United States Government Printing Office | Office of Inspector General

SEMIANNUAL REPORT TO CONGRESS

April 1, 2008 through September 30, 2008

The U.S. Government Printing Office

For well over a century, the U.S. Government Printing Office (GPO) has been fulfilling 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 about 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 provides leadership and coordination as well as evaluates GPO's internal control structure. It 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. It 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.

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.

The OIG is dedicated to acting as an agent of positive change—changes that will help GPO improve its efficiency and effectiveness as it undertakes its era of unprecedented transformation.

Contents

Message from the Inspector General

This Semiannual Report to Congress marks a milestone in the Office of Inspector General at the GPO. Twenty years ago, the President signed Public Law 100-504, which included the *Government Printing Office Inspector General Act of 1988*, thereby establishing a statutory Office of Inspector General at GPO. While the Inspector General Act of 1978 set the ground work for Offices of Inspectors General in Executive Branch agencies, the GPO Inspector General Act established the first statutory Inspector General within the Legislative Branch. It would not be until 2005 before the GPO OIG was joined by another statutory Legislative Branch Inspector General at the Library of Congress. And since then, Congress has added the U.S. Capitol Police, Architect of the Capitol, and the Government Accountability Office.

During the past twenty years, the GPO OIG has undergone significant change. At one time the GPO OIG had a staff of more than 50, with an audit group dedicated to financial and compliance work and an investigative unit that dealt primarily with employee misconduct and contractor issues. As the size of the Agency was reduced, so too has the number of staff in the OIG. Today, while less than half the size of its peak, the responsibilities of the OIG have grown dramatically. The Agency's unprecedented transformation to digital information processing and high-tech security printing has brought to the OIG new and complex challenges that are met by dedicated auditors, inspectors, and criminal investigators.

The complexity of the work is borne out in this semiannual report. Our Office of Audits and Inspections is responsible for the oversight of several contractors facilitating robust independent verification and validation (IV&V) of two significant GPO programs – the implementation of the Future Digital System (FDsys) and transition of legacy systems to Oracle integrated business solutions. These IV&V efforts have helped identify risks and vulnerabilities to these programs so that if corrected, GPO may be assured of greater chance of success upon deployment. The emphasis on information technology and security will continue to evolve as do the inherent risks and vulnerabilities of the IT systems at GPO. To that end, we continued to address efforts to protect the e-Passport Production system, as well as assess GPO's Public Key Infrastructure and GPO's transition planning for Internet Protocol Version 6. Such reviews were beyond comprehension when the OIG was contemplated twenty years ago.

The Office of Investigations is also in the midst of upgrading its operations as we move into our 21st year. With the recent addition of a new Assistant Inspector General for Investigations, planning is underway to develop more complex contract and procurement fraud cases as well as continue to address matters in technology related crimes, workers' compensation fraud, and employee misconduct. And while the advance of technology has changed how the agency does business and the types of criminal and administrative matters our office will confront, there are still those who live in the past and have failed to embrace fundamental tenets of respect and consideration to fellow employees. During this reporting period, an investigation by the OI resulted in the indictments of three GPO employees for the physical abuse of a vulnerable employee. While twenty years ago such activity might have been dismissed as horseplay, in a 21st century workforce such behavior cannot be tolerated. I applaud the vigorous investigation by our OI which resulted in these indictments.

While we reflect upon our progress over the past twenty years, I am encouraged by the strength of character and commitment of the OIG to look forward to the future and meet the needs of the OIG with a renewed sense of vitality.

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 provided comments on proposed legislation and regulations. The work of each of the OIG components is summarized below.

The Office of Audits and Inspections (OAI) issued 7 reports with a total of 16 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency, and continued working with management to close recommendations from earlier reporting periods. OAI continued its IV&V work on FDsys and Oracle E-Business Suite implementation and completed an audit of diversity management programs at GPO in response to a congressional request. OAI also completed a follow-up audit of centrally charged travel expenditures that resulted in identifying approximately $8,495 in erroneous payments and performed a security audit of the databases that support the Passport production systems. Finally, OAI completed a WebTrust assessment report of GPO's Certification Authority and an assessment on GPO's transition planning for Internet Protocol Version 6.

The Office of Investigations (OI) opened 18 investigative cases, closed 20, and has 22 ongoing investigations. During this reporting period, one investigation resulted in three criminal indictments, and another case was accepted for possible criminal prosecution. One case against a contractor was referred for administrative action. In addition, due to its investigative efforts, a forfeiture of $226,821.74 in workers' compensation was assessed against an individual who was also taken off workers' compensation rolls. A cost savings to the Government of $42,000 per year will also be realized ($420,000 in actuary amount over 10 years).

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 that the OIG faces as well as congressional and media relations and information requests. During this reporting period, OALC reviewed several audit and investigative reports, assisted OI with several matters that the Department of Justice accepted for civil and criminal prosecution, and oversaw OI operations for 3 months during the absence of an Assistant Inspector General for Investigations.

In addition, OALC provided legal advice to the U.S. Capitol Police Inspector General in a variety of matters and reviewed and provided comments to an Agency Directive on Workers' Compensation. OALC also acted on a variety of matters as the OIG liaison to the GPO General Counsel, including support with GPO litigation matters, and the GPO Office of the Chief of Staff. Finally, OALC participated in the Council of Counsels to the Inspector General (CCIG). In that role, OALC led a task force for developing language for new GPO- produced, secure credentials for OIGs throughout the Federal Government. OALC also coordinated development, with the GPO Web Development and Creative Services Division, of an informational Web site for the CCIG.

OIG Management Initiatives

Personnel Update

During this period, several changes occurred in OI. Ronald Koch, the Assistant Inspector General for Investigations, retired. Several other members of the Investigations team left to join other OIGs. As a result, OI welcomed three new members in August.

We are excited that Debra Miller has joined the OIG OI as the new Assistant Inspector General for Investigations. Debbie has an impressive record in the OIG community. She began her OIG career in 1982 as a Special Agent with the Environmental Protection Agency's OIG and then later moved to NASA's OIG where she worked on sensitive and complex criminal and civil investigations. One significant achievement at NASA was her work as the lead agent on the investigation of the Hubble Space Telescope primary mirror flaw. That investigation resulted in a civil settlement of $25 million with the mirror manufacturer, at the time the largest recovery by the NASA OIG. Most recently, Debbie initiated and developed the Social Security Administration OIG's contract fraud investigative program. Debbie graduated from Florida State University with a Bachelor of Science in Criminology.

Elisabeth Heller joined the OI as a Special Agent. Elisabeth comes to us from the Department of Health

and Human Services OIG where she worked as a Special Agent. Previously, she worked at the Office of Personnel Management as a Special Agent working on personnel security investigations. Elisabeth graduated from George Mason University with a Bachelor of Science in Criminal Justice.

Latarsha Isom joined the OIG as a Special Agent. Latarsha comes to us from the Treasury Department's Bureau of Engraving and Printing, where she worked for the last 10 years, most recently as an investigator in the Office of Security. Latarsha graduated from Central Connecticut State University with a Bachelor of Arts in Psychology.

The OALC also welcomed a new member. Timothy Harbeck became the first law clerk to work for the GPO OIG helping on a variety of research and policy matters. Tim graduated from the University of Virginia with a Bachelor of Science in Mechanical Engineering. Before attending law school, Tim worked as a Patent Examiner at the U.S. Patent and Trademark Office focusing on Business Methods applications. Tim is in his second year of law school at the George Mason University Law School.

"Indeed, a conversation about diversity is not possible unless all diverse populations and cultures that enrich our workforce are included in the discussion."

Testimony on GPO's Diversity Management Programs by J. Anthony Ogden, Inspector General, before the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia on September 16, 2008.

