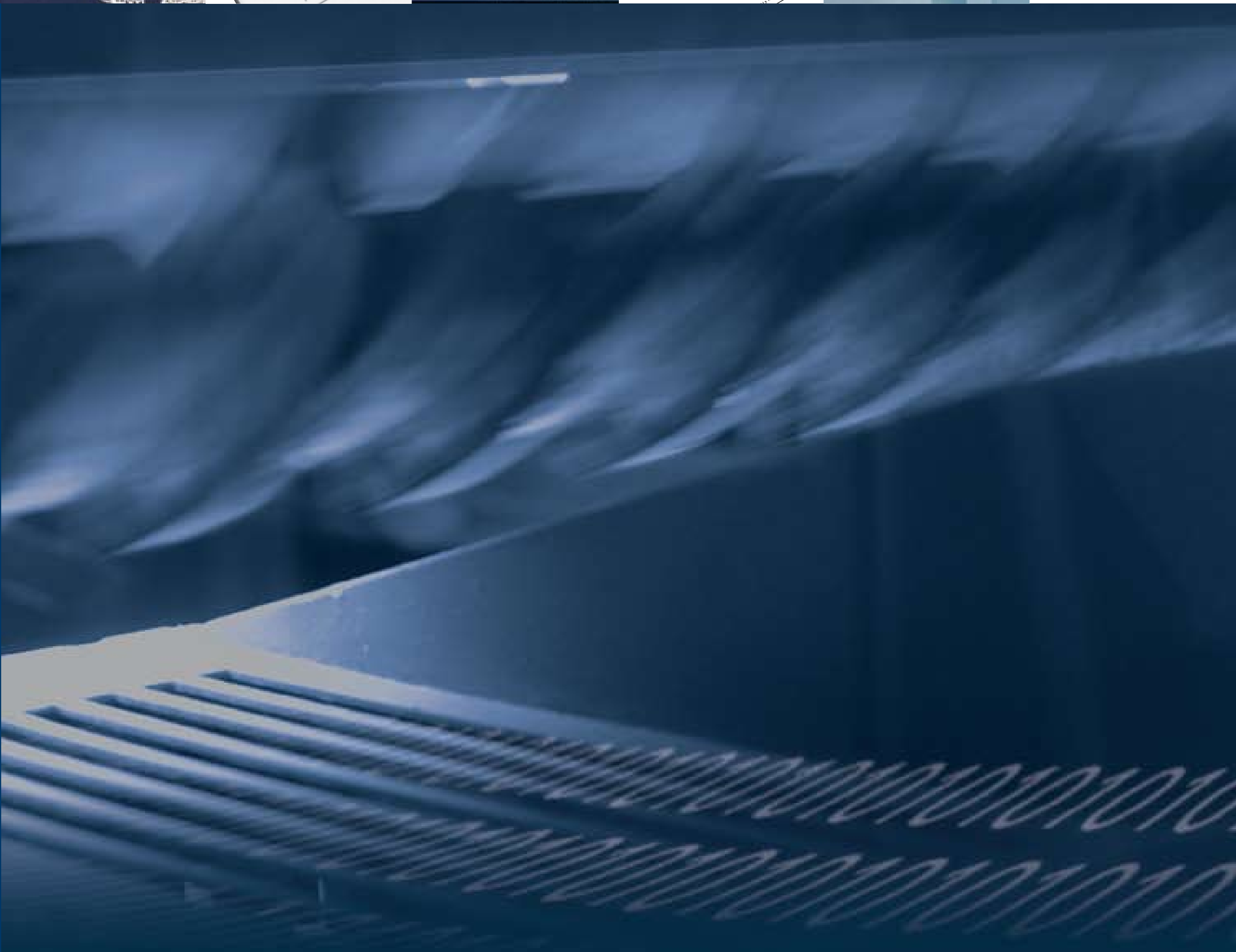


United States Government Printing Office | Office of Inspector General

SEMIANNUAL REPORT TO CONGRESS

October 1, 2007 through March 31, 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).

