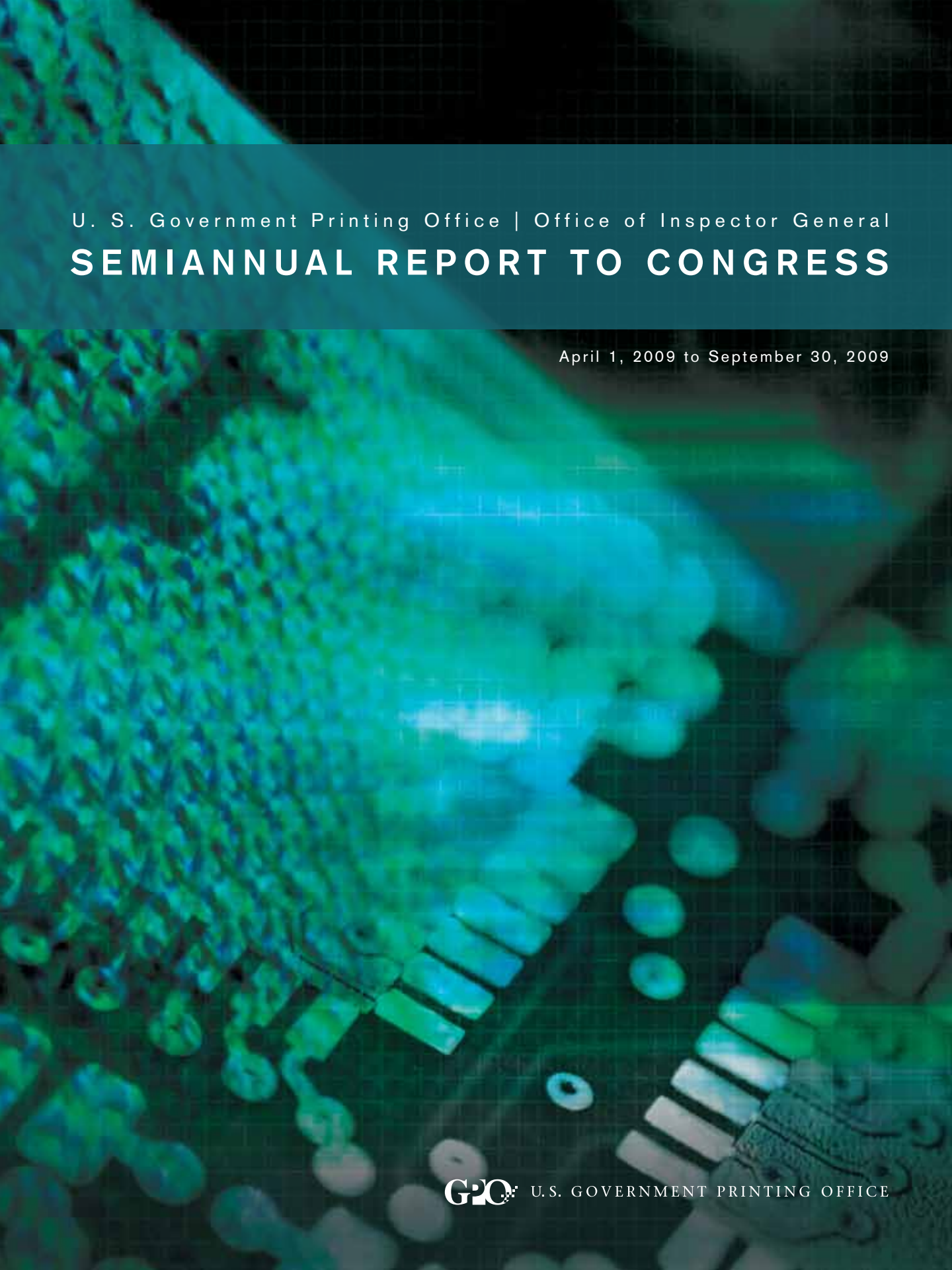


U. S. Government Printing Office | Office of Inspector General

SEMIANNUAL REPORT TO CONGRESS

April 1, 2009 to September 30, 2009

GPO 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 these responsibilities, the OIG conducts audits, assessments, investigations, inspections, and other reviews.

CONTENTS

MESSAGE FROM THE INSPECTOR GENERAL

For an Agency in transition, the words of its founding father could not be more appropriate. In order to adhere to its maxim, *Keeping America Informed*, GPO must continue to grow and progress in order to achieve success. Change is not only inevitable – it is, and will continue to be, a standard operating principle for the future. This is true for the Agency and the OIG as well. Our charge will be to adapt and meet the evolving demands of the Agency as it moves forward with its transformation and to strive for continuous improvement in our operations. And, consonant with *our* responsibility to keep America informed, the OIG must continue to adhere to the tenets of accountability and transparency.

During this reporting period, our Office of Audits and Inspections continued its oversight activities of several significant and critical GPO programs—the implementation of the Federal Digital System (FDsys), e-Passport printing and production system, and GPO's Public Key Infrastructure. In addition, we issued audit reports on accounts payable service billings and GPO's Workers' Compensation Program. The reports' recommendations and management's adoption thereof will aid the Agency's growth and progress so it may strengthen program management, improve security planning, and successfully deploy vital Agency programs.

Without continual growth and progress, such words as improvement, achievement, and success have no meaning.

—Benjamin Franklin

The Office of Investigations has undergone formidable growth during this reporting period. As I noted in the last Semiannual Report, the Office of Investigations was shifting its focus to address procurement and financial fraud vulnerability. At that time, 38% of open cases were in the area of procurement fraud. Now, the number is 61%. Indeed, the number of procurement fraud cases has increased more than 200% (from 7 to 23) since this time last year. This success is borne out of unrelenting dedication to growth and progress.

In addition to these efforts, the quick action of the Office of Investigations uncovered no wrongdoing related to the Agency's posting to the Internet of a sensitive document that received national media attention. However, this report also made recommendations to the Agency to help protect against unwanted disclosure of sensitive information in the future. Finally, an investigation disclosing evidence of false statements by four GPO employees resulted in notices by the Agency of its intent to terminate their employment.

In this report, we update the Agency's significant management challenges and note that the Agency has addressed several challenges in the area of sustainable environmental stewardship and made considerable progress in its emergency and continuity of operations planning. However, we also note that the Agency has still not implemented policies and procedures to protect sensitive information, including personally identifiable information (PII). Additionally, we spotlight ongoing challenges in the Human Capital arena–challenges that present opportunities for growth and progress that, with commitment by GPO senior management, should lead to significant operational improvement.

A final note, it continues to be a privilege to work with steadfast professionals who strive for excellence, accuracy, and integrity in service to the vision, mission, and goals of the OIG.

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

During this reporting period, the OIG continued directing its resources toward those areas of greatest risk within GPO. We provided a variety of services, including program and financial audits, inspections and assessments of key operations, and investigative activity resulting in criminal or administrative actions. We also consulted on a variety of Agency issues and the Inspector General provided comments on proposed legislation on issues affecting the Inspector General community as Chairman of the Legislation Committee of the Council of Inspectors General on Integrity and Efficiency. The work of each of the OIG components during this reporting period is summarized below.

The Office of Audits and Inspections (OAI) issued six new audit and assessment reports. Those six reports contained 37 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. OAI continued to oversee the Independent Verification and Validation (IV&V) efforts related to the implementation of the Federal Digital System (FDsys), the annual audit of GPO's financial statements and the assessment of GPO's Public Key Infrastructure (PKI) services.

Among OAI's significant accomplishments during this reporting period:

- issued the results of an audit of GPO's Passport Printing and Production System (PPPS) to evaluate security configurations for the key Oracle databases supporting production of ePassports and determine whether GPO was enforcing an appropriate level of security. The OIG issued a sensitive report containing recommendations intended to further strengthen PPPS security and reduce the risk of system compromise;
- issued the results of reviews conducted under contract by an Independent Public Accountant (IPA) on GPO's Public Key Infrastructure (PKI) services. GPO's PKI ensures the highest level of protection for electronic information that travels over ordinary, nonsecure networks. The IPA's attestation reports found that GPO PKI Certification Practices are in conformity to the Federal Common Policy Framework and the GPO Certification Policy and that GPO management's assertions over the controls of its Certification Authority are fairly stated;
- issued a seventh quarterly report on IV&V of GPO's FDsys and made recommendations designed to strengthen FDsys program management, particularly for future FDsys releases.

- issued an audit concerning GPO's processes and procedures of invoice payment finding that controls over accounts payable can be strengthened and more consistently followed; and
- issued the results of an audit of GPO's Workers' Compensation Program finding that GPO's Office of Workers' Compensation had made significant changes and implemented many of the recommendations from a 2002 OIG audit. The changes have resulted in strengthened controls over workers' compensation claims and cases.