Executive Council on Integrity and Efficiency

The President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) were both established by Executive Order to coordinate and enhance governmental efforts, to promote integrity and efficiency, and to detect and prevent fraud, waste, and abuse in Federal programs. The PCIE comprises 32 Inspectors General (IGs) that the President appoints. The ECIE comprises 35 IGs that agency directors appoint. The OIG at GPO is a member of the ECIE and participates regularly in its activities.

In ongoing response to the Senate Appropriations Committee request that the legislative branch IGs communicate, cooperate, and coordinate with each other on an informal basis, the legislative branch IGs continued to meet on a quarterly basis. The meetings continue to improve communications and contact between the Legislative Branch IGs. During this reporting period, the Legislative Branch IGs provided comments about legislation to amend the Inspector General Act of 1978, as amended, (IG Act) in an effort to aid committee staff understanding of distinctions with Executive Branch IGs.

Legislative Branch IGs also developed a comprehensive audit plan and completed a summary report of an audit of all legislative branch agency diversity offices. The summary report was produced at the request of the Chairman of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia of the House Committee on Oversight and Government Reform, and presented in a hearing before this Subcommittee on September 16, 2008. Quarterly meetings continue to rotate among IG offices of the Legislative Branch. Updates and the progress of those meetings will be provided in our respective semiannual reports.

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, as the Legislative Branch member of the ECIE Legislative Committee, the IG provided comments to the committee on bills that would amend the IG Act. The comments focused on how the proposed amendments would affect the Legislative Branch IGs. In addition, OALC reviewed and provided comments on the Agency's Directive on the Office of Workers' Compensation Programs.

GPO Management Challenges

GPO is well into its 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 our April 2007 Semiannual Report to Congress, the OIG provided management a list of issues we identified as most likely to hamper the Agency's efforts if not addressed with elevated levels of attention and resources. We update the management challenges in this report.

We continue to note the issue of a new headquarters facility for GPO. As previously reported, management has maintained for years that the current GPO facility is too large and antiquated and requires an extraordinary amount of financial resources to operate and maintain. Estimates for building upkeep costs during fiscal year (FY) 2008 exceed $35 million. The Agency proposed to Congress a plan for relocating to new facilities specifically sized and equipped for future requirements and more effectively able to meet the needs of its customers. Although the challenges associated with such a move will be significant for the Agency, Congress must still approve any relocation of GPO operations. Members of Congress have expressed interest in the issue and urged that the Agency continue its efforts toward approval. Limited movement in this regard has, however, taken place. The OIG has planned a review of the proposed move to ensure that plans are based on supported and documented economic assumptions and the Government's future interests are adequately protected. The information reviewed thus far supports significant cost savings.

GPO's Top 10 Management Challenges

1. Strategic Planning.
2. Management of Human Capital.
3. Improved Financial Management.
4. Continuity of Operations.
5. Internal Controls.
6. Security and Intelligent Documents.
7. Supporting Congressional Printing.
8. Information Technology and Systems (IT&S) Management.
9. Customer Service.
10. Acquisitions.

Our update of management challenges follows:

1. Strategic Planning. As previously noted, to realize and sustain the GPO Vision, each individual business unit within the Agency must develop and implement its own clear and succinct strategic plan that aligns with the GPO blueprint, *A Strategic Vision for the 21st Century*. We have urged that business units develop plans that cascade goals and objectives from the Agency's plan to achieve employee buy-in and keep transformation efforts on track. In the absence of clearly articulated plans, senior management cannot easily determine whether the business units are working together toward a common goal.

During this reporting period, GPO continued to make progress in its efforts to implement the spirit of the Government Performance Results Act (GPRA). Although not required to follow all the mandates of GPRA, Congress urged GPO to embrace its tenets. In that vein, the GPO Quality Assurance office helped the Agency stay on point in achieving its 2008 goals and objectives by measuring and reporting its success through its Balanced Scorecard (BSC). The Agency's BSC is the framework that helps translate its strategy into operational objectives. To that end, work is nearly complete on GPO's Strategic Performance Plan and Achievements, which reports Agency achievements in meeting its goals and outcomes. Building on its successful performance measurement program, GPO has set its sights on rolling out an employee initiative during FY 2009 that will educate employees on its strategic posture and BSC. We are encouraged that management has made strategic planning a priority. Continued progress will help transformation efforts stay on track during this critical transition time.

2. Management of Human Capital. We previously highlighted challenges GPO 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 will continue confronting significant issues related to transformation of the GPO workforce 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.

During this reporting period, 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 diversity program, improvements can be made toward enhancing diversity of the Agency's corps of senior-level employees. The results of this audit are discussed in more detail in the Audits and Inspections section of this report.

The results from the GPO Employee Survey released in 2006 show that while job satisfaction is relatively high, "communications at GPO" stand out as not having improved since 2004. When compared against results from the 2004 Federal Human Capital Survey, GPO actually rated lower in almost all identical items. Human Capital has, however, developed a plan addressing those and other challenges as well as providing opportunities for improving communications at GPO.

In previous reporting periods and particularly during this last reporting period, management has implemented several programs that have greatly improved communications with all GPO employees. For example, during this reporting period the Employee Communications Office (ECO) implemented the *link* program, which uses NetPresenter software to disseminate GPO-related information to all GPO workstation PCs (via screen savers) as well as to flat screen monitors located throughout GPO buildings. ECO will use *link* to supplement its existing lines of communications with employees, such as email communications (GPO Headlines, Leaders' Update) and 'webbies' (content on the Intranet homepage). Thus, we no longer consider this issue a significant management challenge.

3. Improved Financial Management. GPO has been migrating 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 will provide GPO with integrated and flexible tools that will help successfully support business growth and customer technology requirements for products and services. To oversee and support such a complex effort, the GPO Oracle Program was created. Although investment in the integrated system presents opportunities for enhanced efficiency and cost savings, such an investment brings with it significant risk in the event the system does not meet user requirements. GPO must implement the program on time, within budget, and with a satisfactory result.

The OIG continued Independent Verification and Validation (IV&V) activities associated with implementation of the Oracle E-Business suite. IV&V provides GPO with an independent assessment of project status, satisfaction of user needs, and project cost effectiveness. During FY 2008, IV&V focused on the Oracle Release 2 project. The main goal of Release 2 is to implement Project Costing and Project Billing. Additional capabilities will be added to Purchasing, Inventory, Accounts Payable, Receivables, and other implemented Oracle modules. The IV&V resulted in several recommendations designed to improve management of the project as well as future Oracle projects. Management concurred with each recommendation and proposed responsive corrective actions. IV&V efforts for Release 2 will continue into FY 2009.

The OIG also continues to oversee activities of KPMG LLP (KPMG), the Independent Public Accountant (IPA) conducting the annual financial statement audit. KPMG is auditing the GPO FY 2008 consolidated financial statements and assessing the status of the FY 2007 findings to determine whether they will need to be reported again in the FY 2008 audit report. The results of the FY 2008 audit will be reported during the next reporting period.

4. Continuity of Operations (COOP). A previous OIG review of GPO COOP planning revealed that the Agency may not be adequately prepared to deal with a significant event such as a natural or man-made disaster. Our report contains several recommendations including, most fundamentally, that GPO adopt planning requirements and critical elements identified in Federal Preparedness Circular 65, "Federal Executive Branch Continuity of Operations." Management must address the problem of continuing essential functions and be able to resume normal operations within a time frame acceptable to its customers and business partners.

In response to our recommendations, GPO developed a comprehensive draft COOP plan based on the Federal Emergency Management Agency template of key COOP components. The draft 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 for emergencies and discusses known or anticipated categories of emergencies.

Steps continued to be taken during this reporting period to enhance the Agency's COOP posture, including planning and conducting exercises with scenarios that tested alternate production facilities and procedures for notifying essential personnel. The Agency has prepared and begun testing a COOP project completion matrix that will demonstrate what GPO can do to support mission essential functions in the event of COOP activation. The Agency also recruited and hired a business continuity manager to work directly with GPO's various business units in support of the COOP program.