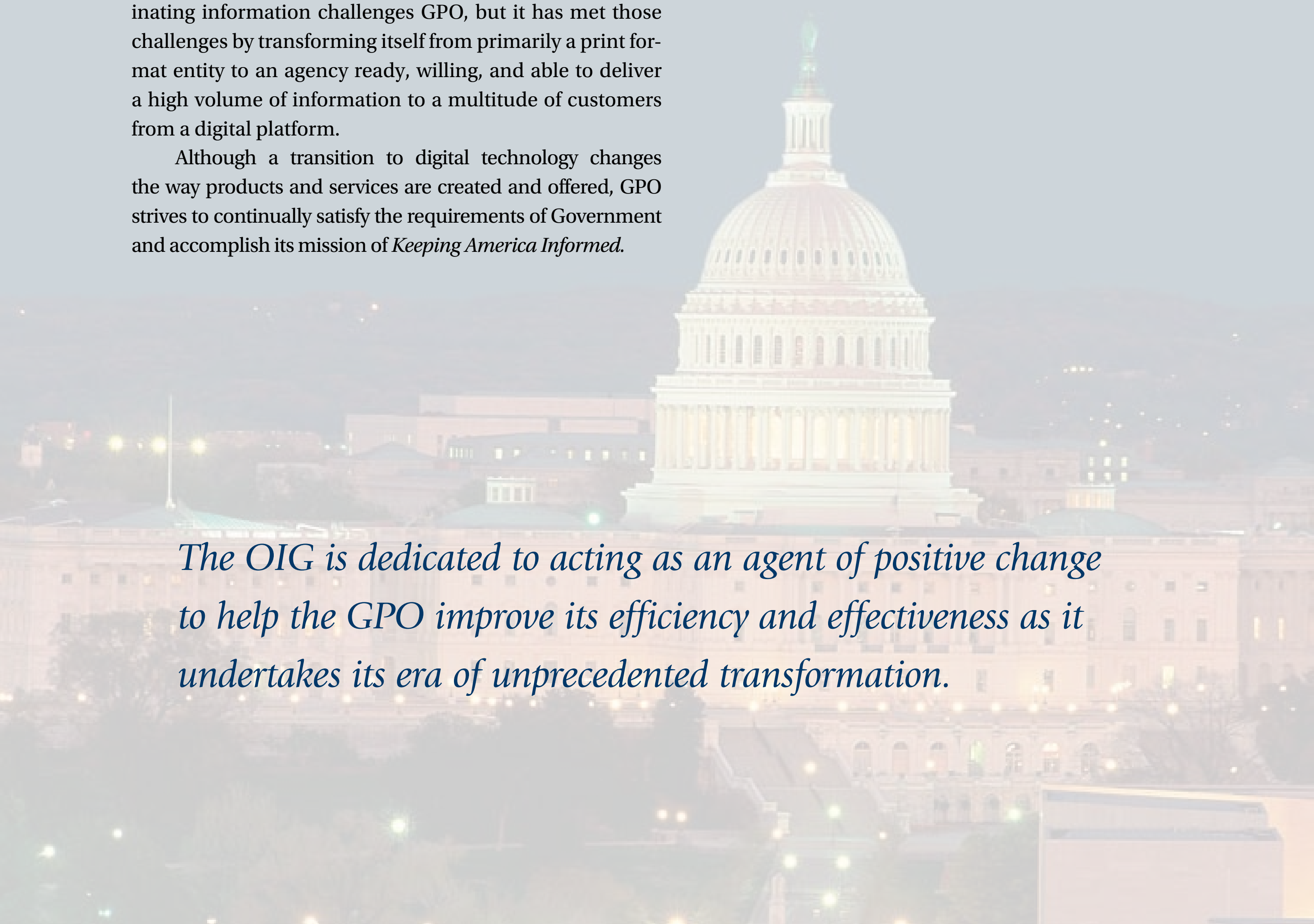
Today about half of all Federal Government documents begin as digital products and are published directly to the Internet. Such an evolution of creating and disseminating information challenges GPO, but it has met those challenges by transforming itself from primarily a print format entity to an agency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

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). The OIG at GPO 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 will promote economy, efficiency, and effectiveness in GPO programs and operations.

The 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. Along with keeping the Public Printer and Congress fully informed about problems and deficiencies, the OIG provides an independent and objective way of relating to administration and operations of the Agency. To accomplish that, the OIG conducts audits, assessments, investigations, inspections, and other reviews.



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

Contents

Message from the Inspector General

During this reporting period, the Government Printing Office (GPO) Office of Inspector General (OIG) continued its focus on critical Agency operations such as passport production, the implementation of Oracle business products, and the Future Digital System (FDsys)— programs fundamental to GPO's success. We continue to make critical programs a priority as project management challenges are inherent in highly technology-driven efforts. Working with management to identify risks and vulnerabilities early on will hopefully help the agency avoid serious problems.

Last fall, the Government Accountablity Office (GAO) reported at least 227 IT projects valued at approximately $10.4 billion in fiscal year 2008 as being poorly planned, poorly performing, or both.[1] While GPO's programs are not among the list, the GAO report reminds us of the importance of effective project management and its integral role in successful capital acquisition. Our office will continue to focus on these issues and work with management in facilitating an enterprise approach to address our recommendations.

The OIG remains committed to the integrity, accountability, efficiency, and effectiveness of GPO programs and operations and our audits, inspections, investigations, and other activities highlighted in this report demonstrate such an ongoing commitment. The Office of Audits and Inspections (OAI) continued its focus on several important technology initiatives critical to the ongoing operations of GPO. Those initiatives included a network vulnerability assessment, review of the passport production operating system, and Independent Verification and Validation (IV&V) of the Agency's FDsys. In addition to those projects, OAI oversaw the annual financial statement audit of GPO as well as completed its review of the new secure printing facility for passport production in Mississippi.

Our Office of Investigations continued with its efforts to not only combat workers' compensation fraud but contract and procurement fraud as well. Those efforts were recognized at the highest level when the President's and Executive Councils on Integrity and Efficiency recognized Special Agents Sonja Scott and Hugh Coughlin with Awards for Excellence. I am proud of their efforts and contribution to the OIG at GPO.

Our dedicated staff will continue to promote efficiency, and combat waste and fraud, and we look forward to working with management in this endeavor.

J. Anthony Ogden

J. Anthony Ogden
INSPECTOR GENERAL
U.S. Government Printing Office

[1] Government Accountability Office, "Information Technology: Further Improvements Needed to Identify and Oversee Poorly Planned and Performing Projects," GAO-07-1211T.

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 6 reports with a total of 35 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency. OAI also continued working with management to close recommendations from earlier reporting periods.