The Office of Investigations (OI) opened 39 complaints for preliminary investigation and 21 full investigations, closed 12 investigations, and currently has 38 ongoing investigations. Twenty-three complaints were closed to investigations and 24 complaints remained open at the end of this period. Six complaints were referred to GPO management or other agencies, while nine were closed with no action. Nine investigations resulted in referrals to GPO management for potential administrative action.

Of the open complaints and investigations, 35 involve allegations of procurement fraud, demonstrating OI's increased efforts to address procurement and financial fraud vulnerability within GPO. This significant increase in procurement fraud cases is partly the result of OI's proactive efforts to engage and educate GPO management, particularly by providing procurement fraud presentations to staff of the 15 GPO Regional Printing Procurement Offices and procurement officials throughout GPO during FY2009.

Several ongoing investigations are being conducted in coordination with the Department of Justice, including its Antitrust and Public Integrity Divisions. As part of these investigations, the Inspector General (IG) issued twenty subpoenas for documents and the OI conducted two consent searches on separate employee misconduct cases.

Among OI's significant accomplishments during this reporting period:

- issued a Management Implication Report (MIR) communicating the findings of an investigation of GPO's publication and Internet posting of House Document 111-37 (HD 111-37). HD 111-37 contains a 266-page list of U.S. civilian nuclear sites, locations, facilities, and activities declared to the International Atomic Energy Agency (IAEA) by the President of the United States. While our investigation found no wrongdoing on the part of GPO or its employees, our MIR recommended additional controls that may help identify and prevent an unwanted disclosure of sensitive information in the future;
- issued a recommendation to GPO management to suspend a GPO vendor and its officers from doing business with GPO for lack of business integrity and responsibility based on an investigation into false statements and claims by the company. GPO has suspended the company pending proposed debarment;
- issued a Report of Investigation that disclosed evidence that several employees made false statements during the conduct of their employment. GPO issued notices to four employees of its intent to terminate their employment and placed them on administrative leave pending the resolution of the personnel actions; and
- issued a Report of Investigation concerning alleged overtime fraud by a GPO employee. Although there was insufficient evidence to support the allegations, the Report detailed weaknesses in controls that govern overtime authorization and approval for certain GPO employees and made recommendations for improving internal controls.

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 also reviews and edits all audit, inspection, and investigative reports prior to approval by the IG.

During this reporting period, OALC hired a new law clerk to provide support to the OIG and to accomplish several legal research tasks.

Among the OALC accomplishments during this reporting period:

- reviewed, edited, and approved twenty subpoenas;
- oversaw the successful remodel of the OIG office to better accommodate the security needs of the OI and space for contractors;
- completed the upgrade of laptop computers equipped with encryption software for staff;
- developed an internal policy to protect personally identifiable information;
- revamped the "brand" look of the OIG in written products and communications;
- completed two congressional requests for information;
- provided support to the IG in his capacity as Chairman of the Legislation Committee of the Council of Inspectors General on Integrity and Efficiency. In this capacity, OALC helped the IG provide comments to several congressional committees on pending legislation affecting the IG community;
- coordinated and supervised the successful launch of an informational Web site for the Council of Counsels to the Inspector General, designed and supported by GPO's Digital Media Services; and
- 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, OIG senior managers participated in a retreat to strengthen the leadership team and develop strategies to improve OIG operations and measure performance. One particular area of discussion was the development of collaborative efforts between OAI and OI in such areas as procurement and data mining to effectively uncover indicators and specific instances of fraud. In addition, senior managers have committed to update the OIG strategic plan by the end of calendar year 2009 and to conduct an office-wide retreat soon thereafter to discuss its implementation.

Personnel Update

During this period, the OIG welcomed one new employee and a law clerk to its staff. In July, Kenyon Dugan joined OI as a Senior Special Agent. Kenyon came to the OIG from New York City, where he worked as a Special Agent with the Internal Revenue Service, Criminal Investigations Division. Kenyon holds degrees in Accounting and Taxation. Prior to becoming a Special Agent for IRS, he held progressively responsible positions in accounting and auditing both in the private sector and for the City of Philadelphia. OI is now fully staffed with five Special Agents, a Special Agent-in-Charge, and an Assistant Inspector General for Investigations.

In May, Rachel Aksman joined the OALC as its new law clerk. Rachel is a graduate of the University of Virginia and is currently a third-year law student at the George Mason University Law School. Before joining the OIG, Rachel worked as a law clerk for Smolen Plevy, a law firm in Vienna, Virginia.

COUNCIL OF INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

On October 14, 2008, the Inspector General Reform Act of 2008, Public Law 110-409, established the Council of Inspectors General on Integrity and Efficiency (CIGIE). The mission of CIGIE is to address integrity, economy, and effectiveness issues that transcend individual Government agencies and 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.

To accomplish its mission, the CIGIE will identify, review, and discuss 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 GPO IG was elected to serve a two-year term as the Chairman of the CIGIE Legislation Committee. The Legislation Committee is dedicated to providing helpful and timely information about congressional initiatives to the IG community; soliciting the views and concerns of the community in response to congressional initiatives and requests; and presenting views and recommendations to congressional entities and the Office of Management and Budget (OMB) on issues and initiatives of interest.

On behalf of the CIGIE Legislation Committee, the IG provided testimony on April 21, 2009, before the Senate's Ad Hoc Subcommittee on Contracting Oversight on "Improving the Ability of Inspectors General To Detect, Prevent, And Help Prosecute Contracting Fraud." In addition, the IG wrote letters to several congressional committees on various legislative matters affecting the IG community, most significantly to:

- express support of S. 629, the Part-Time Reemployment of Annuitants Act of 2009. This legislation would provide the IG community with an extra hiring flexibility to accomplish expanded oversight responsibilities. The bill was amended to the National Defense Authorization Act and passage is expected;
- provide feedback about provisions of S. 139, the Data Breach Notification Act, that may confuse requirements under federal law and executive guidelines, specifically under the Federal Information Security Management Act (FISMA), that agencies should notify their respective IGs of any breach of PII;
- recognize the importance of whistleblower protection for Federal employees, yet express concern about S. 1507, the Whistleblower Protection Enhancement Act of 2009, which would impose strict time requirements that could interfere with IG's investigative priorities and discretion; and
- express support for IG subpoena authority to include the attendance and testimony of non-Federal agency witnesses to aid audits and investigations that may be hampered by the lack of cooperation of private contractors, grantees, and former employees.

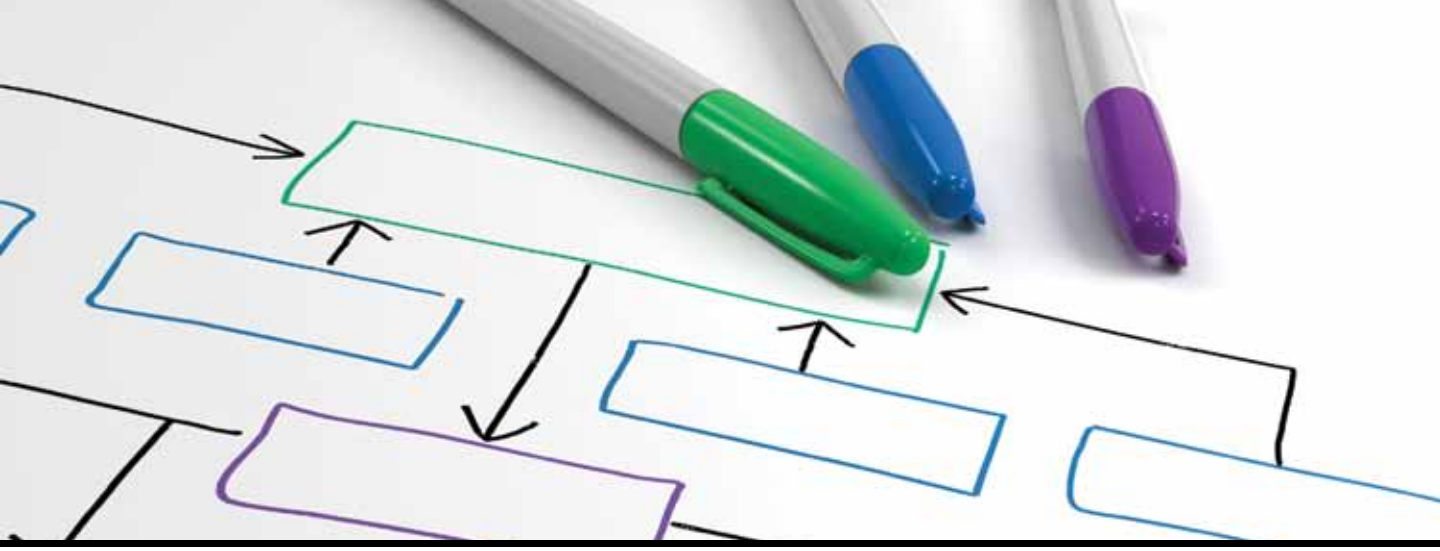
Legislative Branch IGs continued to meet quarterly in response to a Senate Appropriations Committee request that the IGs throughout the Legislative Branch communicate, cooperate, and coordinate with one another on an informal basis. During this reporting period, meetings were hosted by the House of Representatives IG and the GPO IG. Among the issues discussed and under consideration are:

- shared training opportunities for Legislative Branch OIG personnel;
- cross-cutting Legislative Branch audits and inspections to include concerns regarding agency protection of PII;
- joint efforts to improve environmental conditions and reduce costs;
- development of consistent OIG privacy protection policies; and
- 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 of GPO. It then makes recommendations in each semiannual report on the impact of such 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 will continue to play an active role in that area.