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. Practically 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 that KPMG conducts also addresses internal controls 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)[1] No. 112, "Communicating Internal Control Related Matters Identified in an Audit." SAS No. 112 establishes standards and provides guidance on communicating matters related to an entity's internal control over financial reporting identified in a financial statement audit. The standard requires that the auditor communicate control deficiencies that are "significant deficiencies" and "material weaknesses."

KPMG is auditing the Agency's FY 2008 consolidated financial statements and assessing the status of FY 2007 findings that included several deficiencies related to internal control over financial reporting. Those deficiencies included (1) inadequate reconciliation controls, (2) misapplication of generally accepted accounting principles, and (3) information technology (IT) general controls. KPMG did not consider any of those deficiencies to be material weaknesses.

6. Security and Intelligent Documents (SID). As the Federal Government's leading provider of secure credentials and identity documents, management regards SID as a business unit best exemplifying the Agency's transformation toward high-technology production. During FY 2008, SID successfully manufactured more than 23 million electronic passports for the Department of State and established a new, secure smart card credential center to support the Department of Homeland Security's Customs and Border Patrol (DHS/CBP) Trusted Traveler Program (TTP). Also in FY 2008, to provide a COOP capability for passport production, the Agency successfully established a second secure manufacturing site at a renovated facility on the Stennis Space Center in Mississippi.

As a provider of secure Federal e-Credentials, SID worked with DHS/CBP to design, produce, secure print, personalize with laser engraving, mail, and fulfill the orders for

[1] Auditing standards promulgated by the Auditing Standards Board of the American Institute of Certified Public Accountants.

border crossing cards. The Trusted Traveler program provides expedited CBP processing at Canada and Mexico border crossings for people who have undergone background checks. The program maintains three databases of traveler information, and each has its own intelligent ID card that contains a radio frequency chip for remote reading. The programs are Nexus, for travel between the United States and Canada; Secure Electronic Network for Travelers Rapid Inspection (SENTRI), for use on the U.S./Mexico border; and Free and Secure Trade, for approved commercial truck drivers traveling between the three countries.

SID made the smart card program possible by reaching two critical milestones. First, SID established a secure e-Credential production capability. It selected an experienced integrator that could provide a turnkey solution for the personalization functions of the program, including all necessary equipment, systems, and technical support services.[2] The personalization equipment and system configured for GPO enables the Agency to offer a broad range of e-Credential capabilities. Second, DHS/CBP requisitioned from GPO hundreds of thousands of secure Trusted Traveler Cards

During FY 2008, SID successfully manufactured more than 23 million electronic passports for the Department of State and established a new, secure smart card credential center to support the Department of Homeland Security's Customs and Border Patrol (DHS/CBP) Trusted Traveler Program (TTP).

Although other concerns received attention, several matters must continue as a priority for management. Although GPO and the Department of State finalized a Memorandum of Understanding in December 2007, management needs to continue to address technology as well as data security related to the electronic passport, inventory volume, and storage of blank passport books. During FY 2008, we assessed the operating system security of the Passport Printing and Production System (PPPS). We recommended several steps that would improve security and integrity controls. During FY 2008, we also initiated an audit of database security for that system.

Finally, GPO faces the challenge of deploying its own Homeland Security Presidential Directive 12 (HSPD-12) infrastructure and issuance of identity credentials to employees and contractors. The overall responsibility for a GPO-wide HSPD-12 Program lies with GPO's Chief Management Officer and Security organizations. SID designs, prints, personalizes, and distributes the card. While not legally required to comply with HSPD-12, we continue to recommend that the Agency strive toward voluntary compliance. To that end, several control objectives are critical for meeting the security, efficiency, fraud prevention, and privacy protection goals that HSPD-12 requires and the Agency must maintain throughout the lifecycle of deployment.

Whatever its intentions, the Agency should employ the best practices established by HSPD-12 and begin addressing several of the control objectives, including separating duties for registering and issuing credentials; using original identity source documents; using appropriate background investigations; and using smart cards as person-identity-verification credentials. The OIG will continue to monitor Agency efforts regarding internal deployment of HSPD-12 and conduct audits as necessary for Agency compliance with Federal Information Processing Standards Publication 201, "Personal Identify Verification of Federal Employees and Contractors."

7. Supporting Congressional Printing. In a previous reporting period, we noted that the Joint Committee on Printing expressed concerns to management that apparently stem from late deliveries of printed versions of legislative documents the House of Representatives and Senate require. Reported reasons for the late deliveries included changes in staffing, reorganization of the workforce, use of use-or-lose leave during critical times, and various IT matters. During this reporting period, management has, as in our last reporting period, consistently produced and delivered congressional products on time. We therefore no longer consider this issue a significant management challenge.

8. Information Technology and Systems Management. As GPO transforms from an ink-on-paper operation to a highly efficient and secure multimedia digital

[2] The equipment and processes are operated exclusively by GPO employees, and the integrator now provides consulting services.

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, provide GPO with 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 Agency ability to respond to customer needs and must be replaced. In FY 2008, IT&S completed a 5-year strategy that should help guide the Agency through implementation of new systems and retirement of legacy systems. In FY 2009, FDsys, human resource systems, and certain Oracle E-Business modules are scheduled to be operational.

Because GPO provides services to Executive Branch agencies who 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 the overall information security program, including critical systems. We conducted a follow-on FISMA assessment in FY 2008. We also conducted the annual 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.

As the Agency fulfills its mission in the vital arena of electronic information dissemination and E-Government, GPO established a PKI that will serve the needs of the Agency, its legislative branch partners, and other Federal partners.[3] The PKI is cross-certified with the Federal Bridge Certificate Authority—a substantial and necessary step toward using PKI for the 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 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. Finally, the OIG will continue to lead IV&V activities associated with the ongoing implementation of the Oracle E-Business Suite and implementation of FDsys.

9. Customer Service. As the Agency moves closer to its goal of transforming to a 21st Century information processing and dissemination operation, customer services for GPO must reflect and advance that transformation. To ensure success in the future, management must maintain the appropriate focus, staffing, and alignment with its 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 to—not because they must. Transformation of the traditional GPO customer relationship requires a continuing evolution toward state-of-the-art customer relations management.

10. Acquisition. The OIG continues to be concerned with the Agency's ability to efficiently and effectively acquire the high-technology goods and services necessary for transforming the Agency. Acquisitions such as FDsys and the upcoming e-Passport procurement require a professionally trained contracting workforce skilled at carrying out nontraditional acquisitions. In addition, in concert with the Public Printer's Sustainable Environmental Stewardship initiative, the Agency must be able to navigate the acquisition rules to determine how best to promote this initiative through every product it buys and provides for its customers.

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


UNITED STATE
GOVERNMEN
PRINTING OF

Office of Audits and Inspections (OAI)

OAI, as required by the IG Act, conducts independent and objective performance and financial audits relating to GPO operations and programs, and oversees the annual financial statement audit an IPA firm under contract performs. OAI also conducts short-term inspections and assessments of GPO activities that generally focus on issues limited in scope and time. All OIG audits are performed in accordance with generally accepted government auditing standards (GAGAS) 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 seven new audit and assessment reports. Those 7 reports contained a total of 16 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, 2008, 39 recommendations were open.

B. TeamMate Audit Software Implementation

OAI continued its implementation of TeamMate audit software during this reporting period. TeamMate automates the entire workpaper process, including preparation, review, report generation, and global issue tracking, and OAI will use the program to increase the efficiency and productivity of the entire audit process including risk assessment, scheduling, preparation, review, report generation, and global issue tracking. TeamMate was originally designed for all types of audits, including compliance, contract, controls, efficiency and regulatory reviews, financial, government, IT, investigations, procedural, and security. OAI has successfully begun using TeamMate for new audit assignments.