The Office of Investigations (OI) opened 17 new investigative cases in response to 417 complaints or allegations and closed 21 matters. Through its investigative efforts during this period, GPO may realize a future savings $44,800 a year ($448,000 in actuary amount over 10 years) if the subject of an Office of Workers' Compensation fraud investigation is taken off the rolls. Management responded to a Management Implication Report (MIR) concerning shipping and storage procedures of a security material used to create passports. As a result of damaged shipments, the OIG recommended strengthening security and storage procedures for the material. OI is also currently investigating two criminal matters.

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, an administrative subpoena, a request for mail cover, and assisted OI with several matters that the Department of Justice accepted for civil and criminal prosecution. OALC also reviewed three Agency directives.

OALC helped coordinate responses to three congressional requests for information or assistance. In November 2007, the Chairman of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia of the House Committee on Oversight and Government Reform requested a review of diversity offices throughout agencies of the legislative branch. As a result of meetings with the Subcommittee's staff, the OAI will conduct an audit of GPO's Equal Employment Opportunity Office to assess how diversity programs are yielding desired results, the accuracy of the dispute and discrimination data being reported to Congress, and whether the diversity offices are sufficiently independent of the agency's general counsel and agency head. We expect to conclude this audit by late June.

In December 2007, the Committee on Oversight and Government Reform requested a list of outstanding recommendations the OIG made to the Agency since January 1, 2001. In January 2008, the OIG responded to the request. And in March 2008, the Chairman of the House Committee on Energy and Commerce and the Chairman of the Subcommittee on Oversight and Investigations requested OIG assistance in conducting a review of matters relating to the management and security of the e-Passport supply and production chain. That project is ongoing.

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) and is coordinating the development, with the GPO Web Development and Creative Services Division, of an informational Web site for the CCIG.

OIG Management Initiatives

Personnel Update

After significant discussions regarding the relative pay of OIG criminal investigators in relation to other OIG offices throughout the Federal Government, the Agency agreed to provide Law Enforcement Availability Pay (LEAP) to OIG criminal investigators, effective the first pay period of the calendar year. OALC worked with the Agency to develop and implement a directive for LEAP.

The OIG community recognized two of our special agents during this reporting period. At the President's and Executive Council on Integrity and Efficiency (PCIE/ECIE) Awards Ceremony on October 27, 2007, Senior

Special Agent Sonja L. Scott received an Investigative Award of Excellence for her investigation of two separate incidents involving workers' compensation fraud. In one case, the Office of Workers' Compensation Program (OWCP) of the Department of Labor issued a recovery notice to the claimant to repay GPO $947,000 received over 30 years, one of the largest in the history of the OWCP program. The other matter resulted in the individual pleading guilty to workers' compensation fraud with an order to repay $386,000 to the Agency.

Senior Special Agents Hugh D. Coughlin and Walter B. Martin IV (currently employed by the Defense Criminal Investigative Service) were also awarded the Investigative Award for Excellence for their investigation of two Government employees complicit in the systematic theft of more than 4,000 print cartridges, valued in excess of $110,000, from GPO and selling or pawning the equipment for personal profit. The employees pled guilty to theft of Government property, were ordered to make restitution in excess of $110,000, and one was sentenced to five months in jail while the other was sentenced to two years of probation.

Executive Council on Integrity and Efficiency

The PCIE and 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, and 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 regarding legislation to amend the Inspector General Act of 1978 (IG Act) in an effort to aid committee staff understanding of distinctions with executive branch IGs. In addition, legislative branch IGs coordinated a response and developed a comprehensive plan to address 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, regarding the request for a review of all legislative branch agencies' diversity offices. Quarterly meetings continue to rotate among the IG offices of the legislative branch. Updates and the progress of those meetings will be provided to Congress 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.

During this reporting period, OALC reviewed three Agency directives. First, OALC reviewed and updated the Agency's directive on its Program to End Waste, Fraud, and Abuse in GPO Programs and Operations, which, among other things, details the role and responsibilities of the IG, the Public Printer, and GPO employees in combating waste, fraud, and abuse. OALC also reviewed and provided comments on an Agency draft directive on Information Security Forensics Program, which delineates Agency responsibility regarding preservation of electronically stored information. Finally, OALC helped develop and implement the Agency's new directive on LEAP for OIG criminal investigators.

The OIG continued discussions with management regarding the process for establishing, updating, and communicating GPO directives to Agency employees. The OIG again urged management to update several directives, including the directive regarding the GPO workers' compensation program.

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.

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 and will provide updates in future reports.

We continue to note the issue of a new 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 during 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. The OIG, therefore, encourages management to continue making the matter a priority.

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, the GPO Quality Assurance Office made strides in their efforts for implementing provisions of the Government Performance and Results Act (GPRA). Although not required to follow all the mandates of GPRA, Congress has urged GPO to embrace its tenets. The Quality Assurance Office helped the Agency identify specific goals, objectives for each goal, and ways for measuring success through development of what GPRA refers to as a Balanced Scorecard. Moreover, work is nearly complete on GPO's Strategic Performance Plan and Achievements, which highlights Agency goals, objectives, performance in achieving those goals, and key achievements. GPO is also developing strategic plans for each business unit and incorporating Agency goals into each business unit's Balanced Scorecard to ensure work toward common goals and advance the Agency's Strategic Vision. We are encouraged that management made strategic planning a priority. Continued progress will help transformation efforts to stay on track during this critical transition time.