Although there were no legislative proposals relating to GPO programs and operations, the OIG has requested the GPO General Counsel provide the OIG the opportunity to review and provide comments on pending agency directives, to include a recommended directive to PII. As of the end of this reporting period, a copy of the proposed directive had not been provided to the OIG for review or comment.



GPO MANAGEMENT CHALLENGES

GPO is well into its digital platform transformation, having established several key initiatives that will help the Agency meet its mission in the ever-changing digital environment. Substantial and challenging risks that could affect successful implementation of the programs and initiatives will continue. In previous Semiannual Reports to Congress, the OIG identified 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 continue to update the Agency's management challenges as the agency moves forward in its transformational efforts.

1. Sustainable Environmental Stewardship. As the largest industrial manufacturer in the District of Columbia, the 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. The Public Printer has outlined a proactive plan of action so that GPO can become a more efficient operation that makes better use of the resources under its control. Some of the initiatives include moving from web offset presses to digital equipment, accelerating the re-engineering of business processes, conducting energy audits, using paper that goes beyond minimum requirements for recycled content, and installing a green roof.

GPO'S TOP 10 MANAGEMENT CHALLENGES

1. Sustainable Environmental Stewardship.
2. Management of Human Capital.
3. Improved Financial Management.
4. Continuity of Operations.
5. Internal Controls.
6. Security and Intelligent Documents.
7. Protection of Sensitive Information.
8. Information Technology and Systems Management.
9. Business Development and Customer Service.
10. Acquisitions.

We previously reported management's concerns that the GPO facility is too large (contains three times more space than needed), too operationally inefficient (functions are spread over four buildings and multiple floors), and too expensive to operate given its size, age, and condition. Accordingly, GPO has proposed a new facility that would more appropriately meet Agency needs and be more energy efficient. This also fits with the Agency's environmental stewardship initiative.

We noted in our last SAR that the Government Accountability Office (GAO) found that GPO "... did not conduct cost-benefit analyses that explored a full range of options for obtaining a new facility."[1] We further noted that in light of Congressional impetus to convert government facilities to "High-Performance Green Buildings," GPO should conduct a complete cost-benefit analysis to fully explore the best options for a new facility that would potentially reap economic as well as environmental benefits. While this is an aggressive goal, it is consistent with the Agency's objectives and with the environmental and economic objectives of the Congress and Obama Administration.

GAO also noted two additional issues impeding the efforts to obtain a new facility, namely GPO's lack of legislative authority to outlease property and retain and use the proceeds from an outlease and its lack of expertise in managing leases as a landlord. We urge the Agency to develop a comprehensive plan of action to address these additional impediments to this challenging but important objective.

The Public Printer has also outlined an aggressive, environmental stewardship plan for GPO. During this reporting period, GPO made significant progress in this area. Recently, GPO announced that it is now printing the *Congressional Record* on 100% recycled paper. Additionally, GPO utilized *American Recovery and Reinvestment Act* money through GSA to replace 18, or nearly half, of all GPO fleet vehicles with "green" vehicles.

We continue, however, to urge management to promote and integrate "green thinking" into all

business processes and advance through performance metrics, reward programs, and other means, a new culture of "green thinking" and sustainability initiatives throughout the Agency. For example, we still urge an integrated approach to green acquisition by incorporating "green thinking" into the entire procurement process. As with the printing of the *Congressional Record*, future stewardship initiatives will require a top to bottom and bottom to top commitment. Employee empowerment will be absolutely necessary for the Agency to achieve its goals and sustain them.

GPO's environmental executive has recommended to the OIG issues to explore with the GPO Legislative Branch counterparts. First, the consolidation of waste hauling contracts, to obtain a more favorable rate for recycled goods as well as ensure that each agency can participate in recycling efforts. Second, the consolidation of 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. And finally, the sharing of service contracts to achieve economies of scale and uniformity throughout the Legislative Branch agencies. The GPO OIG has communicated these issues to its OIG

[1] See GAO-09-329R, accessible at http://www.gao.gov/new.items/d09392r.pdf.

counterparts and urges the Agency to address these issues directly with management 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 to 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.

2. Management of Human Capital. We continue to highlight the challenges the Agency faces in "right sizing" its workforce while at the same time attracting employees with the right skill sets for the new GPO. The Chief Human Capital Officer continues to confront significant issues related to GPO workforce recruitment and development and must also advance creative solutions that will help the Agency meet its ongoing workforce needs—in part by building a diverse, qualified applicant pool.

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 showed that while GPO has voluntarily adopted several components for establishing a model Federal government diversity program, improvements can be made toward enhancing diversity of the Agency's corps of senior-level employees. We recommended that the Public Printer adopt all or a combination of the leading practices that the GAO recommends to establish a model Federal government program and GPO management agreed with our recommendation. As of this reporting period, GPO management has not provided a comprehensive plan for addressing the implementation of the recommendation.

While we have previously reported that GPO has made strides with respect to establishing and maintaining a diverse workforce, during this reporting period, the Agency faced additional diversity and EEO challenges. These were highlighted, in part, by several negative responses of employees and management officials to the Agency's recognition of Lesbian, Gay, Bisexual, and Transgender Month. Additionally, the House Committee on Appropriations in its report on Legislative Branch appropriations directed the Public Printer to submit quarterly reports on the progress being made in reducing the number of EEO complaints at GPO. While the Agency has begun management training on "EEO and Discriminatory Harassment," comprehensive diversity training for managers and employees at GPO is still needed.

We expect in the next reporting period a comprehensive implementation plan to address our audit recommendation, to include cultural sensitivity and diversity training for GPO managers and employees.

Improvements are still needed in other areas. For example, the Office of Personnel Management (OPM) completed a Human Capital Management Review of the GPO in late 2008. The objectives of the review were to determine GPO adherence to merit systems principles as well as compliance with applicable laws and regulations, and assess efficiency and effectiveness in administering human capital and human resources management programs and systems.

Among the significant findings of the OPM evaluation were that GPO (1) had not finalized its long-term strategic goals and objectives, (2) had not conducted a workforce analysis to identify its mission-critical occupations and competencies, (3) had no indication that the existing human capital function had the capacity and data structure needed to partner strategically with managers to conduct workforce analysis and planning, and (4) was not assessing its organizational, occupational, and individual needs or evaluating 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 indicated it has either planned or initiated actions that address the recommendations.

Finally, based on its own experience, the OIG is concerned with Human Capital's ability to perform successful workforce analysis, planning, and on-boarding. Within the last calendar year, the GPO OIG has hired six new personnel within the Office of Investigations. All of these employees have encountered problems with the hiring process, some of them quite serious. We are aware that an internal review

of the on-boarding process is currently underway by GPO organizational architects to assess whether the problems are isolated or more systemic. We will await the result of this review before assessing next steps. We anticipate the need for additional audit work beyond the current internal review.

3. Improved Financial Management. GPO substantially completed the 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. During FY 2009, the OIG completed IV&V activities associated with implementation of the Oracle E-Business suite. IV&V provided GPO with an independent assessment of project status, satisfaction of user needs, and project cost effectiveness.

The OIG continues to oversee the activities of KPMG LLP (KPMG), the Independent Public Accountant (IPA) conducting the annual financial statement audit. KPMG issued an unqualified opinion on the GPO's FY 2008 consolidated financial statements, stating that the Agency's financial statements were presented fairly, in all material respects, and in conformity with generally accepted accounting principles. KPMG did, however, identify three significant deficiencies, one of which—financial reporting controls—was considered a material weakness. Failure to adequately address and mitigate this material weakness could potentially prevent the Agency from obtaining future unqualified opinions on its financial statements. During this period, KPMG commenced work on the audit of GPO's FY 2009 consolidated financial statements. As part of the FY 2009 audit, KPMG will assess the corrective actions planned or taken by GPO to address the deficiencies identified during the FY 2008 audit.