C. External Peer Review of the Board of Governors of the Federal Reserve System

Section 3.55 of the GAGAS requires that each audit organization performing audits or attestation engagements have an external peer review performed by reviewers independent of the audit organization being reviewed at least once every three years.

The elements of quality control are described in GAGAS. A quality control system encompasses the organizational structure as well as the policies adopted and procedures established to provide reasonable assurance of conforming with GAGAS. The design of the system, and compliance with it in all material respects, are the responsibility of the audit organization. The objective of the external peer review is to determine whether the internal quality control system was adequate as designed and complied with to provide reasonable assurance that applicable auditing standards, policies, and procedures were met.

The OIG conducted an external peer review of the Board of Governors of the Federal Reserve System's Inspector General Audit Organization (Board OIG) for the 18-month period ending March 31, 2008. We conducted our review in accordance with the guidelines established by the PCIE and ECIE and rendered an unqualified opinion on the Board OIG's audit quality control system in effect for the 18-month period ending March 31, 2008.

D. Future Digital System – Independent Verification and Validation

The FDsys will be a comprehensive information lifecycle management system that will ingest, preserve, provide access to, and deliver content of all 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. It will have 6 clusters (Content Management, Content Preservation, Content Access, Content Delivery, Content Submission, and Infrastructure), which comprise 25 or more functional areas. A multiyear, multirelease integration effort will be used to design, procure, develop, integrate, and deploy selected technologies and components of FDsys.

During the last reporting period, GPO reorganized the FDsys Program with respect to GPO and contractor participation and responsibilities. The reorganization reduces contractor tasking and increases GPO efforts.

GPO is now managing development, integration, and deployment of FDsys. A contractor is developing the actual FDsys software and support procurement and installation of the system hardware.

The OIG is responsible for IV&V work associated with developing and implementing FDsys. We contracted with American Systems[4] to conduct the evaluations. American Systems has extensive IV&V experience with the Federal sector, and IV&V work will 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 – IV&V activities regarding the cost, schedule, and risk associated with development and implementation to evaluate overall program management effectiveness.
- Technical – IV&V activities regarding the resources, system requirements, architecture and design documents, and other critical deliverables associated with FDsys development and implementation.
- Testing – IV&V activities regarding the Design Validation Test Plan and test efforts performed by the implementation team to verify the adequacy and completeness of testing activities.

In Section G, we discuss our report resulting from these IV&V efforts, which are ongoing and will continue throughout the life of the project.

FDsys is being implemented through a series of releases, with each release building upon the features of the previous. During this reporting period, our IV&V team performed a gap analysis to determine the differences between the original plan for development of FDsys known as R1C and the current plan to deploy R1C2[5] in December of 2008. The gap analysis revealed that R1C2 has significantly less functionality than R1C and that R1C2 is costing more and taking longer to deploy, while providing less functionality and less data.[6] Specifically:

- The estimated cost to complete R1C2 exceeds the anticipated cost of R1C by $8 million ($24 million for R1C2 versus $16 million for R1C). An additional $10 million is the estimate to complete all the original R1C.
- The planned completion date for R1C2 is a year and a half after the original date for R1C (December 2008 for R1C2 versus June 2007 for R1C). An additional year is the estimate to complete all of R1C.
- The amount of data available for the R1C2 deployment will be significantly less than was planned for R1C (as measured by document collections, 8 to 10 collections for R1C2 versus 55 collections planned for R1C). There is no estimate for when the remaining collections will be made available.

E. Oracle Release 2 – Independent Verification and Validation

GPO is implementing the Oracle E-Business Suite in a series of phased releases with incremental functional capabilities. GPO has completed some early implementation start-up projects to become familiar with Oracle technology and work processes and to develop successful project implementation skills. The current project, Release 2, is implementing the Oracle Projects module, which consists of project costing and project billing. Other capabilities will be added to Purchasing, Inventory, Accounts Payable, Receivables, and other implemented Oracle modules.

The OIG will oversee IV&V work associated with implementation of the Oracle E-Business Suite. We contracted with Noblis[7] to conduct the IV&V evaluations. Noblis has extensive IV&V experience with the Federal sector. Our IV&V work noted that the Release 2 project has had some difficulties associated with requirements gathering and "to-be"

[4] American Systems, located in Chantilly, Virginia, is a large IT company with significant experience in the realm of IV&V for Federal civilian and Defense Agencies, including the Department of State, the Navy, and the U.S. Agency for International Development.

[5] The original targeted first public release of FDsys R1C has now been divided into three releases: R1C2 in late 2008, R1C3 in mid-2009, and R1C4 in late 2009.

[6] Our gap analysis does not separate costs or performance associated with the time periods before and after the reorganization of the FDsys program.

[7] Noblis, located in Falls Church, Virginia, is a nonprofit science, technology, and strategy organization that helps Federal and private sector clients solve complex systems, process, and infrastructure problems.

process definitions. However, steps have been taken to remedy many of the weaknesses. In Section G, we discuss our report resulting from these IV&V efforts, which are ongoing and will continue throughout the life of the project.

F. Financial Statement Audit Activity

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG is conducting the audit under a multi-year contract for which the OAI provides oversight as the Contracting Officer's Technical Representative (COTR). OAI also assists with facilitating the external auditor's work as well as reviewing the work performed to ensure it complies with GAGAS. 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 2007 consolidated financial statements, stating that its financial statements were presented fairly, in all material respects, in conformity with generally accepted accounting principles. KPMG identified three significant deficiencies for FY 2007: (1) inadequate reconciliation controls, (2) misapplication of U.S. generally accepted accounting principles, and (3) general IT controls. KPMG made recommendations addressing each deficiency and GPO management concurred with the recommendations.

KPMG is currently auditing GPO's FY 2008 consolidated financial statements and assessing the status of the FY 2007 findings to determine whether they will need to be reported again in the FY 2008 audit report, along with potentially new findings and recommendations.

G. Audit and Inspection Reports

1. Assessment Report 08-07 (Issued May 30, 2008)

Protection of E-Passport Production System (PPPS)

The PPPS includes various computer applications and operating systems that support production of passports. GPO's Plant Operations Division administers PPPS computer applications while the GPO Chief Information Officer (CIO) is responsible for administering PPPS operating systems. While performing a security audit of databases that support the PPPS hosted in Washington D.C., the OIG identified an issue related to protection of the e-Passport network and related computers. We issued a separate sensitive report containing recommendations that would help further strengthen controls over PPPS. Management took prompt corrective action to implement the recommendation.

While performing a security audit of databases that support the PPPS hosted in Washington D.C., the OIG identified an issue related to protection of the e-Passport network and related computers.

2. Assessment Report 08-08 (Issued August 8, 2008)

Federal Digital System Independent Verification and Validation – Third Quarter Observations and Recommendations

As noted above, the OIG contracted with American Systems, a company with significant experience in the realm of IV&V for Federal civilian and Defense agencies, to conduct IV&V for the public release of FDsys. As part of its contract, the contractor is assessing the state of program management, technical and testing plans, and other efforts related to this public release. The contractor is required to issue to the OIG a quar-

terly 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. Additionally, at the end of each FDsys release phase, the contractor is required to issue a release phase summary program management report that addresses delivery of the technical baseline according to the FDsys Master Program Schedule and the risks that affect the schedule's critical path to the next phase.

During this reporting period, the Agency implemented a reorganization of the Government and contractor participation and responsibilities as well as implemented a new design for FDsys. According to GPO officials, the primary reason for the reorganization was management's dissatisfaction with contractor performance. Although the OIG's first quarterly report identified various weaknesses in program management practices the contractor used for the Release 1.B pilot system, our IV&V contractor was not tasked to investigate or evaluate the reasons behind GPO's decision to reorganize the program, and accordingly did not render an opinion on the reorganization. The contractor was, however, responsible for informing the OIG of the risks the FDsys program faces at the end of each quarter.