2. Management of Human Capital. We previously highlighted challenges GPO faces in "rightsizing" 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 to confront significant issues related to transformation of the GPO workforce and must advance creative solutions that will help the Agency meet its ongoing workforce needs, in part by building a diverse, qualified applicant pool.

Recognizing passport production as a priority, Human Capital must continue to tackle current and ongoing needs of plant operations so a reliable workforce is in place that can not only meet security requirements but also understand the need in the passport production facility for strict quality assurance and compliance. We previously reported that workforce issues affecting plant operations will be particularly important with respect to the plan to have the Secure Production Facility (SPF) fully operational by April 2008. Accomplishing such a milestone would require execution of a plan designed to hire, train, and place on site 50 personnel who can staff the SPF by March 1, 2008. As of the end of this reporting period, 28 personnel have been hired and reported for duty at the SPF and are being trained. Additional hiring and training will continue through the next reporting period.

GPO is also committed to having an Agency workforce that is diverse. The Agency has a goal of attracting, hiring, developing, and retaining a quality diverse workforce. During this reporting period, we initiated an audit at the request of Congress to review GPO diversity programs, particularly those related to establishing a more diverse population in senior leadership positions.

The results from the GPO Employee Survey released in 2006 show that while job satisfaction is relatively high, “communications at GPO” stands out as not having improved since 2004. When compared to results from the 2004 Federal Human Capital Survey, GPO actually rated lower in almost all identical items. Human Capital has, however, developed a plan that addresses those and other challenges as well as provides opportunities for improving communications at GPO. Improving communications at GPO will require ongoing support from management.

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. 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 contracted Independent Verification and Validation (IV&V) activities for two early implementation projects related to 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. The IV&V identified several vulnerabilities with both projects, and the OIG recommended that management strengthen controls that would help mitigate risks associated with those vulnerabilities. Management concurred with each recommendation and proposed responsive corrective actions. IV&V efforts for the second release of Oracle—including implementations related to inventory and procurement—were ongoing during this reporting period.

The OIG also continues to oversee activities of KPMG LLP (KPMG), the Independent Public Accountant (IPA) conducting the annual financial statement audit. During this period, KPMG completed its audit of the FY 2007 financial statement for which the Agency again received an unqualified opinion. The OIG and KPMG are planning for the FY 2008 audit.

4. Continuity of Operations (COOP). A previous OIG review of the 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 its 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.

Further steps that will enhance the Agency's COOP posture were taken during this reporting period, including planning and conducting exercises with scenarios that tested alternate production facilities and procedures for notifying essential personnel. The Agency is in the process of preparing a COOP project completion matrix that will demonstrate what GPO can do to support mission essential functions in the event of COOP activation.

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 every OIG audit includes an assessment 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 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 the 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 this reporting period, KPMG completed its audit of GPO's FY 2007 financial statements. KPMG's review of the internal control over financial reporting resulted in several deficiencies including (1) certain reconciliation controls should be improved, (2) in two instances there was a misapplication of generally accepted accounting principles, and (3) IT general controls should be improved. KPMG did not consider any of those deficiencies as material weaknesses.

6. Security and Intelligent Documents (SID). Management regards SID as the business unit that best exemplifies the Agency's future direction. Since our last report, GPO officially became a provider of Secure Federal e-Credentials. SID made that possible by reaching two critical milestones. First, SID established live secure e-Credential production capability. It reviewed Request for Proposal (RFP) responses and selected an experienced integrator that could provide a turnkey solution, including all necessary equipment, systems, and technical support services. The system configured for GPO enables the Agency to offer a broad range of e-Credential capabilities. Second, the Department of Homeland Security submitted a Standard Form-1, "Printing and Binding Requisition," to GPO for hundreds of thousands of secure Trusted Traveler Cards.

Although showing progress in meeting unprecedented demand from the Department of State, producing blank passports remains a significant concern from a security and quality assurance standpoint. The OIG will remain diligent in reviewing passport-related matters and has dedicated a Supervisory Auditor to review several issues during upcoming reporting periods.

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 during this reporting period, management needs to address technology as well as data security related to the electronic passport, inventory volume, and storage of blank passport books. Although we note progress regarding certain COOP vulnerabilities, several COOP-related issues still need to be addressed, and the OIG will continue to focus on several issues during upcoming reporting periods.

GPO also faces the challenge of deploying its own Homeland Security Presidential Directive 12 (HSPD-12)

infrastructure and issuance of identity credentials to employees and contractors. While not legally required to comply with HSPD-12, we continue to recommend that the agency strive towards voluntary compliance. To that end, several control objectives are critical for meeting the security, efficiency, fraud prevention, and privacy protection goals HSPD-12 requires and must be maintained throughout the lifecycle of deployment. Whatever the Agency's intentions, it should employ the best practices established by HSPD-12 and begin to address 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 to ensure compliance with Federal Information Processing Standards (FIPS) Publication 201 (FIPS-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 (JCP) expressed concerns to GPO 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 improved automation and data back-up and established specific hiring policies resulting in manning levels that have allowed Plant Operations to consistently produce and deliver congressional products. The OIG will continue to monitor the situation to make sure GPO continues meeting the demands of congressional printing.