4. Continuity of Operations. Development of the Agency's Continuity of Operations (COOP) capabilities will continue as a top management challenge. A previous OIG review of COOP planning contained several recommendations designed to improve the overall COOP posture of the Agency including most fundamentally that GPO adopt planning requirements and critical elements identified in Federal Preparedness Circular 65, "Federal Executive Branch Continuity of Operations." GPO developed a comprehensive COOP plan based on the Federal Emergency Management Agency template of key COOP components. The plan discusses issues such as essential functions, interoperable communications, delegations of authority and testing, training, and exercises. The Agency also developed an Occupant Emergency Plan (OEP) as a companion to its COOP. The OEP presents appropriate responses

to emergencies and discusses known or anticipated categories of emergencies.

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 during the most recent period included (1) a shelter-in-place exercise for all GPO employees, (2) distribution of fundamental facts to all GPO employees concerning the prevention of H1N1 and seasonal influenza infection, and (3) a COOP exercise at the Laurel Distribution Center. The COOP exercise at Laurel tested the GPO emergency notification system as well as the ability to produce the *Congressional Record* at the alternate location and use alternate computing facilities.

5. Internal Controls. GPO management establishes and maintains a system of internal controls for effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Almost all OIG audits include assessments of a program, activity, or function's applicable control structure. Several ongoing audits of GPO activities are assessing internal controls.

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."

During the FY 2008 financial statement audit, KPMG identified three significant deficiencies related to internal control over (1) financial reporting, which it considered a material weakness; (2) the processing of human resources information; and (3) information technology general controls. KPMG will assess the corrective actions taken and planned by GPO to address these deficiencies as part of the FY 2009 consolidated financial statement audit. Additional issues related to internal controls were identified in an audit of accounts payable service billings. The audit, described in more detail in the OAI section, found that controls over accounts payable, including the processes and procedures for tracking vendor invoices from receipt through payment, could be further strengthened and more consistently followed. The OIG made recommendations to GPO management to help improve controls over accounts payable service billings, and specifically, GPO's processes and procedures for invoice payment.

6. Security and Intelligent Documents. As the Federal Government's leading provider of secure credentials and identity documents, management regards Security and Intelligent Documents (SID) as a business unit best exemplifying the Agency's transformation toward high-technology production. During FY 2009, SID reported the successful manufacturing for the Department of State of more than 10.4 million electronic passports. The Washington, D.C. facility produced over 7.4 million passports while the Secure Production Facility (SPF) located as a COOP site in Stennis, Mississippi, produced more than 3 million passports.

SID continues to operate the Washington, D.C. based Secure Credential Center (SCC) to support the Department of Homeland Security's Customs and Border Protection (DHS/CBP) Trusted Traveler Program (TTP). During this reporting period, SCC began producing, personalizing, and distributing the Department of Health and Human Services Center for Medicare and Medicaid Service's Medicare identification cards to citizens of Puerto Rico.

In addition, SID reported completion of two critical process improvement methodologies in the Washington, D.C., Stennis SPF, and SCC facilities. The first process, known as 5S, is a series of defined steps and audits to achieve efficiencies in manufacturing process flows, in equipment use and placement, and in work environment housekeeping standards. The SID reported that the 5S program yielded significant and noticeable changes in the production spaces and created safer and more streamlined process flows. Additionally, SID reported the completion of a library of standard operating procedures, work flows, and work instructions for the manufacturing processes to underpin the efforts and lay foundation for the future certification in International Standards Organization (ISO) 9000 manufacturing standards.

SID also reported that it is working to complete the certification process for the SCC to become a facility qualified to handle, personalize and distribute HSPD-12 cards. This certification is expected in the spring of 2010 and will allow GPO's SCC to more comprehensively serve federal government organizations in the area of secure credentials.

GPO, in cooperation with the Department of State's Bureau of Consular Affairs, plans to issue a Request for Proposal in FY 2010 for the procurement of eCovers used in the manufacturing of U.S. Passports. The proposed eCovers 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 the ISO.

7. Protection of Sensitive Information. GPO must establish rules of conduct and appropriate administrative,

technical, and physical safeguards to ensure that sensitive information is adequately identified and protected. 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 personally identifiable information (PII). This includes PII contained in information systems as well as paper documents. In accordance with Office of Management and Budget (OMB) Memoranda 06-15 and 07-16, Executive Branch agencies have had to implement policies and procedures to protect and respond to the breach of PII as far back as the middle of 2007.

The OIG has advised GPO of its concerns regarding the protection of PII. As reported in OIG Report 07-09 – *GPO Compliance with the Federal Information Security Management Act,* dated September 27, 2007, and again in our draft FISMA report dated August 7, 2009, GPO's Information Technology and Systems division is making progress in protecting PII contained in information systems. However, much

work remains, including the issuance of an Agency directive on the protection of PII, designation of an official responsible for managing and monitoring the Agency's privacy compliance efforts (e.g. Chief Privacy Officer), full use of privacy impact assessments, and increased data encryption.

During this reporting period, due to the importance of this issue, the OIG developed and issued an internal policy on the protection of PII within the OIG's control. An Agency directive has been drafted to address the PII issue agency-wide. The OIG has requested a draft of the PII policy for review and comment. We also note that the Human Capital Office has taken steps to remove or redact certain PII from certain transmittals.

In addition, during this reporting period, we issued an MIR on the publication of a sensitive document, House Document 111-37, which contained sensitive information regarding our nation's nuclear sites. While we found no wrongdoing on the part of GPO, we recommended that GPO management provide more training to GPO staff on the handling and protection of sensitive information.

Finally, we recognize that GPO management concurred with our previous reporting period 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 to establish and oversee a comprehensive sensitive information protection program. We urge management to develop and implement the policies, procedures, and training necessary to address this most serious issue. The OIG will continue to monitor GPO's progress in addressing the protection of sensitive information.

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

Noteworthy challenges for the IT&S function include establishing a top level Enterprise Architecture and support for a number of significant initiatives, including FDsys, the e-Passport system, digital publication authentication using a Public Key Infrastructure (PKI), information system management, implementation of the Oracle E-Business Suite, and implementation of digital human resources systems. To create a plan that will help mitigate risks on aging legacy systems, IT&S initiated an analysis of legacy applications and its impact on business operations. Legacy systems increasingly inhibit the Agency's ability to respond to customer needs and must be replaced. IT&S recently completed a 5-year strategy that should help guide the Agency through implementation of new systems and retirement of legacy systems. Certain releases of FDsys, and Oracle E-Business became operational during FY 2009.

Because GPO provides services to Executive Branch agencies that must comply with the Federal Information Security Management Act of 2002 (FISMA), 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 an assessment of compliance with FISMA to identify any gaps and deficiencies in GPO's overall information security program, including critical systems. We initiated a follow-on FISMA assessment in FY 2008, which was being finalized during this reporting period. We also initiated our annual independent assessment of the GPO enterprise network infrastructure to evaluate the level of security controls in place that help protect IT resources from unauthorized access and compromise.

To fulfill its mission in the vital arena of electronic information dissemination and e-Government, GPO established a PKI that serves the needs of the Agency, its Legislative Branch partners, and other Federal partners.[2] The PKI is cross-certified with the Federal Bridge Certificate Authority—a substantial and necessary step toward using PKI for the

[2] By encrypting information, PKI ensures the highest level of protection for electronic information that travels over ordinary, nonsecure networks.

benefit of a variety of customers. PKI will serve as an important contributor for future revenue-generating activities within GPO.

To partially meet PKI certification provisions, the OIG conducts interim and annual compliance reviews that determine whether assertions related to the adequacy and effectiveness of the controls over GPO's PKI Certificate Authority operations are fairly stated based on underlying principles and evaluation criteria. As reported in the OAI Section, these compliance reviews were successfully conducted by an IPA and overseen by the OIG. Finally, the OIG will continue to lead IV&V activities associated with the ongoing implementation of FDsys.

9. Business Development 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.

GPO previously undertook reorganization of several business units to better serve its various Government customers. Specifically, the Agency created three new business units to improve service. Elements under the previous Customer Services business unit were realigned into two separate business units: Print Procurement and Sales and Marketing. Print Procurement was formed to handle the transaction process on behalf of Federal customers to commercial vendors whereas Sales and Marketing provides Web services, creative services, marketing research, and consultation to Federal customers. The third new business unit, Operations Support, includes engineering and environmental services. This business unit provides technical maintenance expertise, in house support, safety procedures and environmental compliance to the GPO manufacturing operations. This realignment of business units was initiated to help streamline processes, strengthen customer relationships, and develop new sales opportunities.

The Employee Communications Office also conducted a survey of focus groups within customer services to identify key strengths that could be leveraged and key barriers to improving service to customers. While many strengths and barriers were identified, the most common of them across the focus groups was the need for standard operating procedures which, if properly developed, would ensure that GPO customers receive the same quality service regardless of what team or individual within the Agency is providing it. GPO should continue these efforts undertaken to enhance business development and customer service. GPO should also review and update its Strategic Vision and reevaluate the Business Units' alignment with the Agency's mission and objectives.

