted in previous reporting periods, the OIG advised GPO of its concerns regarding protection of sensitive information, including PII. FISMA requires each agency to 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's IT&S Division is making progress in protecting PII contained in information systems. However, at the completion of our latest assessment, GPO had not designated an official responsible for managing and monitoring the Agency's privacy compliance efforts. As a result, privacy requirements have not been adequately identified and communicated to other responsible officials.

We are encouraged though that progress has occurred in this area during this reporting period.

We recognize that management concurred with our previous recommendations that GPO immediately identify any contracts and contractors handling PII, review security requirements, request security plans, conduct on-site surveys and inspections, and appoint a GPO Privacy Officer who will establish and oversee a comprehensive sensitive information protection program. Indeed, during this reporting period, GPO issued two Directives addressing PII. The first one, Directive 110.15C, "U.S. Government Printing Office Contract Review Board (CRB)," dated March 29, 2010, prescribes the functions, the composition, and the responsibilities of GPO's CRB and addresses PII issues related to print contract awards involving PII. The CRB provides an objective and independent review of select proposed procurement actions of Print Procurement or Acquisition Services for compliance with applicable GPO and Government laws, polices, and procedures. The Directive specifically states that for awards involving PII or other sensitive information, before the contract is awarded, contracting officers must provide the CRB with "signed and dated confirmation from the GPO's Federal agency customer that the proposed awardee meets all PII or sensitive information handling requirements . . . [and] a copy of the security plan. . . ."

Directive 825.41, "Protection of Personally Identifiable Information," dated March 30, 2010, establishes a framework for the protection of PII at GPO. Under the Directive, the Public Printer will appoint a person at the senior manager level as Privacy Officer (PO) who will implement the Directive. The first tasks the PO will undertake will be review of PII held by all 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. We will monitor implementation of Directive 825.41 to ensure that safeguards are in place, implemented, and followed.

6. Acquisitions and Print Procurement. As with other Federal agencies across the Government, 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 $675 million in acquisitions during FY 2009, we remain concerned that the Agency has not devoted the resources necessary to conduct independent assessments of Acquisition Services that clearly identify gaps in effective performance and implement a plan for resolving critical issues, as required for executive branch agencies under the Services Acquisition Reform Act of 2003 and OMB guidelines.

Last year OMB provided guidelines to executive branch agencies to 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.[8] Although GPO is not required to follow OMB guidelines in that area, we believe that the Agency would benefit from performing that review process of Acquisition Services. We look forward to the results of the independent assessment that the Public Printer announced in his November 30, 2009, letter to Congress.

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. 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 our office so we can review and investigate Agency contracting actions and administration. Acquisition Services should comply with the MMAR by properly documenting contract files.

In addition, we are concerned 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

[8] GAO Report GAO-05-218G, September 2005, http://www.gao.gov/new.items/d05218g.pdf.

the operations of companies that provide critical components for the e-Passport. Acquisition Services should work in coordination with the Office of General Counsel and SID to ensure that all contracts related to the e-Passport, and other sensitive identity products, include such language to ensure proper security plans and oversight rights.

Finally, as discussed below on the issue of environmental stewardship, GPO's Acquisition Services should develop a goal of advance sustainable acquisition. Executive Order 13514, dated October 5, 2009, requires executive branch agencies to ensure that 95 percent of applicable contracts meet sustainability requirements. We recommend that GPO set an equally ambitious goal as part of its sustainable procurement agenda.

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 for results. Better budget and performance integration has become even more critical for results-oriented management and efficient allocation of scarce resources among competing needs. OIG auditors and the contractors they oversee are vital in keeping the Federal Government's financial information and reporting transparent, valid, and useful to agency decision makers and other stakeholders. GPO has completed migration of current business, operational, and financial systems, including associated work processes, to an integrated system of Oracle enterprise software and applications known as the Oracle E-Business Suite. 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) information technology (IT) general and application controls.[9]

With respect to financial reporting controls, KPMG identified specific deficiencies concerning the 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.

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. The power loss incident in 2009, which directly affected production of the *Congressional Record*, brought the issue of COOP to the foreground 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 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 to take the necessary steps for enhancing its COOP posture, including planning and conducting exercises with scenarios that tested alternate production facilities and procedures for notifying essential personnel. Accomplishments

[9] 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.

during the most recent reporting period included an Executive Offices COOP exercise in February 2010. This exercise was the first involving executive leadership and some support units, and included relocation to a non-GPO facility for strategy and decision making. The primary goal of the exercise was to familiarize the necessary people 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 exercise's goals were demonstrated, areas needing improvement were identified and recommendations were made to further improve the Agency's COOP posture.

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 various Government customers. This realignment of business units was initiated to help streamline processes, strengthen customer relationships, and develop new sales opportunities. GPO should continue these efforts to enhance business development and customer service and measure their level of success to ensure a culture of continuous improvement.

Nevertheless, after almost six 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 to date to measure its accomplishments, its shortcomings, and its renewed vision for the future.

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 comprising 100 percent post-consumer waste. GPO is also printing the *Federal Register* on 100 percent post-consumer waste paper. Progress continues on other initiatives including, moving from Web offset presses to digital equipment, accelerating the re-engineering of business processes, conducting energy audits, and installing a green roof.

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, we urge an integrated approach to green acquisition. In October 2009, the President issued E.O. 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. Although not required to adhere to the Executive Order, we urge that management adopt its tenets and develop written polices 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 management to address these issues directly with officials in other legislative branch agencies.