8. Information Technology and Systems (IT&S) Management. As GPO transforms from an ink-on-paper operation to a highly secure multimedia digital dissemination 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 IT&S, including security issues, provide GPO with new and emerging 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, e-Passport system, Public Key Infrastructure (PKI), network management, and implementation of the Oracle financial management system. To create a plan that will help mitigate risks for GPO 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 addition, 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 and personal data. During FY 2007, the OIG conducted an assessment of GPO compliance with FISMA to identify any gaps and deficiencies in the Agency's overall information security program as well as critical Agency systems. We will conduct 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.[2] 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 periodic compliance reviews that determine whether assertions related to the adequacy and effectiveness of the controls over its PKI Certificate Authority operations are fairly stated based on underlying principles and evaluation criteria.

Finally, as identified in Management Challenge 3 and Management Challenge 10, the OIG will continue to lead IV&V activities associated with the ongoing implementation of the Oracle financial management system and implementation of FDsys.

9. Customer Service. As it moves closer to its goal of transforming to a 21st Century information processing and dissemination operation, GPO's customer services 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. GPO is implementing a phase of its new FDsys, which is envisioned as a world-class system capable of preserving and providing permanent public access to information published by the Federal Government. Successful acquisition and implementation of the approximate $29 million system is critical to the Agency's future as a 21st Century information processing and dissemination operation.

The OIG is conducting FDsys IV&V activities. IV&V activities will determine whether system implementation is consistent with the FDsys project and cost plan, and whether the delivered system meets GPO requirements. The first report on IV&V efforts identified several weaknesses that if not promptly addressed, could lead to schedule risk and cost overruns for Release 1.C of FDsys. Release 1.C is the public release of the system. Weaknesses in the implementation included (1) insufficient use of earned value analysis, (2) lack of an Integrated Baseline Review, (3) risks associated with testing, (4) lack of system capabilities documentation, and (5) insufficient Configuration Management Plan.

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 require a professionally trained contracting workforce skilled at carrying out nontraditional acquisitions. As such, organizational and staffing issues confronting the Agency remain a significant challenge.

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

UNITED STATE
GOVERNMEN
PRINTING OFF

Office of Audits and Inspections

The Office of Audits and Inspections (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. 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 also provides accounting and auditing assistance to the OIG Office of Investigations (OI) 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 35 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. GPO management took actions to close 16 open recommendations during the reporting period. As of March 31, 2008, 31 recommendations were still open.

B. Audit Accomplishments – Audit and Inspection Reports

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

GPO Network Vulnerability Assessment

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 used vulnerability scanning tools, which the OIG selected and the IT&S Security Division approved. 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 team found 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. Management concurred with each recommendation and is taking corrective action.

2. Audit Report 08-02 (Issued November 19, 2007)

Report on the Consolidated Financial Statement Audit of the Government Printing Office for Fiscal Years (FY) Ended September 30, 2007 and 2006

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG conducted the FY 2007 audit under a multiyear contract for which OAI served as the Contracting Officer's Technical Representative (COTR). The oversight ensured that the audit complied with generally accepted government auditing standards. OAI also assisted with facilitating the external auditor's work as well as reviewing work performed. In addition, OAI provided administrative support to the KPMG auditors and coordinated the audit with GPO management.

KPMG issued an unqualified opinion on the GPO FY 2007 consolidated financial statements, stating that the Agency's financial statements were presented fairly, in all material respects, in conformity with generally accepted accounting principles. KPMG identified the following significant deficiencies, which KPMG did not consider to be material weaknesses: (1) certain reconciliation controls need improvement; (2) generally accepted accounting principles were misapplied in two nonroutine transactions; and (3) general controls for IT need improving. KPMG made recommendations that address each condition. Management concurred with the recommendations and has either planned or initiated responsive corrective action.

3. Audit Report 08-03 (Issued January 28, 2008)

GPO General Ledger Account 6612, General Expense – Supplies

GPO policy requires that all expenditure transactions are categorized by object class. Department officials use General Ledger Account 6612, General Expense – Supplies (Account 6612), or Object Class 26.11, "General and Administrative Supplies and Materials," to record purchases of general supplies and expenses. That account also includes administrative and general office supplies, furniture, uniforms, and other supplies and materials not used in the production process. Purchases classified as Account 6612 are made with either a GPO purchase card or through the Agency's Materials Management Procurement and Control System II (MMPCS II). Beginning in FY 2002, the balance for Account 6612 fluctuated from $6.2 million to a high of $7.2 million in FY 2004 and decreased to $4.7 million in both FYs 2005 and 2006.

An OIG audit evaluated the appropriateness of transactions within Account 6612 to (1) determine whether GPO implemented appropriate management controls over transactions charged to the account; (2) evaluate the effectiveness of the procedures used to reconcile the account; and (3) determine whether use of the account complies with applicable laws and regulations. The audit found that controls were not always effective over purchase transactions within Account 6612 that were made in the first 6 months of FY 2006. Further, controls over transactions charged to Account 6612 can be improved to include prompt and timely posting and proper reconciling of transactions and ensuring that charges to the account are for items such as supplies and materials as described in GPO's Object Class Instruction. The audit specifically identified that:

- Regardless of object class, GPO purchase card transactions were classified as Account 6612, without reconciling individual transactions to a specific department or object class.
- Items such as materials, supplies, equipment, and services procured through the MMPCS II were often incorrectly classified as Account 6612.
- The Office of Workforce Development, Education, and Training acquired training for some GPO departments that was not charged to the using organization.
- The posting of purchases charged to Account 6612 was not consistently performed throughout the fiscal year.