10. Acquisitions. As with other Federal agencies across the Government, GPO faces challenges in its acquisition function. Acquiring goods and services, especially those necessary to transform the Agency and to provide services to its Federal customers, in an efficient, effective, and accountable manner is essential. With over $750 million in acquisitions during FY2008, we remain concerned that the Agency has not devoted the resources necessary to conduct assessments of the acquisition function to clearly identify gaps in effective performance and implement a plan to resolve critical issues, as required for Executive Branch agencies under the Services Acquisition Reform Act of 2003 and Office of Management and Budget (OMB) guidelines.

Last year, OMB provided guidelines to Executive Branch agencies to conduct internal reviews of the acquisition function required under OMB Circular A-123. OMB used the GAO "Framework for Assessing the Acquisition Function at Federal Agencies" as the standard assessment approach.[3] Although GPO is not required to follow OMB guidelines in this area, we believe that the Agency would greatly benefit from performing that acquisition review process and urge management to undertake this initiative.

[3] See GAO-05-218G, September 2005, accessible at http://www.gao.gov/new.items/d05218g.pdf.

OFFICE OF AUDITS AND INSPECTIONS (OAI)

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 37 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 September 30, 2009, 32 recommendations were open.

B. Federal Digital System (FDsys) – Independent Verification and Validation (IV&V)

The FDsys will be a comprehensive information life cycle management system that will ingest, preserve, provide access to, and deliver content from the three branches of the Federal Government. The system is envisioned as a comprehensive, systematic, and dynamic means of preserving electronic content free from dependence on specific hardware and/or software. FDsys has three major subsystems: the content management subsystem and content preservation subsystem which are accessible to GPO internal users only; and the access subsystem for public content access and dissemination. A multiyear, multirelease integration effort is being used to design, procure, develop, integrate, and deploy selected technologies and components of FDsys.

The OIG is responsible for IV&V work associated with developing and implementing FDsys. We contracted with American Systems due to their extensive IV&V experience within the Federal sector. American Systems has been contracted to conduct programmatic and technical evaluations of the FDsys Program to determine whether system implementation is consistent with the FDsys project plan and

cost plan and meets GPO requirements. Additionally, IV&V will monitor development and program management practices and processes to anticipate potential issues. Specific IV&V tasks include:

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

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

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

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

In January 2009, GPO released a public Beta version of the FDsys access subsystem, containing 8 of the 55 GPO Access collections. The content management and content preservation subsystems, supporting the Internal Service Provider, Congressional Publishing Specialist, Preservation Specialist, and Report user roles, was released in late March 2009. Over the last six months, the PMO has continued to update these FDsys subsystems, collectively referred to as Release 1. In addition, a major re-design has been implemented[4], 14 additional GPO Access Collections have been deployed, and numerous software problems have been corrected.

As of July 30, 2009, GPO has expended $33 million (unaudited) to deploy Release 1, substantially exceeding the original planned cost of $16 million. In addition, Release 1 has considerably less functionality in terms of the system requirements than was originally planned. Despite the recent updates, FDsys Release 1 still contains less than half (i.e. 21 of 55) of the GPO Access Collections; thus, both systems must be operational to ensure all GPO content is available to the public. Additionally, the deployment date for Release 1 was over a year and a half later than the original plan. Many factors have contributed to these cost, schedule, and technical overruns. As of the end of this reporting period, Release 1 is not complete nor GPO's "system of record" for all GPO publicly available content.

A complete IV&V assessment of the quality of the FDsys Program moving forward into FY 2010 is difficult at this time. The Program has met their initial goal of fielding a system, even though Release 1 contains less functionality than originally planned. Some products developed during the first Release were of high quality and will serve the Program well in the future. Other products are of reasonable quality and with some improvement will make future FDsys releases easier to manage. Still other products will require significant work to be useful on future releases. We believe the primary challenges for the FDsys Program are in the areas of program management, system engineering leadership and technical direction, and an adequate test program for the FDsys system. Our IV&V goal is to continue reporting to the PMO and GPO management on key risks and issues, and provide value-added recommendations to help mitigate those risks.

In Section D, we discuss the IV&V report issued during this reporting period.

C. Financial Statement Audit

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG is conducting the FY 2009 audit under a multiyear contract for which OAI serves as the Contracting Officer's Technical Representative (COTR). The oversight provided ensures that the audit complies with generally accepted government

[4] During deployment of two large FDsys Collections, memory overflow problems were encountered during ingest processing. As a result, the FDsys repository and architecture had to be re-designed.

auditing standards. OAI also assists with facilitating the external auditor's work as well as reviewing the work performed. In addition, OAI provides administrative support to the KPMG auditors and coordinates the audit with GPO management.

KPMG issued an unqualified opinion on GPO's FY 2008 consolidated financial statements, stating that the Agency's financial statements were presented fairly, in all material respects, and in conformity with generally accepted accounting principles. However, KPMG did identify three significant deficiencies including (1) financial reporting controls; (2) controls over processing human resource information; and (3) IT general controls.

During this reporting period, KPMG commenced work on the audit of GPO's FY 2009 consolidated financial statements. The 2009 audit includes assessing the status of the FY 2008 findings to determine whether they will need to be reported again in the FY 2009 audit report, along with potentially new findings and recommendations.

D. Audit and Inspection Reports

1. Audit Report 09-09 (Issued July 16, 2009)

Oracle Database Security for GPO's Passport Printing and Production System

GPO has a Memorandum of Understanding with the Department of State for producing, storing, and delivering all U.S. electronic passports (e-Passports). GPO's Passport Printing and Production System (PPPS) includes various computer applications and system software, including database systems, which support production of e-Passports. GPO's Security and Intelligent Documents business unit is responsible for PPPS and administers and manages its applications. The Information Technology and Systems Division (IT&S), under the direction of the Chief Information Officer (CIO), administers and supports PPPS system software, including database software. PPPS uses a series of Oracle databases. If databases are not configured securely, PPPS data and production are vulnerable to compromise, including disruption of system services.

The OIG conducted an audit to evaluate security configurations for the key Oracle databases supporting production of e-Passports and determine whether GPO was enforcing an appropriate level of security. As part of the audit, we reviewed the Agency's IT Security Program Statement of Policy, the PPPS System Security Plan, and the benchmarks for Oracle databases that the Center for Internet Security publishes. GPO must comply with each of these requirements when administering IT security. The OIG issued a sensitive report containing recommendations intended to further strengthen PPPS security and reduce the risk of system compromise.

2. Assessment Report 09-10 (Issued September 23, 2009)

GPO PKI Certification Practices Statement Conformity with the Federal PKI Common Policy Framework and the GPO Certificate Policy – Attestation Report

As part of GPO's Shared Service Provider (SSP) certification process, the Federal Public Key Infrastructure Policy Authority (FPKI-PA) required an evaluation of GPO's Certification Practices Statement (CPS) for the GPO Certification Authority (CA) that will be issuing digital certificates under the SSP program for conformity to the Federal Common

Policy Framework and the GPO Certification Policy (CP). The SSP program was established under the Federal Identity Credentialing Committee and the FPKI-PA to give Federal departments and agencies a way to access PKI services while leveraging previous government investments. Under the Electronic Government Act of 2002, the Office of Management and Budget determined that, beginning in FY 2006, Federal agencies that intend to use PKI services must buy from qualified service providers operating under the Federal Common Policy Framework.

To conduct the assessment, the OIG contracted with Ernst & Young (E&Y), licensed by the American Institute of Certified Public Accountants (AICPA), to provide PKI-related assurance services.

The assessment determined that the CPS was in conformity with the Federal PKI Common Policy Framework and the GPO CP.

3. Assessment Report 09-11 (Issued September 23, 2009)

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

GPO has implemented a PKI to support its mission related to electronic information dissemination and e-government, and to meet GPO customer expectations that documents are official and authentic. The GPO PKI is certified with the Federal Bridge Certificate Authority (FBCA) whose certification provisions require that the GPO PKI undergo an annual independent compliance review. To satisfy this compliance requirement, the OIG tasked E&Y to conduct a WebTrust assessment of GPO's CA. The assessment was conducted in accordance with the AICPA "WebTrust Principles and Criteria for Certification Authorities."

The assessment represents an evaluation of whether GPO management's assertions related to the adequacy and effectiveness of controls over its CA operations is fairly stated based on underlying principles and evaluation criteria. The assessment also measured the GPO CA's compliance with reporting requirements of the FPKI-PA.

For the period July 1, 2008 through June 30, 2009, the E&Y issued an Attestation Report which expressed its unqualified opinion that GPO's management assertion related to the adequacy and effectiveness of controls over its CA operations, was in all material respects, fairly stated based on the AICPA WebTrust for Certification Authorities Criteria. Additionally, the E&Y issued a Letter of Supplementary Information to address additional FPKI-PA reporting requirements.