We have included in our work plan a review of energy use at GPO to determine whether a comprehensive plan exists for implementing energy-related projects, as part of an overall plan that helps reduce emissions, energy consumption, and energy costs. We 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 conducted by an IPA firm under contract. OAI also conducts short-term inspections and assessments of GPO activities generally focusing 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 six new audit and assessment reports. Those 6 reports contained 45 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency. OAI continued its work with management to close open recommendations carried over from previous reporting periods. As of March 31, 2010, a total of 52 recommendations from previous reporting periods remain open.

B. FINANCIAL STATEMENT AUDIT

(Audit Report 10-02, Issued January 8, 2010)

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG conducted the FY 2009 audit under a multiyear contract for which OAI serves as the Contracting Officer's Technical Representative (COTR). The oversight ensures that the audit complies with Government Audit Standards. OAI also assisted with facilitating the external auditor's work as well as reviewing the work performed. In addition,

OAI provided administrative support to the KPMG auditors and coordinated the audit with GPO management. OIG oversight of KPMG, as differentiated from an audit in accordance with Government Audit Standards, was not intended to enable us to express, and accordingly we did not express, an opinion on GPO's financial statements, the effectiveness of internal controls, or compliance with laws and regulations. However, our oversight, as limited to the procedures outlined earlier, disclosed no instances in which KPMG did not comply, in all material respects, with Government Audit Standards.

KPMG 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 be material weaknesses. Those deficiencies were: (1) financial reporting controls and (2) information technology (IT) general and application controls.

With respect to financial reporting controls, KPMG identified specific deficiencies concerning the 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.

KPMG did not disclose any instances of noncompliance with certain provisions of laws, regulations, and contracts or other matters required to be reported under Government Audit Standards. KPMG made recommendations for each condition and management concurred with those recommendations and has either planned or initiated responsive corrective action.

C. AUDIT AND INSPECTION REPORTS

1. 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

The GPO FDsys program is intended to modernize the GPO information collection, processing, and dissemination capabilities it 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 ninth quarterly report, which was for the period July 1, 2009, through September 30, 2009, identifies a number of technical risks associated with FDsys configuration management and risk management activities. The report contains 11 recommendations designed to strengthen these activities. Management generally concurred with the recommendations and has either taken or proposed responsive corrective actions.

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

GPO's Compliance with the Federal Information Security Management Act

FISMA requires that each executive branch agency develop, document, and implement an agency-wide program for providing 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 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 the 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. Many of the weaknesses identified during the FY 2007 baseline assessment still exist. The OIG made a total of 21 recommendations, which, if implemented, will help further move GPO toward FISMA compliance.

3. Assessment Report 10-04 (Issued January 19, 2010)

GPO Network Vulnerability Management

Network vulnerability management is the process of identifying and protecting systems and applications that are potentially vulnerable to attack in an organization's network segment. Identifying vulnerabilities is a vital part of an information security program. Vulnerabilities present malicious users with an opportunity to gain unauthorized access to a system. There are many ways to discover vulnerabilities. For example, automated scanning tools are typically used to assess systems and applications for known vulnerabilities. In addition, patch management tools can identify systems that haven't been patched and therefore may pose vulnerabilities. Organizations often use a combination of those tools as part of an overall vulnerability management program.

GPO's Passport Printing and Production System (PPPS) is a set of common hardware and software integrated with custom printing machinery for the purpose of printing, stitching, and binding components of the U.S. passport. Public-facing servers are Web servers accessible to any computer connected to the Internet. Access is commonly achieved through a client program known as a Web browser. Web servers allow people to submit and query information in a common graphic user interface. Public-facing

servers at GPO include GPO Access and the Federal Depository Library Program Desktop.

An OIG assessment of the GPO network vulnerability management program focused specifically on GPO's passport production system environment and public-facing servers. The overall objective of the assessment was to determine whether GPO maintains a robust and effective vulnerability management program that can identify and circumvent common internal and external network threats in those environments. To accomplish our objectives, we observed and evaluated GPO's network scanning policies and process, analyzed the implementation of production firewalls and routers, reviewed the effectiveness of software configuration and patch management processes, and followed up on outstanding recommendations from previous network vulnerability assessments conducted by the OIG.

The OIG issued a sensitive report detailing that the Agency implemented a robust and effective vulnerability management program that does identify and circumvent common internal and external network threats related to both the PPPS and public-facing servers. We also concluded that since our last assessment the program has been significantly strengthened.

4. 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

The tenth quarterly report identified 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. The report contains six recommendations designed to mitigate risks and strengthen overall management of the FDsys program. 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. These 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. The unresolved recommendations will be followed up on during the next reporting period.

5. Audit Report 10-06 (Issued March 31, 2010)

Security of GPO's e-Passport Supply Chain

GPO is the sole source for producing U.S. passports for the U.S. Department of State. In FY 2007, GPO printed its last legacy passport and began producing only e-Passports to respond to Department of State requirements that passports be compliant with the International Civil Aviation Organization's (ICAO) standards for international passports. ICAO decided in favor of using contactless chip technology in passports that could be inserted into the passport covers to enable the storing of biometric and other information about the passport holder. In FY 2008, the Agency produced 23.6 million e-Passports.