This third quarter report contains findings and recommendations that further strengthen management of the FDsys program and management's response to those recommendations. Management concurred with each of the recommendations and either took or proposed responsive corrective actions.

3. Audit Report 08-09 (Issued August 8, 2008)

Follow-up Audit of Centrally Charged Travel Expenditures

GPO has an agency account with MasterCard through the Bank of America (BoA) for the centralized charging and billing of various common travel expenditures. The agency also has contracted with National Travel Services, Inc. (NTS) to provide assistance to GPO travelers in making travel arrangements including airline, rail, hotel, and rental car reservations. A previous OIG audit of centrally charged travel expenditures conducted in May 2006 concluded that controls were not effective over (1) travel fares charged to the GPO's Agency MasterCard account and (2) service fees charged directly to GPO.

The May 2006 audit identified approximately $32,000 in travel fares and service fees associated with travel by GPO employees during FY 2005 that could not be reconciled with official travel records. The audit also found that before authorizing monthly payments to BoA, the Agency/Organization Program Coordinator did not verify that travel fares and NTS service fees charged to the Agency MasterCard account were for actual travel expenses. The OIG recommended that the:

- GPO Chief Financial Officer (CFO) eliminate use of the Agency MasterCard account for airline and rail tickets and direct that NTS charge tickets to either the individual GPO traveler's Government-issued MasterCard or personal credit card.
- The GPO CFO direct NTS to charge service fees to each individual GPO traveler's Government-issued MasterCard or personal credit card.

Management concurred with the recommendations and agreed to implement corrective actions. The OIG subsequently performed this follow-up audit to determine whether recommendations made in the May 2006 audit were effectively implemented. The follow-up audit showed that although management implemented changes in policy addressing the recommendations, problems similar to those identified in our May 2006 audit continued. For example, throughout almost all of FY 2007, the GPO Travel Manager authorized payments to BoA of approximately $96,512 for travel fares and service fees for 147 employees whose expenses were charged to the Agency MasterCard account—despite the fact that 36 (24 percent) of those employees had a Government-issued MasterCard. Charging fares and fees to the wrong account continued because ineffective controls hampered the GPO Travel Manager from identifying questionable charges for travel fares and service fees NTS makes through the Agency MasterCard account with BoA. Because the controls were ineffective, monthly invoices to BoA for the Agency MasterCard account were not reconciled to travel vouchers.

Reconciliation would have verified whether travel fares and service fees NTS billed through BoA were accurate, were actually incurred for official business, and

complied with Agency policy. Because reconciliations did not take place, the GPO Travel Manager was not able to determine that NTS charged $24,233.61 in travel fares and service fees to the Agency MasterCard account for 56 trips taken by the 36 employees who possessed a Government-issued MasterCard. Adding to that condition, 14 employees subsequently submitted travel vouchers requesting reimbursement for travel fares and service fees charged to the Agency account. We identified approximately $8,495 that GPO can recover because of erroneous payments.

A total of three recommendations were made to further strengthen management of GPO travel expenditures. Management concurred with each recommendation and implemented responsive corrective actions.

"Everyone in the workplace should be afforded the opportunity to develop, perform, and advance to their maximum potential based solely on their merit and without regard to race, color, religion, national origin, gender, age, disability, or sexual orientation."

Testimony on GPO's Diversity Management Programs by J. Anthony Ogden, Inspector General, before the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia on September 16, 2008.

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

Diversity Management Programs at GPO

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 Subcommittee requested that the OIGs of each Legislative Branch Agency assess the programs the diversity offices have in place to address diversity concerns.[8] The objectives of the audit were to review diversity within GPO, specifically to:

- Identify and assess the diversity program at GPO to determine if it is yielding the desired results—that of creating a more diverse population of women and minorities in top leadership positions, specifically the Senior Level Service (SLS).[9]
- Evaluate the accuracy and completeness of the complaints and discrimination data reported to Congress.
- Assess the degree to which diversity offices or functions are independent of the General Counsel and the Public Printer.

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, prior to this audit commencing, senior officials at GPO began adopting some elements of both EEOC Management Directive-715 (MD-715) and the leading diversity management practices identified by the Government Accountability Office (GAO).

In addition, GPO has made progress in developing its pool of Grade 15s (PG-15s) to ensure a qualified minority pool for the Agency's SLS.[10] However, improvements can be made toward enhancing diversity of the Agency's corps of SLS employees. The audit also showed that GPO complaints and discrimination data reported to the EEOC during FY 2007 and eventually reported to Congress were accurate and complete. Finally, although diversity management programs are incorporated in the Affirmative Employment Program Division of the EEO Office, the Director of EEO is independent of the General Counsel, and to a certain extent independent of the Public Printer in EEO matters.

Opportunities exist for GPO to develop a more diverse population of qualified women and minorities in top leadership positions. We made two recommendations to management: 1) incorporate the remaining essential elements of MD-715 and 2) implement the nine leading practices for diversity management

[8] Other legislative branch agencies include the Library of Congress, Government Accountability Office, Architect of the Capitol, and the Capitol Police.

[9] SLS is the GPO equivalent to the Senior Executive Service (SES).

[10] At GPO, a Printing Office Grade (PG) 15 is the senior most grade and is generally equivalent to the General Schedule Grade 15 classified by the Office of Personnel Management. Positions at GPO above Grade PG-15 are in the SLS.

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

5. Assessment Report 08-11 (Issued September 18, 2008)

WebTrust Assessment of GPO's Certification Authority – Attestation Report

GPO 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, whose certification provisions require that the GPO PKI undergo an annual independent compliance review. To satisfy this compliance requirement, the GPO OIG tasked an IPA firm to conduct a WebTrust assessment of its Certification Authority (CA). The assessment was conducted in accordance with the American Institute of Certified Public Accountants (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 are fairly stated based on underlying principles and evaluation criteria.

From July 1, 2007, through June 30, 2008, the IPA issued an Attestation Report expressing its unqualified opinion that the GPO management assertion related to its CA operations was in all material respects fairly stated based on the AICPA WebTrust for Certification Authorities criteria. The report is sensitive.

IPv6 is a developing Internet protocol which will provide many benefits such as more Internet addresses, higher qualities of service, and better authentication, data integrity, and data confidentiality.

6. Assessment Report 08-12 (Issued September 30, 2008)

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

The OIG assessed Agency planning for the 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 which will provide many benefits such as more Internet addresses, higher qualities of service, and better authentication, data integrity, and data confidentiality.

OMB recently announced that all Executive Branch agencies met a June 30, 2008, deadline for successfully demonstrating IPv6 capability of network backbones. While GPO was not required to meet the OMB deadline, IPv6 capability provides certain benefits to GPO as industry provides products and services that are IPv6-enabled.

The OIG assessment identified that GPO plans to transition to IPv6 as part of a broad acquisition plan that will update its IT infrastructure. Specific target dates for these updates have not been finalized. The OIG believes that the planned transition is an effective long-term approach. In the short term, GPO should consider implementing the minimum IPv6 requirement, which should ensure that resources such as FDsys are capable of ingesting information from IPv6 sources. Two recommendations were made to management to enhance planning for the IPv6 transition. Management concurred with each of the recommendations and has either taken or planned responsive corrective actions.

7. Assessment Report 08-13 (Issued September 30, 2008)

Oracle E-Business Suite Release 2 Independent Verification and Validation – Program Management

The OIG contracted with a nonprofit science, technology, and strategy organization to conduct IV&V of the GPO

Oracle Program's E-Business Suite Release 2 implementation. The overall objective of IV&V is to determine whether system implementation is consistent with the Oracle project plan and cost plan, and whether the delivered system meets GPO requirements. The contractor is tasked with assessing program management, technical, and testing activities associated with the Release 2 implementation and required by the contract to issue a monthly program risk assessment as well as summary reports for program management, technical, and testing IV&V.