The recommendations we made to management should, if implemented, not only improve management controls over the appropriateness of purchase transactions posted to Account 6612 but also help properly classify, reconcile, and post future purchase transactions as well as comply with applicable GPO instructions and procedures. Management concurred with each recommendation and implemented changes before the end of this reporting period.

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

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – First Quarter Observations and Recommendations

The FDsys program is a multimillion dollar effort that GPO is funding and managing to modernize the GPO 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. The OIG tasked the contractor with assessing the state of program management, technical, and testing plans and other efforts related to the public release of FDsys. The contractor must report to the OIG each quarter 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.

Between July and September 2007, the contractor completed an initial assessment of the FDsys prime contractor's program management practices used for the Release 1.B pilot system. The goal of that assessment was to analyze practices, assess effectiveness, and provide potential recommendations for improving management of the implementation for Release 1.C—in other words, its public release. The contractor reviewed the Program Management Plan, Risk Management Plan, Risk Database, the results of an Independent Risk assessment, several monthly reports and program reviews, variance analysis reports, and configuration management plans and practices.

The initial IV&V assessment showed that the prime contractor established a strong basis for good program management practices for Release 1.B. We identified, however, some weaknesses that could lead to schedule risk and cost overrun for Release 1.C if not addressed soon. 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.

After issuing the draft report, GPO changed some aspects of the FDsys program to include assuming program control. However, our original findings and recommendations are still applicable, and management responded based on the new plan for the FDsys program. The report contains 14 recommendations designed to strengthen management of the FDsys program. Management's corrective actions were responsive.

5. Audit Report 08-05 (Issued March 28, 2008)

Planning for GPO's Secure Production Facility

GPO is the sole source for producing, storing, and delivering U.S. passports for the Department of State. GPO produces those passports at a facility in Washington, D.C. To meet an increased requirement for passports and ensure continued production in case of disruption, an alternate production facility is needed. GPO is in the process of establishing such a facility in Mississippi. That facility, which GPO calls the Secure Production Facility (SPF), is planned to be up and running in April 2008, at an estimated cost of $41.4 million. The OIG performed an audit that evaluated planning for the SPF to determine if planning sufficiently ensured that the SPF would be delivered on schedule, meet GPO requirements and needs, and meet requirements for applicable Federal facilities.

The audit revealed that the SPF Team did a commendable job in a relatively short time of organizing the project, identifying and documenting project requirements, and developing implementation plans and acquisition strategies to ensure the project met its objectives. The OIG has supported the need for an alternate facility for passport production since 2005 and believes that the site selected in Mississippi more than meets the requirements. The report states that nothing has come to OIG attention indicating that the SPF will not operate as planned and provide the Agency a second source for producing U.S. passports. However, while evaluating the planning for the project, we found that because of time constraints and other factors (some of which according to management were beyond their control), GPO did not implement several of the formal and standard project management tasks GAO, the Office of Management and Budget, and various executive branch project management guidelines recommend. We found that before project commencement:

- Although GPO evaluated alternative sites for the SPF, it did not perform a comprehensive alternatives analysis to render support for its selection of the SPF location.
- GPO did not prepare a formal project charter.
- GPO did not develop a project plan, risk management plan, or acquisition plan.

Except for acquisition planning, GPO was not required by any Federal law or regulation to follow the recommended tasks. However, those tasks are considered to be best practices for use by Federal agencies in conducting facility acquisition projects. Therefore, we urged GPO to incorporate the tasks to the extent possible for the remainder of the SPF implementation project to help deliver the project on schedule and within budget. Moreover, the Agency should incorporate the tasks and recommendations herein for future facility acquisition projects.

We made two recommendations to management regarding development of formal project documentation which, if implemented, should deliver the remainder of this project, and any future facility acquisition project, on schedule and under budget. Management developed an SPF Master Project Plan that contains the formal project documents addressed in our recommendations. Management stated that it will use the SPF Master Project Plan along with lessons learned from the SPF as a basis for managing future projects. We considered management's actions responsive to both recommendations and closed the recommendations when we issued the report.

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

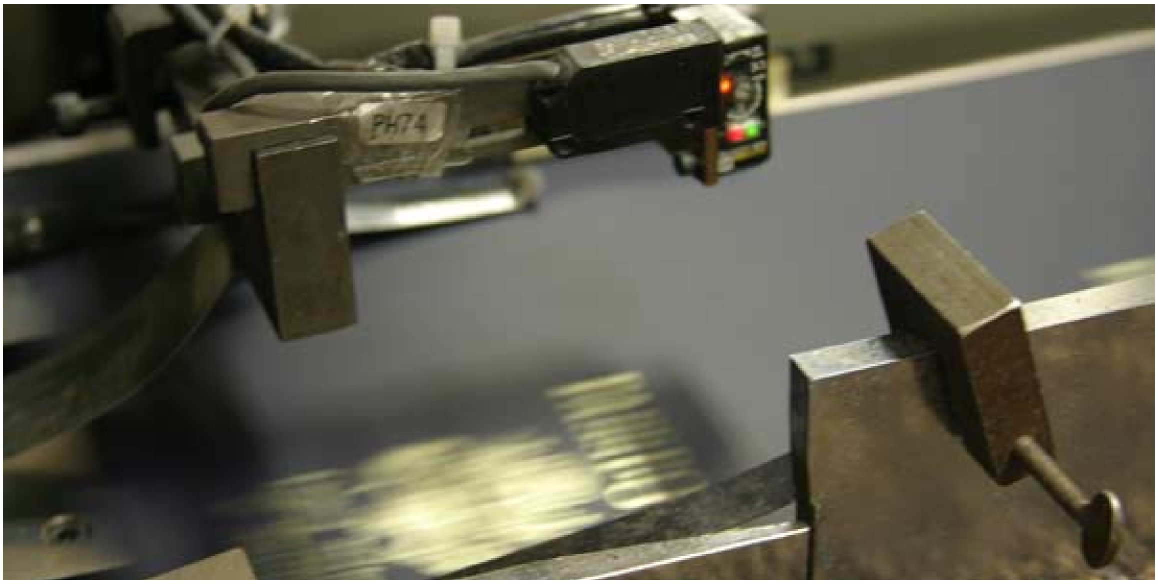
Operating System Security for GPO's Passport Printing and Production System