The e-Passport book GPO produces contains more than 60 commercially available and uniquely assembled materials. Those materials include items such as cover stock, security paper, security inks, security threads, and security functions, both covert and overt. Suppliers of those materials are located throughout the United States and in several foreign countries. SID selects suppliers and materials in collaboration with the Department of State. The Department of State also collaborates with SID to perform security assessments of both the suppliers of computer chips for the e-Passport as well as for the subcontractor responsible for inserting the chips into the passport covers. SID is solely responsible for vetting and performing security assessments of the remaining companies that supply e-Passport components.

The OIG conducted an audit that assessed the adequacy of GPO's security over its e-Passport

components and supply chain. The audit identified that the e-Passport supply chain security process was largely informal and that different GPO offices with overlapping e-Passport security responsibilities, such as SID, Acquisitions, Operations Support, Plant Operations, and Security Services, were working autonomously and had not coordinated their efforts. GPO should ensure continued security of the e-Passport supply chain by establishing a formal security oversight process.

In particular, because of this informal supply chain security process, the audit identified the following for the 16 suppliers of either significant components or operations in the e-Passport supply chain: (1) GPO had a total of 16 security assessment reports on only 11 of the 16 suppliers, (2) GPO did not have a direct contractual relationship with 6 of the 16 suppliers, (3) of the 10 e-Passport supplier contracts reviewed, 6 contracts did not contain security plans or security-related requirements, including contracts with a high-risk supplier and several overseas suppliers, and (4) GPO contract files lacked required documentation for 5 of the 10 e-Passport supplier contracts reviewed and did not contain evidence that GPO properly vetted the suppliers to ensure that they could meet GPO requirements in the most secure and economical manner. The audit also identified that GPO could strengthen the security process for storing some finished blank e-Passports and supplies, including the passport book covers containing the inlayed computer chips.

Recommendations were made to GPO management to help further improve the security of the e-Passport supply chain. GPO management concurred with each of the recommendations and has either already implemented or planned responsive corrective actions.

D. STATUS OF OPEN RECOMMENDATIONS

Management officials made progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. For the 52 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

Two recommendations made in this report remain open. The OIG reviewed the status of these recommendations as part of the most recent Network Vulnerability Assessment completed in January 2010.

The assessment identified that implementation of corrective actions is still ongoing.

2. Assessment Report 07-09 (Issued September 27, 2007)

Report on GPO's Compliance with the Federal Information Security Management Act (FISMA)

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 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. The OIG issued a sensitive report concluding that although the Agency has taken steps to comply with FISMA, additional progress is needed to fully comply.

RECOMMENDATION

The report contains 11 recommendations that if implemented will help move GPO toward FISMA compliance.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed corrective actions.

OIG COMMENTS

Management continues to work on implementing corrective actions for the seven remaining open recommendations.

3. Assessment Report 08-06 (Issued March 31, 2008)

Operating System Security for GPO's Passport Printing and Production System

FINDING

The PPPS includes various computer applications and operating systems that support production of passports. The Agency's Plant Operations Division administers PPPS computer applications while its Chief Information Officer (CIO) is responsible for administering PPPS operating systems. If those operating systems are not configured securely, critical computer applications such as databases and custom applications are vulnerable to compromise. The risk associated with compromise to the operating systems hosting such critical applications could result in services being disrupted, sensitive information being divulged, or even subject to forgery. The OIG assessed the security configuration for selected operating systems that support production of passports to determine whether GPO enforces an appropriate level of security.

RECOMMENDATION

The OIG issued a sensitive report containing eight recommendations designed not only to help strengthen security of the PPPS but also reduce the risk of system compromise.

MANAGEMENT COMMENTS

Management generally concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

One recommendation remains open.

4. Audit Report 08-10 (Issued September 11, 2008)

Diversity Management Programs at GPO

FINDING

The OIG audited diversity management programs at GPO in response to a request from the Chairman of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, of the House of Representatives' Committee on Oversight and Government Reform. The audit identified that although not mandated to comply with the guidelines and directives of the Equal Employment Opportunity Commission (EEOC) concerning model affirmative action programs, before the audit was conducted senior officials at GPO began adopting some elements of both EEOC Management Directive-715 (MD-715) and the leading diversity management practices GAO identified. The audit also showed that opportunities exist for GPO to develop a more diverse population of qualified women and minorities in top leadership positions.

RECOMMENDATION

The OIG made two recommendations in the report: (1) incorporate the remaining essential elements of MD-715, and (2) implement the nine leading practices for diversity management GAO identified. Such modifications should help the Agency manage its workforce, create an environment that helps diminish barriers for protected groups, and help attract and retain capable employees from diverse backgrounds.

MANAGEMENT COMMENTS

Management concurred with each recommendation and stated that implementation would require the Public Printer's review and approval.

OIG COMMENTS

Two recommendations remain open. Management continues with implementation of the remaining essential elements of MD-715 and the leading diversity management practices GAO identified.

5. 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 requirement, 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.