This first report is the summary report on Oracle Release 2 program management. Program management IV&V focuses on activities that define and shape the program and projects that support them. As part of program management IV&V, the IV&V contractor analyzed program and project schedules, development processes (for example, change management, issue tracking, and risk management approaches) and conducted risk analyses. The report contained four recommendations designed to strengthen current and future Oracle program management efforts. Management concurred with each of the four recommendations and has either taken or proposed responsive corrective actions.

H. Status of Open Recommendations

Management officials made significant progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. For the 39 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 are limiting 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. Based on corrective action management took, we closed one recommendation when the final report was issued.

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 is working with management and monitoring implementation of the remaining recommendations.

2. Assessment Report 06-03 (Issued March 31, 2006)

GPO Oracle Program Stakeholder Analysis

FINDING

The assessment identified several vulnerabilities associated with the GPO Oracle Program and made recommendations that would help mitigate risks associated with those vulnerabilities. The vulnerabilities identified during the assessment included (1) top management support not aligned with program execution; (2) inadequate functional and technical staffing; (3) lack of a methodology for organizational restructuring; (4) lack of targeted performance metrics; and (5) lack of an effective method for managing program progress.

RECOMMENDATION

To help ensure the Oracle Program meets expectations of its stakeholders, the OIG made 13 recommendations in the areas of staffing, management alignment and organizational restructuring, use of performance metrics, and management of program progress.

MANAGEMENT COMMENTS

Management concurred with each of the report's

recommendations and agreed to take corrective actions throughout implementation of the project.

OIG COMMENTS

As of the end of this reporting period, six recommendations remain open. Management is continuing to work on implementing corrective actions. We anticipate that these recommendations will be closed upon implementation of Oracle Release 2.

3. Assessment Report 07-01 (Issued November 20, 2006)

Report on Early Oracle Implementation: Independent Verification and Validation

FINDING

The OIG initiated IV&V activities beginning with two of the early implementation projects for Oracle. The objective of IV&V is to provide GPO with an independent assessment of project status, satisfaction of user needs, and project cost effectiveness. The OIG issued a sensitive report summarizing vulnerabilities identified during the IV&V activities.

RECOMMENDATION

The report includes 21 recommendations to management for strengthening controls and mitigating risks associated with the vulnerabilities.

MANAGEMENT COMMENTS

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

OIG COMMENTS

Nine recommendations made in this report remain open. Management continues to work on implementing corrective actions.

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

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

FINDING

FISMA requires that each Executive Branch Agency develop, document, and implement an agency-wide program for providing information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[11] Although a legislative branch agency, the Agency has recognized 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 which, 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 is working on implementing corrective actions for the open recommendations. As part of the 2008 FISMA review, we reviewed management's progress in implementing the recommendations. We closed 4 of the 11 recommendations.

5. Assessment Report 07-10 (Issued September 28, 2007)

Report on Perimeter Security Assessment of a GPO Building

FINDING

The Federal Protective Service (FPS), an organization within the DHS, provides law enforcement and security services to the General Services Administration for federally owned and leased facilities. At the request of the OIG, FPS conducted a physical security assessment of a GPO building. The FPS methodology for assessing security in the GPO building included (1) identifying existing countermeasures at the facility, (2) identifying credible threats to the facility, and (3) rating each threat as to potential impact of loss and vulnerability. The sensitive report contains recommendations intended to enhance security of the building.

[11] Section 3541, title 44, United States Code.

RECOMMENDATION

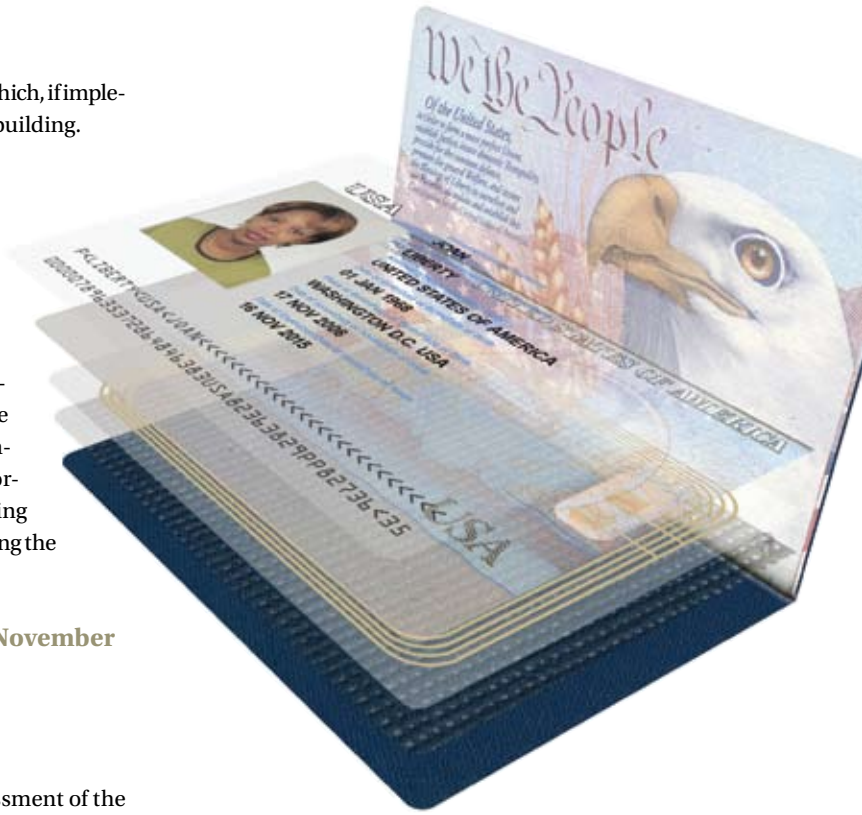
The report contains 12 recommendations which, if implemented, will help enhance security of the building.

MANAGEMENT COMMENTS

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

OIG COMMENTS

During this reporting period, management closed one of the remaining three open recommendations. Two recommendations remain open. With proposed corrective actions in place, we anticipate closing the remaining two recommendations during the next reporting period.



6. 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 audit 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 contained seven recommendations to 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. With proposed corrective actions in place, we anticipate closing the remaining two recommendations during the next reporting period.

7. Assessment Report 08-04 (Issued March 28, 2008)

Federal Digital System Independent Verification and Validation – First Quarter Observations and Recommendations

FINDING

The FDsys program is a multimillion dollar effort that

GPO is funding for modernizing information collection, processing, and dissemination capabilities it performs for the three branches of the Federal Government. The OIG is conducting IV&V of FDsys implementation through a contract with an IT company. Between July and September 2007, the contractor completed its initial assessment of the FDsys prime contractor's program management practices used for the Release 1.B pilot system. The initial IV&V assessment showed that the prime contractor established a strong basis for good program management practices for Release 1.B. We did, however, identify some weaknesses that could lead to schedule risk and cost overrun for Release 1.C if not addressed in a timely manner. Those weaknesses included the following areas.

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

RECOMMENDATION

The report contained 14 recommendations designed to strengthen management of the FDsys program.

MANAGEMENT COMMENTS

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

OIG COMMENTS

During this reporting period, we worked with management to close 8 of the remaining 11 open recommendations. We anticipate closing the remaining three recommendations during the next reporting period.