4. 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

GPO's 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 in its conduct of 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 (formerly R1C2). American Systems is required by the contract 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 processes in controlling risk avoidance

This seventh quarterly report, for the period January 1, 2009 to May 8, 2009, contains recommendations designed to strengthen FDsys program management, particularly for future FDsys releases. Management generally concurred with the report's recommendations with the exception of one. We are in the process of following up with management to reach agreement on the one unresolved recommendation.

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

Accounts Payable Service Billings

The OIG conducted an audit to evaluate GPO's processes and procedures for invoice payment. The specific audit objectives were to (1) assess the adequacy of the system for tracking individual accounts payable invoices from receipt through payment, (2) determine whether discounts, if any, were taken, (3) identify duplicate payments, if any, and (4) identify delays or potential delays in the accounts payable process.

In FY 2007, GPO reported total accounts payable of about $96 million, which included commercial printing, U.S. Government agencies, and other accounts payable. Although commercial printing was the largest category of accounts payable, other accounts payable expenses had increased by approximately 174 percent from FY 2006. Approximately 90 percent of the increase was the result of materials and supplies for the new e-Passports.

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 systems did not always exist.

Specifically, the sampling of transactions identified control weaknesses such as (1) missing end-user approvals, (2) missing support for Contracting Officer payment authorization, (3) no evidence of invoice examination and certification, and (4) hard copy invoice data could not be reconciled to the accounts payable system. As a result, there was no assurance that management controls are operating effectively, which could have resulted in a potential misstatement of monthly and annual financial information. Subsequent to the conclusion of the audit, GPO provided supporting documentation for the exceptions identified during the audit. The audit also identified that generally, if made available by the vendor, discounts were taken. Further, we did not identify any duplicate payments made to vendors or any significant delays in the payment process.

Two recommendations were made to GPO management which, if implemented, will help improve controls over accounts payable service billings, and specifically, GPO's processes and procedures for invoice payment. GPO Management concurred with each of the report's recommendations and has planned corrective actions that we consider responsive.

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

GPO Workers' Compensation Program

The OIG completed an audit of the GPO's Workers' Compensation Program to evaluate the adequacy of its controls. The specific audit objectives were to determine whether (1) GPO's program was complying with appropriate Federal guidelines, regulations,

and directives related to workers' compensation, and (2) GPO employee claims for workers' compensation are supported by required documentation.

The Federal Employees' Compensation Act (FECA) provides income and medical cost protection to covered Federal civilian employees injured on the job, employees who have incurred a work-related occupational disease, and beneficiaries of employees whose deaths are attributable to job-related injuries or occupational diseases. The U.S. Department of Labor (DOL) administers the FECA Program, which provides workers' compensation benefits to GPO employees and others through the Special Benefit Fund.

GPO annually reimburses DOL for the cost of FECA benefits paid on GPO's behalf. FECA provides benefits and compensation for total or partial disability; schedule awards for permanent loss or dismemberment of specified parts of the body; related medical costs; and vocational rehabilitation. GPO manages and administers its workers' compensation program in accordance with FECA through its Office of Workers' Compensation (OWC). As of June 30, 2008, the estimated workers' compensation liability for GPO was approximately $5.45 million.

The audit identified that GPO's OWC should be commended for the improvement in both the organization and management of this program in the time since the previous audit in 2002. Since then, controls over GPO's Workers' Compensation Program have been strengthened and the program has undergone significant changes. OWC's personnel, including its management, have completely turned over. The change in personnel resulted in the implementation of many of the recommendations from the 2002 audit that had either not been implemented or were partially implemented by previous staff and management. The current Chief of OWC has also implemented many changes related to the use of information technology resources previously recommended. As a result of those changes, improvements to the organization have been made and controls over workers' compensation claims and cases strengthened, including its working relationship with the DOL.

We also note that the overall amount of billings from DOL for the cost of workers' compensation benefits paid on GPO's behalf decreased to under $6 million during FY 2007. The total number of GPO workers' compensation claimants decreased from 193 in 2002 to 136 in 2008.

We found no indication that the program was not being operated in accordance with appropriate Federal guidelines, regulations, and directives. Although employee claims for workers' compensation benefits were generally supported with the required documentation, there were several areas where procedural and policy improvements can be made to further enhance and strengthen the GPO's Workers' Compensation Program. A total of two recommendations were made to management, which if implemented, will ensure that the program continues to be operated in an efficient and effective manner. Management generally concurred with the recommendations or agreed to take responsive alternative actions to address the issues identified.

E. Status of Open Recommendations

Management officials made progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. For the 32 recommendations still open, a summary of the finding and recommendations, along with the status of actions for implementing the recommendation and OIG comments, follow.

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. Further details regarding assessment findings can be obtained by contacting the OIG.

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 of the report's recommendations and initiated corrective action.

OIG COMMENTS

Two recommendations made in this report remain open. The OIG continues to work with management to monitor implementation of the remaining two open recommendations, whose status will be further reviewed as part of the OIG's FY 2009 Network Vulnerability Assessment.

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 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, the 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 of the recommendations and proposed corrective actions.

OIG COMMENTS

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

3. Assessment Report 08-01 (Issued November 1, 2007)

GPO Network Vulnerability Assessment

FINDING

The OIG completed a vulnerability assessment of the GPO enterprise network infrastructure and evaluated the level of security controls in place that help protect the Agency's IT resources from unauthorized access and compromise. We limited our assessment to the area between GPO's Internet service provider and the outermost firewall interface where the Agency's publicly available network resources, such as GPO Access, are hosted. That area is commonly referred to as the demilitarized zone, or DMZ. We determined whether GPO (1) maintained a robust and effective vulnerability scanning and management program that identified and circumvented common internal and external threats to its network, (2) used passwords in the DMZ strong enough to prevent brute force attacks, and (3) patched systems in the DMZ in a timely and effective manner. The assessment revealed that there was room for improvement and recommended ways that would not only help strengthen security of the publicly available network resources but also reduce the risk of system compromise and loss of availability.

RECOMMENDATION

The report contains seven recommendations that if implemented will not only help strengthen network security but also reduce the risk of system compromise and loss of availability.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed corrective actions.

OIG COMMENTS

Two recommendations remain open. The status of these recommendations will be reviewed as part of the OIG's FY 2009 Network Vulnerability Assessment.

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

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

FINDING

The Passport Printing and Production System (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 to not only help strengthen security of the PPPS but also reduce the risk of system compromise.

MANAGEMENT COMMENTS

Management generally concurred with each of the recommendations and proposed responsive corrective actions.

OIG COMMENTS

One recommendation remains open.

5. 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 identified by

GAO. 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 identified by GAO. 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 of the recommendations and stated that implementation would require the Public Printer's review and approval.

OIG COMMENTS

The two recommendations remain open. Management has begun implementing the remaining essential elements of MD-715 and the leading diversity management practices identified by the GAO.

6. 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 will provide many 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.

Table of Open Recommendations

Audit	Number of Open Recommendations	Number of Months Open
06-02 GPO Network Vulnerability Assessment	2	42
07-09 GPO's Compliance with the Federal Information Security Management Act	7	24
08-01 GPO Network Vulnerability Assessment	2	21
08-06 Operating System Security for GPO's Passport Printing and Production System	1	18
08-10 Diversity Management Programs at GPO	2	12
08-12 Assessment of GPO's Transition Planning for Internet Protocol Version 6 (IPv6)	1	12
09-01 Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability	3	10
09-02 GPO's Passport Printing Costs	3	9
09-03 FDsys IV&V – Fifth Quarter Report on Risk Management, Issues, and Traceability	4	9
09-04 FDsys IV&V – Security Analysis Report	3	9
09-07 FDsys IV&V – Sixth Quarter Report on Risk Management, Issues, and Traceability	3	9
09-08 Oracle E-Business Suite Release 2 IV&V – Technical	1	6

RECOMMENDATION

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

MANAGEMENT COMMENTS

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

OIG COMMENTS

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

7. 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

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 of the recommendations and proposed responsive corrective actions

OIG COMMENTS

Three recommendations remain open.

8. 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 (DOS). 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 DOS. 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 DOS 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 DOS 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 of the recommendations and proposed responsive corrective actions

OIG COMMENTS

Three recommendations remain open. Management continues to take responsive actions to implement the three recommendations which we anticipate closing during the next reporting period.

9. 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 ten recommendations to management intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with six of the recommendations, partially concurred with one, and nonconcurred with three. Management proposed responsive corrective actions to six of the recommendations. 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.

10. 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 report contained five recommendations intended to strengthen FDsys system security planning and implementation.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed responsive corrective actions.