6. 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

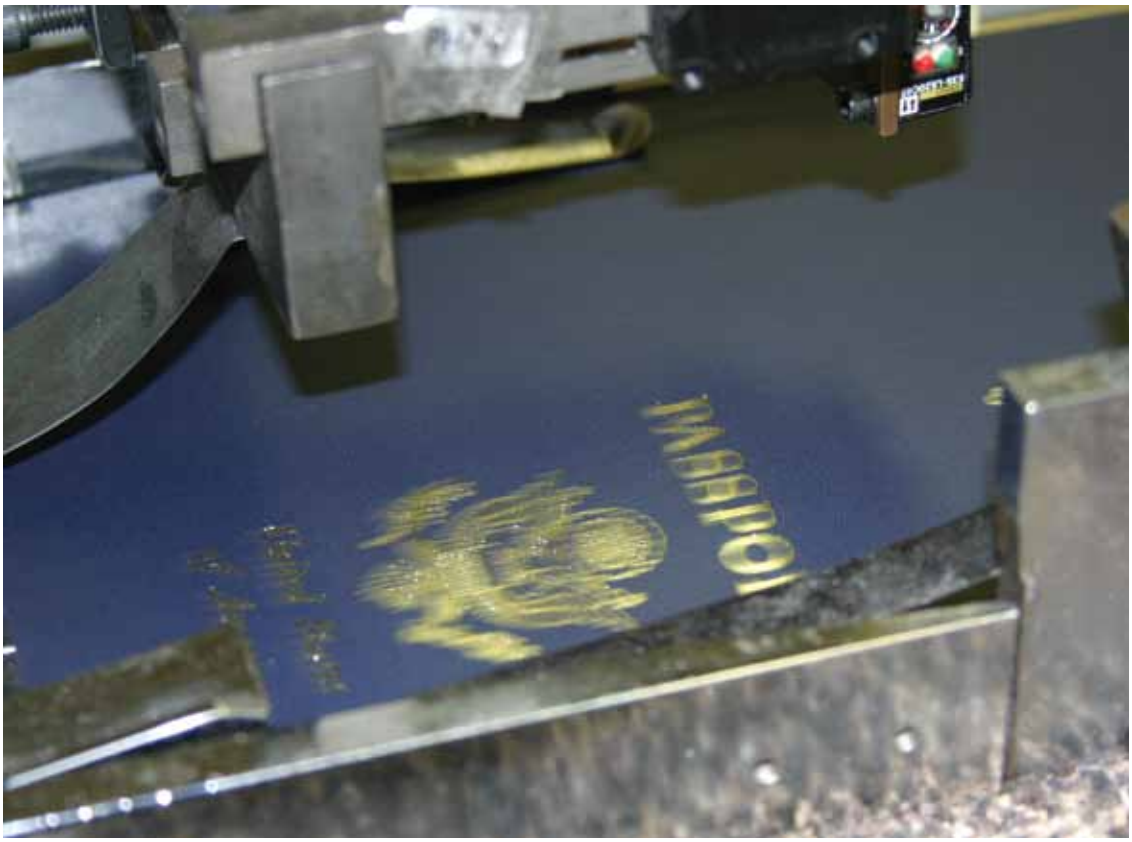
The OIG made five recommendations to management intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

Three recommendations remain open. Management continues to work on implementing corrective actions for these three remaining open recommendations.



7. Audit Report 09-02 (Issued December 22, 2008)

Audit of GPO's Passport Printing Costs

FINDING

GPO is the sole source for producing, storing, and delivering blank U.S. passport books (passports) for the Department of State. During the first 8 months of FY 2008, GPO produced 18.6 million passports and realized revenue from passport sales of more than $275 million, including $71.5 million in net income. The OIG identified two specific areas where GPO can improve the accountability and transparency of its passport costing process to better prepare the Agency for any future audits or reviews by outside entities and promote good customer relations with the Department of State. First, through the May 2008 audit time period, we found that GPO generated more than $43 million in excess cash from passport sales to the Department of State beyond what was necessary to recover costs and provide for mutually agreed upon future capital expansion. That condition occurred because GPO did not revise its original passport pricing structure and did not reach final agreement with the Department of State on a capital investment plan to earmark the excess cash. We also found that GPO, at its discretion, changed its indirect overhead cost allocation methodology for passport costs without documenting the justification and analysis for the change. As a result, the Agency increased the amount of indirect overhead allocated to passport costs from 5.65 percent, or $4 million, in FY 2007, to 52 percent, or $40 million, through May 2008.

RECOMMENDATION

The OIG made five recommendations to management to help GPO improve the accountability and transparency of its passport costing process.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions

OIG COMMENTS

One recommendation remains open. Management is in the process of revising indirect cost rates. We anticipate closure of this recommendation upon implementation of the revised rates.

8. 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. While we disagreed with management's position on the remaining four recommendations, we accepted management's proposed alternative corrective actions.

OIG COMMENTS

Four recommendations remain open. Management continues to take responsive actions to implement the four recommendations.

9. Assessment Report 09-04 (Issued December 24, 2008)

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Security Analysis Report

FINDING

This report provides an overview of key risks and issues identified by the FDsys IV&V team as a result of their review of the revised FDsys system security plan. The IV&V team concluded that the revised system security plan was a greatly improved document reflecting a positive effort to include relevant

security controls. However, the IV&V team concluded that the revised systems security plan did not adequately detail the security controls in place, or those planned to be in place for the protection of confidentiality, integrity, and availability of the systems data and associated resources.

RECOMMENDATION

The OIG made five recommendations intended to strengthen FDsys system security planning and implementation.

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 recommendations.

10. 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 recommendations.

11. 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 23 recommendations remain open. The OIG and IV&V team continue to monitor the status of their implementation.