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

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

FINDING

The PPPS includes various computer applications and operating systems that support production of passports. The Agency's Plant Operations Division administers PPPS computer applications while its 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

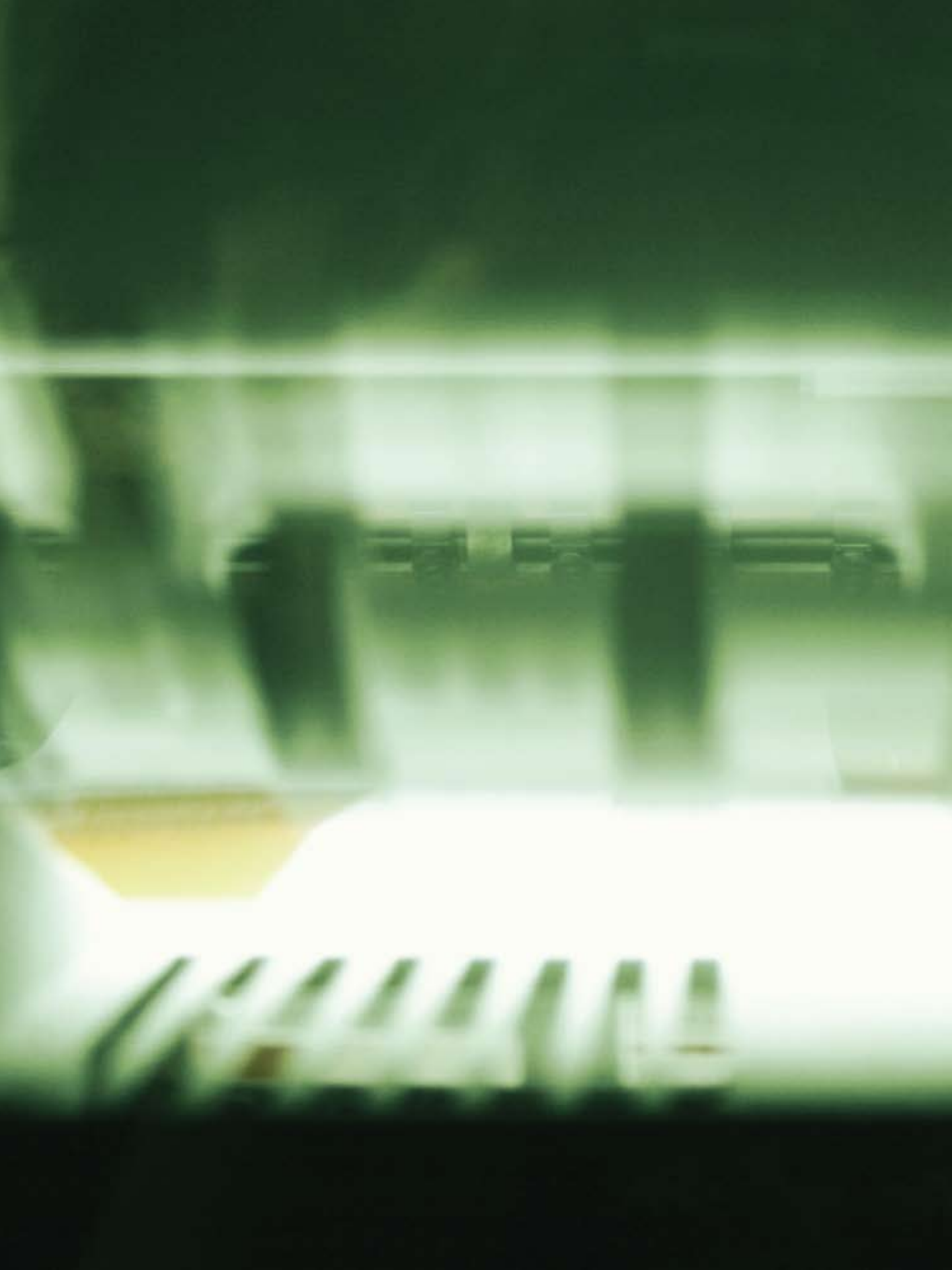
The OIG issued a sensitive report containing eight recommendations designed to not only help strengthen the security of the PPPS but also reduce the risk of system compromise.

MANAGEMENT COMMENTS

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

OIG COMMENTS

During this reporting period, all of the eight recommendations remained open.



Office of Investigations (OI)

The Office of Investigations (OI) conducts and coordinates investigations relating to alleged or suspected misconduct and monetary or material losses occurring in GPO programs and operations. The subjects of OI investigations can be contractors, program participants, management, or other Agency employees. Special Agents in OI are Federal Criminal Investigators. Investigators are also designated as Special Police Officers.

Investigations that uncover violations of Federal law or GPO rules or regulations may result in administrative sanctions, civil or criminal prosecution. Prosecutions may result in court-imposed prison terms, probation, fines, and restitution. OI can also issue Management Implication Reports, which identify issues uncovered during an investigation it believes warrant management's prompt attention.

A. Summary of Investigative Activity

During this reporting period and in response to 50 contacts, complaints, or allegations, OI opened 18 investigative cases and closed 20. OI has 22 ongoing investigations. During this reporting period, one investigation resulted in three criminal indictments, one other case was accepted for possible criminal prosecution, and one case against a contractor was forwarded to the agency for administrative action. In addition, two other workers' compensation investigations resulted in $245,289 in recoveries and $420,000 in cost savings over 10 years.

B. Types of Cases

OI investigative workload includes the following major categories:

Workers' Compensation Fraud

OI investigates GPO employees who allegedly submit false claims or make false statements to receive workers' compensation benefits. OI is working on three investigations involving possible fraudulent claims for workers' compensation.

Procurement Fraud

OI investigates allegations involving GPO contract service providers defrauding the Government in connection with procurement of goods and services. Violations generally include false claims, false statements, wire and mail fraud, product substitution, and Small Disadvantaged Business Program violations. OI has seven open cases involving alleged procurement fraud.

Employee Misconduct

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

Miscellaneous

OI investigates miscellaneous administrative allegations and other types of investigations that do not fall into one of the categories above. Examples of such investigations include theft of Government property, illegal hacking, or requests for investigations by other legislative agencies. OI has five open cases involving miscellaneous matters.

C. Status of Action on Referrals

OI investigative efforts result in both external and internal referrals for action.

External

OI referred eight investigative matters to the Department

of Justice for prosecution. Three GPO employees were indicted for the physical abuse of another employee. Prosecutorial action is pending in one civil and one other criminal matter.

Internal

Two investigative matters were referred to management for action and are pending.

D. Investigative Accomplishments

Workers' Compensation Fraud

An OI investigation resulted in a Department of Labor determination that an Office of Workers' Compensation Programs (OWCP) claimant—a GPO employee—made false statements from 2003 to 2007, claiming no earnings. The OI investigation revealed the employee owned rental property and that since 1998 had been acting as property manager, locating renters, collecting rents, and completing small repairs. A forfeiture of $226,821.74 was assessed, and the individual taken off OWCP rolls. A cost savings to the Government of $42,000 per year will also be realized ($420,000 in actuary amount over 10 years).

In addition, another OI investigation resulted in a Department of Labor determination that another GPO employee was overpaid $17,823 in workers' compensation benefits.

OI's continued proactive, investigative approach and its working relationship with the GPO Health Unit and the Office of Workers' Compensation has also resulted in keeping Agency Sick Injured Administrative costs under $20,000 per month.

A previous reporting period investigation of a GPO Central Office employee of alleged workers' compensation fraud resulted in forfeiture of $34,623.00 of the employee's compensation. During this reporting period, an appeal to that decision was decided in the Government's favor.

Employee Misconduct

An OI investigation involving allegations of the use of Government computers to view and download pornography was referred to management for action. During this reporting period, the employee was terminated from GPO employment for violations of Agency regulations on the use of Government computers and the Internet.

Procurement Fraud

OI investigated a GPO contractor for submitting false claims. The matter has been referred to the Office of General Counsel for possible suspension/debarment.

Another OI investigation, worked jointly with several other law enforcement entities, has revealed fraudulent purchase card transactions. This matter has been accepted for prosecution consideration and the investigation is ongoing.

Several other significant allegations concerning possible procurement fraud were also received by OI. Those investigations are ongoing and will soon be referred to the Department of Justice for prosecution consideration.