OIG COMMENTS

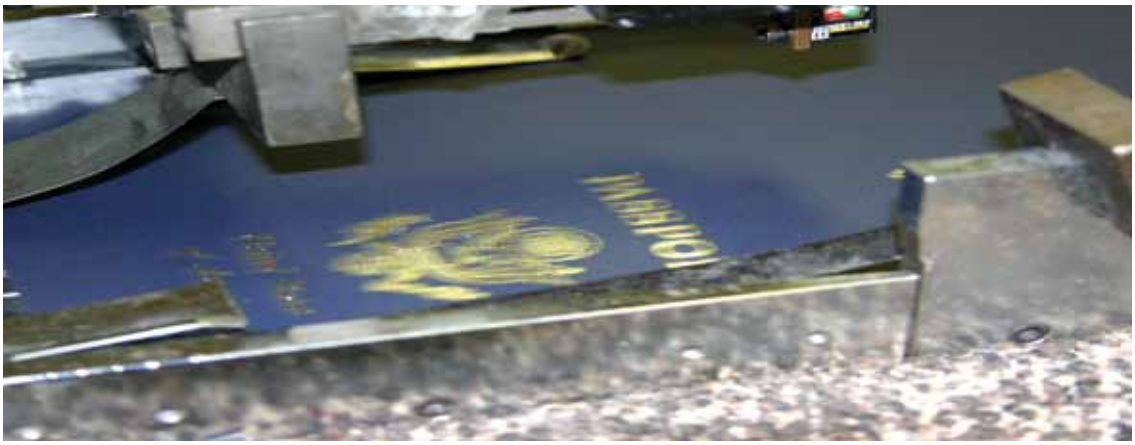
Three recommendations remain open. Management continues to take responsive actions to implement the three recommendations.

11. Assessment Report 09-07 (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 report contained four recommendations intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with each of the report's recommendations and proposed responsive corrective actions.

OIG COMMENTS

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

12. Assessment Report 09-08 (Issued March 31, 2009)

Oracle E-Business Suite Release 2 Independent Verification and Validation (IV&V) - Technical

FINDING

The OIG contracted with Noblis to conduct IV&V for Oracle Release 2. Release 1 was initiated to begin taking advantage of GPO's investment in Oracle technologies and allowing GPO to create a model for future implementation activities. Release 2 adds additional functionality to the original Oracle modules as well as introducing new business processes. The OIG contract tasks Noblis to assess program management, technical, and testing activities associated with the Release 2 implementation. Noblis is required to issue summary reports for program management, technical, and testing IV&V.

The report provides a summary of the key risks and issues identified by Noblis regarding the processes, artifacts, and products related to development of Release 2, with particular emphasis on data conversion, user preparation, user acceptance testing, and deployment planning.

RECOMMENDATION

The report contained ten recommendations intended to strengthen the Oracle Release 2 program.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed responsive corrective actions for each.

OIG COMMENTS

One recommendation related to planning for post deployment remains open.

OFFICE OF INVESTIGATIONS

OI is responsible for conducting and coordinating 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 (MIR), 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 (DOJ), the National Procurement Fraud Task Force and other investigative agencies and organizations.

A. Summary of Investigative Activity

OI continued the process of opening complaint files for conducting preliminary investigations. At the end of last reporting period, 23 complaints remained open. OI opened 39 new complaint files this period, 23 complaints were converted to full investigations, and 9 were closed after preliminary review with no action. Additionally, three complaints were referred to GPO management and three to another agency. Twenty-four complaints remain open at the end of the reporting period.

At the end of the last reporting period, 29 investigations remained open. During this reporting period, 12 investigations were closed and 9 investigations resulted in referrals to GPO management for potential administrative action. Ongoing at the end of this reporting period are 38 investigations.

During this period, seven presentations were made to the DOJ for potential criminal prosecutions. Of those cases presented, DOJ has indicated an interest in pursuing two for possible prosecution. Five presentations resulted in declinations and those cases are now being pursued administratively. No presentations were made for civil purposes during this reporting period.

Several investigations are currently being conducted in coordination with DOJ, including its Antitrust and Public Integrity Divisions. Twenty Inspector General subpoenas were issued during this period. Documents requested include bid preparation and agreements among contractors and/or affiliated companies. Two consent searches were conducted on separate employee misconduct cases.

Specific OI investigative activities and accomplishments are reported in the following categories below: Procurement Fraud, Workers' Compensation Fraud, Employee Misconduct, and Other Investigations.

B. Procurement Fraud Investigations

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. GPO procures more than $750 million of goods and services each year through contracting. With this vulnerability in mind, OI has focused much investigative development to the area of procurement fraud. The inventory of procurement fraud complaints/investigations has increased from 7, just one year ago, to 23 open procurement fraud investigations today, or 61% of our active caseload. This number does not include allegations in complaint status, and still under preliminary review.

PROACTIVE EFFORTS

Throughout this reporting period, the IG and OI management provided procurement fraud presentations to GPO contracting personnel. Our fraud presentations, tailored to the types of contracts administered by GPO, were provided to RPPOs in Atlanta, Dallas, Denver, Hampton, Oklahoma City, Philadelphia, San Francisco, and Seattle. This completed our goal of providing specialized training to staff of the 15 GPO RPPOs within FY 2009. Each presentation has resulted in broad participation by attendees and valuable discussion about procurement fraud vulnerabilities at GPO. As a result of these presentations, we have received specific fraud referrals and several proactive and audit initiatives are under consideration based on input from GPO procurement personnel who participated in the fraud briefings.

In an effort to improve the quality of our investigations, OI held a half-day internal procurement fraud training for our Special Agents. OI management presented examples of procurement fraud allegations and led discussion concerning details to learn from complainants, thorough questioning of witnesses, and documentation required to fully develop each allegation. Additional internal training sessions are planned, including one designed to discuss product substitution, a contract fraud scheme prevalent with fixed-price contracting. Special Agent Elisabeth Heller recently completed a pilot course in Product Substitution, offered by the Federal Law Enforcement Training Center, and has agreed to assist in developing this training for OI.

ACCOMPLISHMENTS

An investigation of a GPO contractor resulted in the suspension and proposed debarment of the company and the company's officers from doing business with GPO as a contractor, subcontractor, or contractor's representative. The investigation found evidence the contractor lacked business integrity that directly affected their present responsibility as a GPO contractor. This

evidence revealed that, throughout contract performance, this vendor failed to comply with specifications of the contract. 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 all work was completed in accordance with all contract terms. The contractor submitted at least ten invoices. This investigation remains ongoing.

The OI also received an allegation of a possible breach of PII by a GPO contractor. The contractor was responsible for producing agency notices to citizens and it was alleged the contractor may have improperly disposed of spoilage containing PII. Within several days, OI investigators responded onsite to interview contractor personnel, review contract specifications, obtain documentation tracking the procedures for spoilage disposal, and evaluate the extent of the breach. The investigation did not identify any specific contract violations by the firm and the information obtained suggested this was an isolated incident. Our findings were immediately reported to GPO management and a Report of Investigation was issued to GPO detailing the full results of the investigation.

In our last Semiannual Report, we noted that another investigation determined that a contractor inappropriately disclosed PII. Because of the possible systemic nature of the issues identified, the IG issued an MIR to the Public Printer. The OIG recommended that GPO identify any contracts and contractors handling PII, review security requirements, request security plans, conduct on-site surveys and inspections, and appoint a GPO Privacy and/or Data Security Officer to ensure integrity in the handling of PII. GPO management concurred with all nine recommendations and further reported verification and proactive efforts concerning vendor compliance with security requirements and plans to work with GPO customer agencies toward implementation of the OIG recommendations.

We also previously reported on an OI investigation, worked in coordination with several other law enforcement entities, that revealed fraudulent GPO and other Government purchase card transactions. During this reporting period, an individual who had pled guilty to fraud charges was sentenced to 100 days in a half-way house and 18 months probation. Restitution of $14,409.19 to the defrauded vendors was also ordered.

During this reporting period, DOJ accepted an investigation that found a GPO vendor made false statements and claims to GPO. DOJ has issued a Civil Demand Letter to the GPO contractor. Further details will be reported in a future period.

C. 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 involving possible fraudulent claims for workers' compensation.

The Assistant Inspector General for Investigations and Special Agent-in-Charge met with the Director of the GPO Office of Workers' Compensation, to facilitate our working relationship and discuss procedures for conducting investigations of interest to their office. Further discussions on specific investigations are anticipated.

D. Employee Misconduct

OI investigates allegations involving GPO employee misconduct. Allegations generally include misuse of Government computers, false statements, theft, assaults, drug violations, gambling, and travel voucher fraud. OI has five open investigations involving alleged misconduct.

ACCOMPLISHMENTS

As a result of an OI investigation, GPO issued notices of intent to terminate from employment to four employees and placed them on administrative leave. The investigation disclosed evidence the employees made false statements during the conduct of their employment. Additional details will be reported in a future period.