12. Audit Report 09-13 (Issued September 30, 2009)

Accounts Payable Service Billings

FINDING

The OIG conducted an audit that evaluated GPO's processes and procedures for invoice payment. The audit found that controls over accounts payable, including the processes and procedures for tracking vendor invoices from receipt through payment, can be further strengthened and more consistently followed. In addition, complete audit trails supporting transactions in the Agency's accounts payable

Table of Open Recommendations

AUDIT	NUMBER OF OPEN RECOMMENDATIONS	NUMBER OF MONTHS OPEN
06-02 GPO Network Vulnerability Assessment	2	48
07-09 GPO's Compliance with the Federal Information Security Management Act	7	30
08-06 Operating System Security for GPO's Passport Printing and Production System	1	24
08-10 Diversity Management Programs at GPO	2	18
08-12 Assessment of GPO's Transition Planning for Internet Protocol Version 6 (IPv6)	1	18
09-01 Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability	3	16
09-02 GPO's Passport Printing Costs	1	15
09-03 FDsys IV&V – Fifth Quarter Report on Risk Management, Issues, and Traceability	4	15
09-04 FDsys IV&V – Security Analysis Report	3	15
09-07 FDsys IV&V – Sixth Quarter Report on Risk Management, Issues, and Traceability	3	15
09-12 Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Seventh Quarter Report on Risk Management, Issues, and Traceability	23	6
09-13 Accounts Payable Service Billings	1	6
09-14 GPO Workers' Compensation Program	1	6
Total	52	

systems did not always exist. Specific weaknesses identified during transaction testing included missing end-user approvals, missing support for Contracting Officer payment authorization, no evidence of invoice examination and certification, and hard copy invoice data that could not be reconciled to the accounts payable system. As a result, there was no assurance that management controls were operating effectively, which could have resulted in a potential misstatement of monthly and annual financial information.

RECOMMENDATION

The OIG made two recommendations to GPO management to help improve controls over accounts payable service billings, and specifically, GPO's processes and procedures for invoice payment.

MANAGEMENT COMMENTS

GPO Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

One recommendation remains open. Management is in the process of completing standard operating procedures for receiving, processing, and disbursing vendor invoices for payment. The recommendation should be completed and closed during the next reporting period.

13. Audit Report 09-14 (Issued September 30, 2009)

GPO Workers' Compensation Program

FINDING

The OIG completed an audit of GPO's Workers' Compensation Program to determine whether GPO's program was complying with appropriate Federal guidelines, regulations, and directives related to worker's compensation, and GPO employee claims for worker's compensation are supported by required documentation. The audit identified that GPO's OWC should be commended for improvements in both the organization and management of this program. Since a previous OIG audit in 2002, controls over the GPO Workers' Compensation Program have been strengthened and the program has undergone significant changes. The audit found that the overall amount of billings from the Department of Labor for the cost of workers' compensation benefits paid on GPO's behalf decreased to less than $6 million during FY 2007. In addition, the total number of GPO workers' compensation claimants decreased from 193 in 2002 to 136 in 2008. The audit identified several areas where procedural and policy improvements could be made to further enhance and strengthen the Workers' Compensation Program.

RECOMMENDATION

The OIG made two recommendations to management designed to ensure that the program continues to be operated in an efficient and effective manner.

MANAGEMENT COMMENTS

Management generally concurred with the recommendations and agreed to take responsive corrective actions or alternative actions to address the issues identified.

OIG COMMENTS

One recommendation remains open. The recommendation should be closed during the next 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. Special Agents in OI are Federal Criminal Investigators (general schedule job series 1811) and are designated as Special Police Officers. 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 identify issues uncovered during an investigation it believes warrant management's prompt attention.

OI is responsible for investigations at all GPO locations, including the 15 GPO Regional Printing Procurement Offices (RPPOs) nationwide. OI also maintains a continuing liaison with the GPO Security Services and Uniform Police Branch, to coordinate efforts impacting these law enforcement programs. Liaison is also maintained with the Department of Justice, the National Procurement Fraud Task Force, and other investigative agencies and organizations.

A. SUMMARY OF INVESTIGATIVE ACTIVITY

At the end of last reporting period, 24 complaints were open. OI opened 26 new complaint files this period, 11 complaints were converted to full investigations, and 8 were closed after preliminary review with no action. Additionally, eight complaints were referred to GPO management and one to another agency. At the end of the reporting period, 22 complaints were open.

At the end of the last reporting period, 38 investigations were open. During this reporting period, 15 investigations were closed, 7 of which resulted in referrals to GPO management for potential

administrative action. Ongoing at the end of this reporting period are 33 investigations.

During this reporting period, we made seven presentations to the Department of Justice for potential criminal prosecutions. Each of those presentations resulted in declinations, and those cases will now be pursued civilly and/or administratively. No formal presentations were made for civil purposes during this reporting period.

Multiple investigations are being conducted in coordination with the Department of Justice, including its Antitrust Division. Twelve 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 seeks to uncover any wrongdoing by GPO contractors or employees during administration of GPO contracts. Violations can include false statements, false claims, kickbacks, product substitution, collusive bidding, bribery, and financial conflicts of interest. In FY 2009, GPO procured over $675 million in goods and services. With such vulnerability in mind, OI has focused much investigative development to the area of procurement fraud. The inventory of procurement fraud complaints/investigations has increased to 23 open procurement fraud investigations today, or 64 percent of our active caseload. Including allegations in complaint status, OI has 31 open procurement matters.