The GPO Passport Printing and Production System (PPPS) includes various computer applications and operating systems that support production of the 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 and could be compromised. The risk associated with compromise to the operating systems hosting such critical applications could result in services being disrupted, sensitive information being divulged, or 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. The OIG issued a sensitive report containing recommendations designed to not only help strengthen the security of the PPPS but also reduce the risk of system compromise.

C. TeamMate Audit Software Implementation

During this reporting period, OAI began implementing and using TeamMate software. TeamMate automates the entire workpaper process, including preparation, review, report generation, and global issue tracking. OAI will use TeamMate 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 by Pricewaterhouse Coopers for all types of audits, including: compliance, contract, controls, efficiency and regulatory reviews, financial, government, IT, investigations, procedural, and security. During this period, software installation was completed and the OAI staff trained on



the software. Any OAI audit begun after training will use TeamMate.

D. Future Digital System (FDsys) – 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 solution 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 this reporting period, GPO implemented a reorganization of the FDsys Program with respect to GPO and contractor participation and responsibilities. The reorganization reduces contractor tasking and increases GPO efforts. GPO will manage development, integration, and deployment of FDsys. A contractor will develop 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 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, we 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 in order 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 B, we discuss the results of our first report resulting from our IV&V efforts, which are ongoing and will continue throughout the life of the project.

E. Status of Open Recommendations

Management officials made significant progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. During this reporting period, GPO management took actions to close 16 recommendations. For the 31 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

Corrective action for the two open recommendations is in progress. The OIG is working with management and monitoring implementation of the two open 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 the implementation of the project.

OIG COMMENTS

Management provided documentation during this reporting period that was sufficient to close two of the eight recommendations that remained open from the previous reporting period. Management is continuing to work on implementing corrective actions for the remaining six open recommendations. We anticipate during the next reporting period continued progress toward closing the open recommendations.

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

Report on Early Oracle Implementation: Independent Verification and Validation (IV&V)

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

A total of 12 of the 21 recommendations were closed during this reporting period. Management continues to work on implementing corrective actions on the nine open recommendations.

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.[3] 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 will review management's progress for implementing the 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 Department of Homeland Security, 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. 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.

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

Management closed four of the seven remaining open recommendations during this reporting period. A total of three recommendations are open. With proposed corrective actions in place, we anticipate closing three recommendations during the next reporting period.

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

Office of Investigations

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 (general schedule job series 1811). 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, or both. Prosecutions may result in court-imposed prison terms, probation, fines, or 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 417 complaints or allegations, OI opened 17 investigative cases and closed 21. Of the investigative matters, 24 are ongoing. During this reporting period, OI issued one administrative subpoena and one mail cover request during investigative efforts.

B. Types of Cases

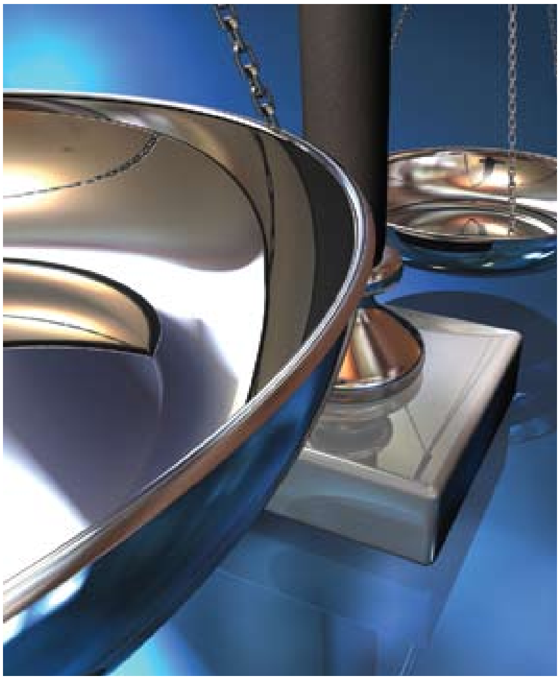
OI investigative workload includes the following major categories:

Workers' Compensation Fraud

OI investigates GPO employees who allegedly submit false claims or make false statements to receive workers' compensation benefits under the Department of Labor's Office of Workers' Compensation Programs (OWCP). We are working on four investigations involving alleged workers' compensation fraud.

Procurement Fraud

OI investigates allegations involving GPO contract service providers defrauding the Government in connection with GPO 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 two open cases involving procurement fraud.