Miscellaneous

OI assisted the Library of Congress OI in a criminal investigation. In addition, at the request of another legislative agency, OI continues to investigate a criminal matter accepted by the Department of Justice's Office of Public Integrity for prosecution consideration.

E. 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.


PUBLIC PAPERS OF THE PRESIDENTS
William J. Clinton
2000–2001
II
PUBLIC PAPERS OF THE PRESIDENTS
George W. Bush
2002
I
UNITED STATES STATUTES AT LARGE
VOL. 117
PART 1, PP. 1–1072
PUBLIC LAWS
LSA
Federal Regulations
Weekly Compilation of Presidential Documents
THE UNITED STATES GOVERNMENT MANUAL 2005-2006
Federal Register

APPENDIX A: GLOSSARY AND ACRONYMS

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.

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
BoA	Bank of America
CA	Certification Authority
CCIG	Council of Counsels to the Inspector General
CFO	Chief Financial Officer
CIO	Chief Information Officer
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
DHS/CPB	Department of Homeland Security's Customs and Border Patrol
DMZ	Demilitarized Zone
ECIE	Executive Council on Integrity and Efficiency
FBCA	Federal Bridge Certification Authority
FDLP	Federal Depository Library Program
FDsys	Future Digital System
EEOC	Equal Employment Opportunity Commission
MD-715	EEOC Management Directive 715
FIPS-201	Federal Information Processing Standard Publication 201
FISMA	Federal Information Security Management Act
FPS	Federal Protective Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GPO	U.S. Government Printing Office
GPRA	Government Performance and Results Act
HSPD-12	Homeland Security Presidential Directive-12
IG	Inspector General
IG Act	Inspector General Act of 1978
IPA	Independent Public Accountant
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
IT&S	Information Technology and Systems
IV&V	Independent Verification and Validation
MIR	Management Implication Report
NTS	National Travel Services, Inc.
OALC	Office of Administrative/Legal Counsel
OAI	Office of Audits and Inspections
OEP	Occupant Emergency Plan
OI	Office of Investigations
OIG	Office of Inspector General
OWCP	Office of Workers' Compensation Programs
PCIE	President's Council on Integrity and Efficiency
PKI	Public Key Infrastructure
PPPS	Passport Printing and Production System
SAS	Statement on Auditing Standards
SID	Security and Intelligent Documents
SLS	Senior Level Service
TTP	Trusted Traveler Program

APPENDIX B: INSPECTOR GENERAL ACT REPORTING REQUIREMENTS

Inspector General Act Citation	Requirement Definition	Cross-Reference Page Number(s)
Section 4(a)(2)	Review of Legislation and Regulations	5
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	7–11 13–22
Section 5(a)(2)	Recommendations for Corrective Actions	13–22 25–26
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	19–22
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	25–26
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)	13–19
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	31
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	32
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	$347,247	$240,687	$587,394
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	1	$8,495
Reports for which a management decision made during reporting period		
■ Dollar value of recommendations agreed to by management	0	$8,495
■ 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

Audit Reports	Funds Put To Better Use
Report on Protection of E-Passport Production System (Assessment Report 08-07, issued May 30, 2008)	$0
Report on Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Third Quarter Observations and Recommendations (Assessment Report 08-08, issued August 8, 2008)	$0
Report on Follow-up Audit of Centrally Charged Travel Expenditures (Audit Report 08-09, issued August 8, 2008)	$8,495
Report on Diversity Management Programs at the Government Printing Office (Audit Report 08-10, issued September 11, 2008)	$0
Report on WebTrust Assessment of GPO's Certification Authority – Attestation Report (Assessment Report 08-11, issued September 18, 2008)	$0
Report on Assessment of GPO's Transition Planning for Internet Protocol Version 6 (Assessment Report 08-12, issued September 30, 2008)	$0
Report on Oracle E-Business Suite Release 2 Independent Verification and Validation – Program Management (Assessment Report 08-13, issued September 30, 2008)	$0
Total	$8,495

Table C-4: Investigations Case Summary

Total New Hotline/Other Complaints Received during Reporting Period	**50**
No Formal Investigative Action Required	37
Cases Opened by OI during Reporting Period	18
Cases Open at Beginning of Reporting Period	24
Cases Closed during Reporting Period	20
Cases Open at End of Reporting Period	22
■ Cases Referred to GPO Management	2
■ Cases Referred to Other Agencies	0
■ Cases Referred to OAI	0

Current Case Openings by Allegation	22	
■ Contract and Procurement Fraud	7	32%
■ Employee Misconduct	7	32%
■ Workers' Compensation Fraud	3	13%
■ Miscellaneous	5	23%

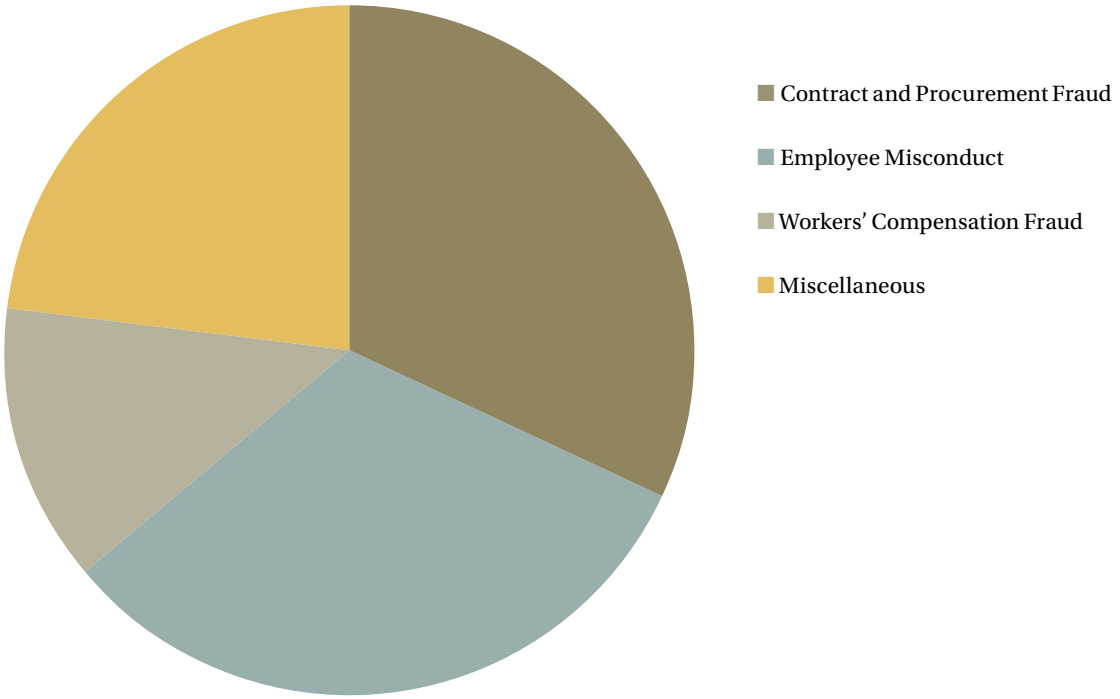


Table C-5: Investigations Productivity Summary

Arrests	0
Total Cases Presented to Prosecuting Authorities	9
Criminal	8
Criminal Declinations	4
Indictments	3
Convictions	0
Guilty Pleas	0
Probation (days)	0
Jail Time (days)	0
Restitutions	$0
Civil	1
Civil Declinations	1
Amounts Recovered Through Investigative Efforts	$245,289
Total Agency Cost Savings Through Investigative Efforts	$420,000
Total Administrative Referrals	0
Contractor Debarments	0
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions	3
Employee Terminations	1
Employee Warned/Other Actions	0
Other Law Enforcement Agency Referrals	0

Office of Inspector General

732 North Capitol Street, NW
Washington, D.C. 20401

202.512.0039
inspectorgeneral@gpo.gov
www.gpo.gov/oig

OIG HOTLINE 1.800.743.7574