Workers' Compensation Fraud

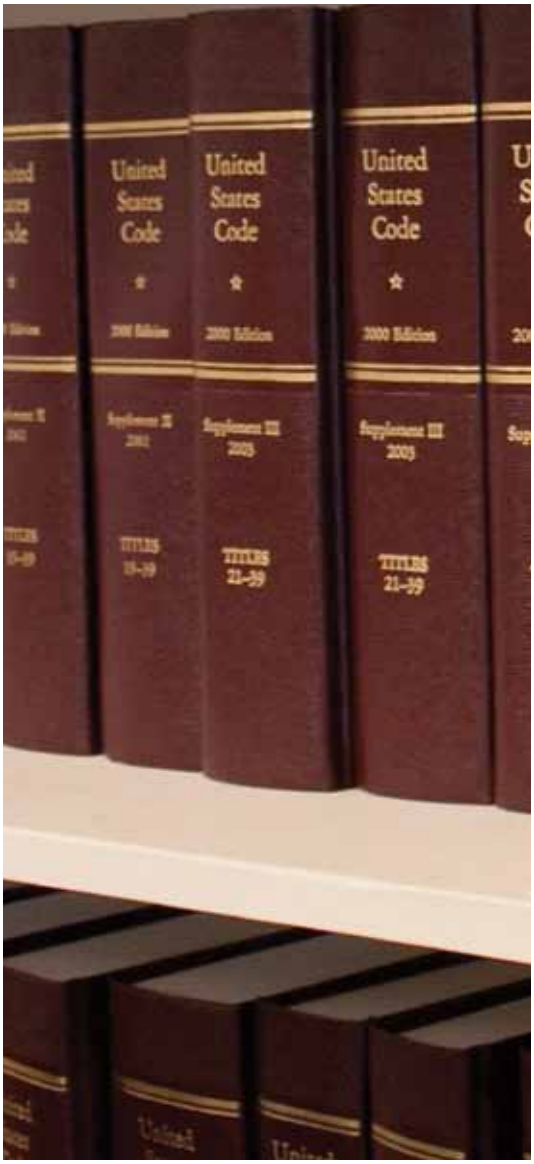
OI investigates GPO employees who allegedly submit false claims or make false statements to receive workers' compensation benefits. We are working on five investigative matters (complaints and investigations) involving possible fraudulent claims for workers' compensation.

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 five 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 theft of Government property, illegal hacking, or requests for investigations by other legislative agencies. OI has two open investigative matters involving these types of allegations.



C. SUMMARY OF INVESTIGATIVE ACCOMPLISHMENTS

Criminal and Civil Cases

- An OI investigation found evidence of a GPO printing contractor who failed to comply with critical contract specifications throughout the performance period. 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 contractor submitted at least 10 invoices to GPO. GPO suspended and proposed debarment of the company and the company's officers from doing business with GPO as a contractor, subcontractor, or contractor's representative. We previously reported that this matter was accepted for action by the Department of Justice and a Civil Demand Letter was issued to the contractor. Negotiations toward civil settlement continue.
- OI is conducting an investigation into allegations of false statements, false claims, forgery, and/or bid collusion by GPO print vendors. OI has the assistance of the Department of Justice Antitrust Division, which is evaluating the case for possible criminal and/or civil action.
- OI continues an investigation of allegations relating to false statements and/or false claims to GPO. OI is coordinating this investigation with the Department of Justice Antitrust Division. The Department of Justice continues to evaluate this case for possible criminal and/or civil action.
- Investigation of a printing contractor determined GPO paid more than $175,000 after the company submitted delivery receipts and invoiced for payment, but failed to perform according to specifications and did not deliver all products. Though the Department of Justice declined criminal prosecution, the investigation continues toward possible civil and administrative resolution.
- We previously reported that an OI investigation of over-billing by a GPO print contractor was accepted for potential civil action by the Department of Justice. Investigation determined that from February 2002 until February 2004 the company President

over billed GPO approximately $499,000. Settlement discussions continue.

Internal Administrative Cases

- 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 Department of Justice Public Integrity Section included numerous interviews, records reviews, and analysis by an independent subject matter expert. The Department of Justice declined prosecution and the investigative results were referred to management. Management proposed terminating the employee. Further details will be reported when final action takes place.
- OI investigated disposition of 18 laptop/portable computers identified as missing from an IT&S storage area at the GPO headquarters building. OI reported to management that as a result of the lack of security and inventory controls in IT&S, in conjunction with general disregard for property management controls outlined in GPO Directive 810.11B, OI was unable to determine the final disposition of 18 missing laptops. The findings of the investigation were referred to OAI, which initiated an audit of IT&S property management protocols. Specific recommendations will be outlined as part of the final audit report.
- An OI investigation disclosed evidence that GPO employees failed to provide truthful information during an administrative investigation conducted by the

GPO HC Office. The Department of Justice declined the matter for prosecution and the OI referred it to management for action. During this period, at the request of GPO Office of General Counsel (OGC), OI agents sought affidavits from witnesses, confirming written reports of their earlier verbal statements. We previously reported that GPO issued notices of intent to terminate from employment four employees and placed them on administrative leave. Three of the employees retired after receiving notice of termination and the fourth received a 30-day suspension and demotion. Further details will be reported when all actions are finalized.

- The Uniform Police Branch referred allegations of a possible physical assault of a GPO contractor by a GPO employee and provided video surveillance footage of the alleged incident. OI reviewed the video and interviewed those involved. The facts of the case were presented to the Department of Justice and declined for criminal prosecution. We recently referred the report of investigation to management for consideration of administrative action and additional employee training in zero violence, EEO, and harassment.
- An investigation was initiated after OI learned a former GPO employee used an official Government travel card to make inappropriate purchases. Investigation determined the former employee, who made no official trips, owed Citibank approximately $4,989 for purchases at retail stores such as Marshalls, Macys, Target, and Walmart. The former employee was able to make these purchases because automatic and appropriate travel card purchasing limitations were not in place. Because the government is not liable for the former employee's non-payment and debt collection options are still available, this matter was not referred to the Department of Justice. The results of this investigation were referred to the GPO management for appropriate action. GPO

now has appropriate purchasing limitations in place for all GPO travel cards.