The OI issued a Report of Investigation concerning allegations of overtime abuse/fraud by a GPO employee. Although the investigation disclosed insufficient evidence to support the allegations, we reported weaknessess in controls that govern the overtime authorization and approval

process for certain GPO employees and made recommendations for process improvement. GPO has reported its intent to implement improvements in these overtime approval procedures.

Another investigation of possible employee misconduct resulted in a written notification to GPO of possible breach of information. Due to the apparent lack of adequate controls, this information was also referred to the OAI and an audit has been initiated to determine the full scope of the issue. GPO also reported they have begun a comprehensive review of its policies and protocols in this area. The investigation remains ongoing.

E. Other Investigations

OI performs 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 investigation by other legislative agencies. OI has five open investigations involving these types of allegations.

ACCOMPLISHMENTS

On August 3, 2009, the IG issued a MIR communicating the findings of our investigation of GPO's publication and Internet posting of House Document 111-37 (HD 111-37), which contains extensive information on U.S. civilian nuclear sites, locations, facilities, and activities. In June, media reports indicated that HD 111-37 was "mistakenly released online…by the Government Printing Office." The OI initiated an investigation to determine GPO's responsibility, if any, for possible security lapses or other violations that may have led to the disclosure of HD 111-37.

Our investigation found no wrongdoing on the part of GPO or its employees. GPO's customer agency is responsible for identifying whether a document is of a sensitive or otherwise restricted nature when requesting document publishing. The Executive Communications Clerk of the U.S. House of Representatives transmitted HD 111-37 to GPO for publication on May 6, 2009, without restriction or special handling requirements. As directed by its customer, GPO printed HD 111-37 on May 6 and posted the document under normal procedures on the GPO Access Web site within a day of printing. When the Clerk notified GPO of the sensitivity of the document on June 2, 2009, it was promptly removed from GPO Access.

Our MIR stated that additional controls at GPO may help identify and prevent in the future an unwanted disclosure of sensitive information. We made four recommendations to GPO management designed to help improve GPO's process for handling and publishing sensitive information. On September 8, 2009, GPO Management concurred and reported they were directing implementation of each recommendation.

After preliminary review, one incident involving potential Title 44 violations was referred to the appropriate OIG for action. This complaint alleged that another agency may be in violation of Government printing laws and the Anti-Deficiency Act. Section 501, Title 44, United States Code requires that, with limited exceptions, GPO print all Government documents, including that of Executive Branch departments and agencies. In addition, section 207 of the Legislative Branch Appropriations Act, supplements section 501, by specifically prohibiting use of appropriated funds for most Government printing procured outside of the GPO.

F. Work-In-Progress

Other significant OI matters are pending as of the end of this reporting period. Disposition and results of those investigations will be provided in future reports.

APPENDICES

APPENDIX A

Glossary and Acronyms

GLOSSARY

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

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

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

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

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

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

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

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

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

Management Implication Report- A report to GPO 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(s) of the finding(s) identified by the IG to take advantage of an opportunity.

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

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

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

Unsupported Costs - Questioned costs not supported by adequate documentation.

Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
CPS	Certification Practices Statement
DHS/CPB	Department of Homeland Security/ Customs and Border Patrol
DMZ	Demilitarized Zone
DOJ	Department of Justice
DOS	Department of State
FBCA	Federal Bridge Certificate Authority
FPKI-PA	Federal Public Key Infrastructure Policy Authority
FDsys	Federal Digital System
EEOC	Equal Employment Opportunity Commission
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GPO	U.S. Government Printing Office
HSPD-12	Homeland Security Presidential Directive-12
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
OALC	Office of Administration/Legal Counsel
OAI	Office of Audits and Inspections
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
PPPS	Passport Printing and Production System
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	6
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	17–30
Section 5(a)(2)	Recommendations for Corrective Actions	17–26
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	20–26
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	28–30
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)	17–26
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	35
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	36
Section 5(a)(10)	Summary of prior Audit and Inspection Reports issued for which no management decision has been made	n/a
Section 5(a)(11)	Description and explanation of significant revised management decision	n/a
Section 5(a)(12)	Significant management decision with which the IG is in disagreement	n/a

APPENDIX C
Statistical Reports

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

Description	Questioned Costs	Unsupported Costs	Total
Reports for which no management decision made by beginning of reporting period	$0	$0	$0
Reports issued during reporting period	$0	$0	$0
Subtotals	$0	$0	$0
Reports for which a management decision made during reporting period			
1. Dollar value of disallowed costs	$0	$0	$0
2. Dollar value of allowed costs	$0	$0	$0
Reports for which no management decision made by end of reporting period	$0	$0	$0
Reports for which no management decision made within 6 months of issuance	$0	$0	$0

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

Description	Number of Reports	Funds Put To Better Use
Reports for which no management decision made by beginning of reporting period	0	$0
Reports issued during the reporting period	0	$0
Reports for which a management decision made during reporting period		
• Dollar value of recommendations agreed to by management	0	$0
• Dollar value of recommendations not agreed to by management	0	$0
Reports for which no management decision made by the end of the reporting period	0	$0
Report for which no management decision made within 6 months of issuance	0	$0

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

Reports	Funds Put To Better Use
Report on Audit of Oracle Database Security for GPO's Passport Printing and Production System (PPPS) (Audit Report 09-09, issued July 16, 2009)	$0
Report on GPO PKI Certification Practices Statement Conformity with the Federal PKI Common Policy Framework and the GPO Certificate Policy – Attestation Report (Assessment Report 09-10, issued September 23, 2009)	$0
Report on WebTrust Assessment of GPO's Public Key Infrastructure Certification Authority – Attestation Report (Assessment Report 09-11, issued September 23, 2009)	$0
Report on Federal Digital System (Fdsys) Independent Verification and Validation – Seventh Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-12, issued September 30, 2009)	$0
Report on Audit of Accounts Payable Service Billings (Audit Report 09-13, issued September 30, 2009)	$0
Report on Audit of GPO Workers' Compensation Program (Audit Report 09-14, issued September 30, 2009)	$0
Total	$0

Table C-4: Investigations Case Summary

Total New Hotline/Other Allegations Received during Reporting Period	65
No Formal Investigative Action Required	26
Investigations Opened by OI during Reporting Period	21
Investigations Open at Beginning of Reporting Period	29
Investigations Closed during Reporting Period	12
Investigations Open at End of Reporting Period	38
Referrals to GPO Management	9
Referrals to Other Agencies	7
Referrals to OAI	1

Current Open Investigations by Allegation	38	
Procurement Fraud	23	61%
Employee Misconduct	5	13%
Workers' Compensation Fraud	5	13%
Other Investigations	5	13%

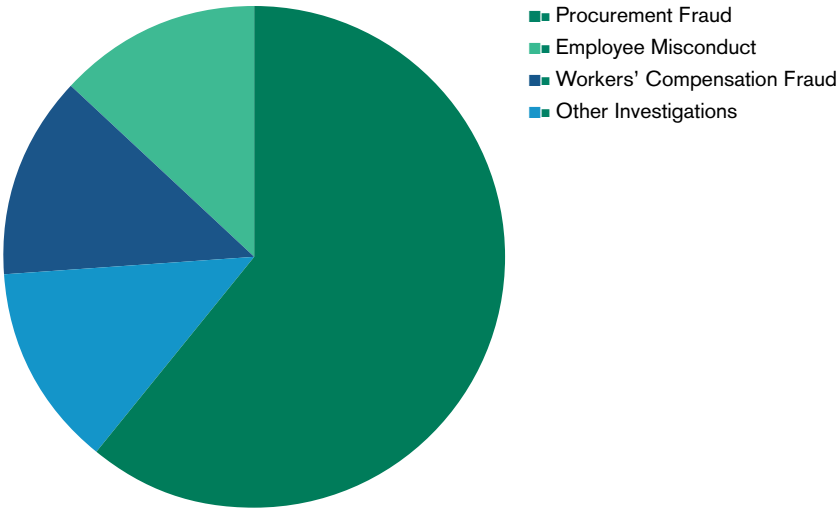


Table C-5: Investigations Productivity Summary

Arrests	0
Total Presentations to Prosecuting Authorities	7
Criminal Acceptances	2
Criminal Declinations	5
Indictments	0
Convictions	0
Guilty Pleas	0
Probation (months)	18
Jail Time (days)	100
Restitutions	$14,409.19
Civil Acceptances	1
Civil Demand Letters	1
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	0
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	9
Contractor Debarments (Proposed)	1
Contractor Suspensions	1
Contractor Other Actions	1
Employee Suspensions	0
Employee Terminations (Proposed)	4
Employee Warned/Other Actions	1
Other Law Enforcement Agency Referrals	2
Inspector General Subpoenas	20
Consent Searches	2

OFFICE OF INSPECTOR GENERAL

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