- OI investigated allegations of a GPO employee on workers' compensation alleged to have provided landscaping services without declaring the income as required by the Department of Labor's Office of Workers' Compensation Programs. Although our investigation determined the employee was mowing lawns for a fee, we could not determine the specific time frames of when these services were provided or how much money was earned. As a result, neither the Department of Labor nor the Department of Justice pursued recovery action against the individual. Our report of investigation was referred to the Department of Labor and the Chief, Workers' Compensation Services for GPO. The Department of Labor indicated they intend to request a second opinion medical evaluation to determine if the initial injury is still active.
- OI received allegations that an employee was using GPO equipment to copy and sell digital video discs (DVDs) during work hours. The employee admitted that for approximately the last 3 years he has sold from 75 to 100 illegally copied movies for about $5 per copy to GPO employees but denied using GPO equipment to make copies of the movies. We found no evidence to support the allegation he was using GPO equipment to make illegal copies of movies. The Department of Justice declined criminal prosecution and the OI referred to management for action. Though action is not final, a 3-day suspension was proposed.
- OI investigated allegations that a GPO employee threatened a co-worker. He was suspended from employment when OI reported facts surrounding charges against him for domestic violence. Further investigation by OI revealed other instances of misconduct. Interviews revealed that since at least 2006, the employee engaged in threatening and unprofessional conduct both with his supervisors and co-workers. Results of OI's investigation were forwarded in support of agency proposed action. The employee resigned while on indefinite suspension.
- OI assisted OPM by conducting interviews of GPO

HC Office personnel during a recent OPM evaluation of GPO's competitive examining authority exercised under a delegation agreement with OPM. OPM presented findings to management and representatives of the OIG. A written report is expected.

External Administrative Cases

- Results of an OI investigation were referred to management for consideration of suspension/debarment of a printing contractor and its officers/owners. The investigation was initiated based on allegations that a GPO contractor submitted a fraudulent shipping receipt and invoice to GPO for payment. Our investigation revealed that in 2008 the company shipped a product with a shortage valued at approximately $6,547, yet billed GPO the full value of $23,000. Investigation also determined the contractor may have acted as a broker and likely subcontracted part of the predominant function to another company in violation of GPO contract terms.
- An OI investigation of a GPO contractor for alleged submission of fraudulent shipping receipts and invoices resulted in the referral of investigative results to GPO management for further review and action. Investigation revealed testimony that the contractor shorted one shipment yet billed in full, substituted higher quality proofs with lower qual-

ity proofs, and attempted to invoice for overnight shipping despite their shipping the proofs through regular mail. Two contracts were subsequently modified and discounted and the third was cancelled by the customer agency for unrelated reasons. Due to the low dollar value, this matter was not referred to the Department of Justice.

- OI investigated allegations of a violation of the Buy American Act by a GPO contractor. A GPO RPPO reported the contractor shipped his product from Canada on two occasions. Research revealed the contractor had only been awarded two small contracts. When contacted by OI, the contractor admitted his company had no facilities in the United States and would be ineligible for further awards. These investigative results were referred to the GPO Managing Director of Print Procurement and OGC for their information.
- OI referred information to the GPO Deputy Manager, Director of Publications and Information Sales, after an investigation determined that, between July 2006 and May 2009, a GPO customer submitted 53 checks to GPO totaling approximately $5,611 not honored by GPO's banking institution because of insufficient funds. Though employees in GPO's Publication Sales Program were instructed to screen sales orders from the subject company, checks continued to be submitted and returned. Though both civil and criminal remedies and penalties exist for passing bad checks, no referral was made to the Department of Justice for prosecution because of GPO's lack of internal controls. The results of this investigation were referred to GPO management, with suggested process improvements.

D. OTHER SIGNIFICANT ACTIVITIES

While OI investigative resources were primarily deployed in response to reported reactive matters represented above, we continue other aggressive efforts to improve our abilities to detect, prevent, and investigate the loss of Government assets. The following summarizes other significant activities occurring in OI:

- During this reporting period, the IG and his executive staff, including managers of OI, held productive meetings with the GPO Acquisitions Services. At the invitation of the Director of Acquisitions Services, OI provided a Procurement Fraud Presentation to staff members.
- Future activities are planned with Acquisitions Services, including a more detailed question and answer session concerning detection of fraud. A joint quality assurance field visit for purposes of OI training is also anticipated.
- OI attended the Print Procurement Managers' meeting, with contracting supervisors from headquarters and RPPOs, and responded to questions concerning reporting fraud allegations to the OIG.
- OI monitored GPO's significant progress toward implementation of OI MIR recommendations relating to GPO contractors and security of PII and the Publication of House Document 111-37 on U.S. Nuclear Sites.
- OI and OAI continue to strategize concerning possible proactive initiatives for detecting fraud within GPO. One such future initiative may involve recurring allegations of product substitution on GPO contracts, particularly in the area of paper specifications.
- Two OI criminal investigators have elected to seek their designations as Certified Fraud Examiners.

APPENDIX

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
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CPS	Certification Practices Statement
COA	Continuity of Access
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
DHS/CPB	Department of Homeland Security/ Customs and Border Patrol
FDsys	Federal Digital System
EEOC	Equal Employment Opportunity Commission
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GBIS	GPO's Business Information System
GPO	U.S. Government Printing Office
HSPD-12	Homeland Security Presidential Directive-12
ICAO	International Civil Aviation Organization
IG	Inspector General
IPA	Independent Public Accountant
IPv6	Internet Protocol version 6
IT	Information Technology
IT&S	Information Technology and Systems
IV&V	Independent Verification and Validation
MIR	Management Implication Report
OA	Organization Architects
OALC	Office of Administration/Legal Counsel
OAI	Office of Audits and Inspections
OGC	Office of General Counsel
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OWC	Office of Workers' Compensation
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PO	Privacy Officer
PPPS	Passport Printing and Production System
PTR	Problem Tracking Report
PURL	Persistent Uniform Resource Locator
RPPO	Regional Printing Procurement Office
SAS	Statement on Auditing Standards
SCC	Secure Credential Center
SID	Security and Intelligent Documents
SPF	Secure Production Facility
SSP	Shared Service Provider
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	21–32
Section 5(a)(2)	Recommendations for Corrective Actions	21–25
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	25–32
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	35–38
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)	21–25
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	43
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	44
Section 5(a)(10)	Summary of prior Audit and Inspection Reports issued for which no management decision has been made	n/a
Section 5(a)(11)	Description and explanation of significant revised management decision	n/a
Section 5(a)(12)	Significant management decision with which the IG is in disagreement	n/a

APPENDIX C

Statistical Reports

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

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

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

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

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

REPORTS	FUNDS PUT TO BETTER USE
Report on Federal Digital System (Fdsys) Independent Verification and Validation – Ninth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-01, issued December 2, 2009)	$0
Report on the Consolidated Financial Statement Audit of the GPO for the FYs Ended September 30, 2009 and 2008 (Audit Report 10-02, issued January 8, 2010)	$0
Report on GPO's Compliance with the Federal Information Security Management Act (Assessment Report 10-03, issued January 12, 2010)	$0
Report on Assessment of GPO Network Vulnerability Management (Assessment Report 10-04, issued January 19, 2010)	$0
Report on Federal Digital System (Fdsys) Independent Verification and Validation – Tenth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 10-05, issued March 24, 2010)	$0
Report on Audit of Security of GPO's e-Passport Supply Chain (Audit Report 10-06, issued March 31, 2010)	$0
Total	$0

Table C-4: Investigations Case Summary

Total New Hotline/Other Allegations Received during Reporting Period	42
No Formal Investigative Action Required	14
Investigations Opened by OI during Reporting Period	10
Investigations Open at Beginning of Reporting Period	38
Investigations Closed during Reporting Period	15
Investigations Open at End of Reporting Period	33
Referrals to GPO Management	15
Referrals to Other Agencies	5
Referrals to OAI	0

Current Open Investigations by Allegation	33	
Procurement Fraud	21	64%
Employee Misconduct	7	21%
Workers' Compensation Fraud	3	9%
Other Investigations	2	6%

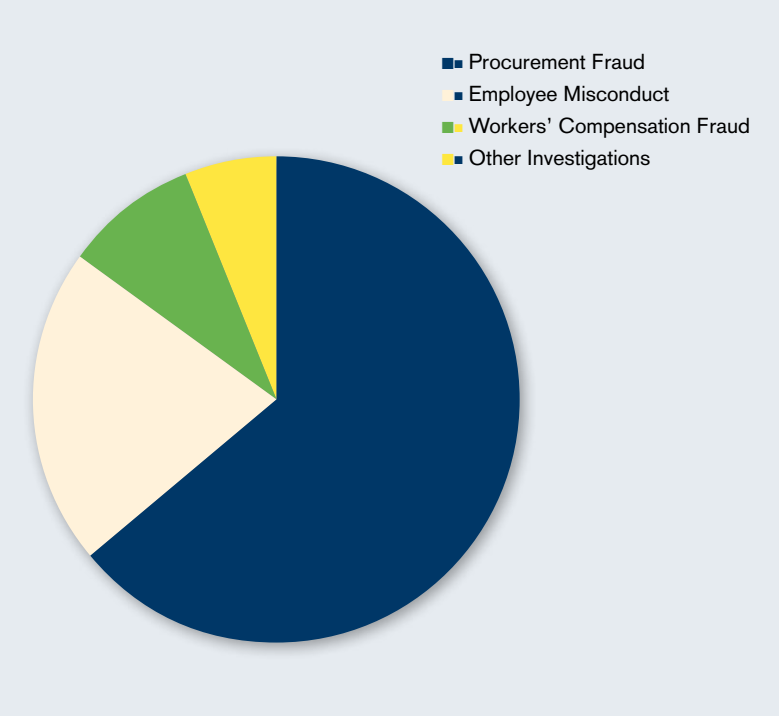


Table C-5: Investigations Productivity Summary

Arrests	0
Total Presentations to Prosecuting Authorities	7
Criminal Acceptances	0
Criminal Declinations	7
Indictments	0
Convictions	0
Guilty Pleas	0
Probation (months)	0
Jail Time (days)	0
Restitutions	0
Civil Acceptances	0
Civil Demand Letters	0
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	0
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	15
Contractor Debarments (Referral)	1
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions (1 Proposed)	2
Employee Terminations (Proposed)	1
Employee Other Actions (resignations)	3
Other Law Enforcement Agency Referrals	4
Inspector General Subpoenas	12

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