Employee Misconduct

OI investigates allegations involving GPO employee misconduct. Allegations generally include misuse of Government computers, theft, assaults, drug violations, gambling, kickbacks, and travel voucher fraud. OI has 11 open investigations involving 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 request for investigations by other legislative agencies. OI has seven 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 five investigative matters to the Department of Justice for prosecution. Prosecutorial action is pending in two civil and three criminal matters.

Internal

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

D. Investigative Accomplishments

Management Implication Reports (MIR)

During the previous reporting period, OI issued an MIR concerning shipping and storage procedures of one of the security materials used to create the passports. As a result of damaged shipments GPO received, the OIG recommended that security and storage procedures for the material be strengthened. During this reporting period, as a result of our recommendations, the Agency responded and modified its security procedures.

Workers' Compensation Fraud

An OI investigation resulted in an OWCP claimant being sent for a second opinion examination by a psychiatrist and an orthopedist. Both physicians found that the subject was able to work with very few restrictions. The subject is in vocational rehabilitation to find suitable work. In addition, the subject of the review will then either be taken from the rolls or given a loss of wages earning capacity, which will reduce his benefits. Should the individual be taken off the rolls completely, the cost savings to the Government would be $44,800 a year ($448,000 in actuary amount over 10 years).

OI's continued proactive, investigative approach and its working relationship with the GPO Health Unit and the Office of Workers' Compensation 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. Final recovery is pending appeal.

Employee Misconduct

An OI investigation involving allegations of the use of a Government computer to view and download pornography was referred to management for action. The employee could be terminated from GPO employment for violations of Agency regulations on the use of Government computers and the Internet.

Procurement Fraud

An OI investigation of a GPO contractor accepted by the Department of Justice for civil prosecution is pending. The contractor is alleged to have filed false claims and statements in connection with contracts valued at approximately $438,000. Civil action in this matter could result in fines and restitutions of approximately $1,800,000.

OI investigated a GPO contractor for pre-billing before production and submitting false claims. The matter is pending a U.S. Attorney decision whether to take civil action against the company and company officials. As a result of that investigation, an investigation was initiated to determine the extent to which GPO contractors may be pre-billing or submitting false claims prior to the production and delivery of customer product.

Miscellaneous

OI assisted the Library of Congress OIG in a criminal investigation. In addition, at the request of two other legislative agencies, OI is investigating a criminal matter accepted by the Department of Justice's Office of Public Integrity for prosecution and concluded the investigation of another matter concerning a GPO employee who was on detail to work in Congress.

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 detailed 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
PUBLIC LAWS
LSA
January 2005
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.

Significant Deficiency - A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control over financial reporting.

Unsupported Costs - Questioned costs not supported by adequate documentation.

Abbreviations and Acronyms

CCIG	Council of Counsels to the Inspector General
CIO	Chief Information Officer
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
DMZ	Demilitarized Zone
ECIE	Executive Council on Integrity and Efficiency
FDLP	Federal Depository Library Program
FDsys	Future Digital System
EEO	Equal Employment Opportunity
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
IT	Information Technology
IT&S	Information Technology and Systems
IV&V	Independent Verification and Validation
JCP	Joint Committee on Printing
LEAP	Law Enforcement Availability Pay
MIR	Management Implication Report
MMPCS II	Materials Management Procurement and Control System
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
SPF	Secure Production Facility

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 13–16
Section 5(a)(2)	Recommendations for Corrective Actions	13–16 22
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	17–19
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	21
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)	13–16
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	27
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	28
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	$347,247	$240,687	$587,934
Reports issued during reporting period	$0	$0	$0
Subtotals	$347,247	$240,687	$587,934
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	$347,247	$240,687	$587,934
Reports for which no management decision made within 6 months of issuance	$347,247	$240,687	$587,934

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

Audit Reports	Funds Put To Better Use
Report on GPO Network Vulnerability Assessment (Assessment Report 08-01, issued November 1, 2007)	$0
Report on the Consolidated Financial Statement Audit of the Government Printing Office for Fiscal Years (FY) Ended September 30, 2007 and 2006 (Audit Report 08-02, issued November 19, 2007)	$0
Report on Audit of GPO General Ledger Account 6612, General Expense – Supplies (Audit Report 08-03, issued January 28, 2008)	$0
Report on Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – First Quarter Observations and Recommendations (Assessment Report 08-04, issued March 28, 2008)	$0
Report on Audit of Planning for GPO's Secure Production Facility (Audit Report 08-05, issued March 28, 2008)	$0
Report on Assessment of Operating System Security for GPO's Passport Printing and Production System (Assessment Report 08-06, issued March 31, 2008)	$0
Total	$0

Table C-4: Investigations Case Summary

Total New Hotline/Other Complaints Received during Reporting Period	**417**
No Formal Investigative Action Required	400
Cases Opened by OI during Reporting Period	17
Cases Open at Beginning of Reporting Period	28
Cases Closed during Reporting Period	21
Cases Open at End of Reporting Period	24
■ Cases Referred to GPO Management	5
■ Cases Referred to Other Agencies	1
■ Cases Referred to OAI	0

Current Case Openings by Allegation	**24**	
■ Contract and Procurement Fraud	2	8%
■ Employee Misconduct	11	46%
■ Workers’ Compensation Fraud	4	17%
■ Miscellaneous	7	29%

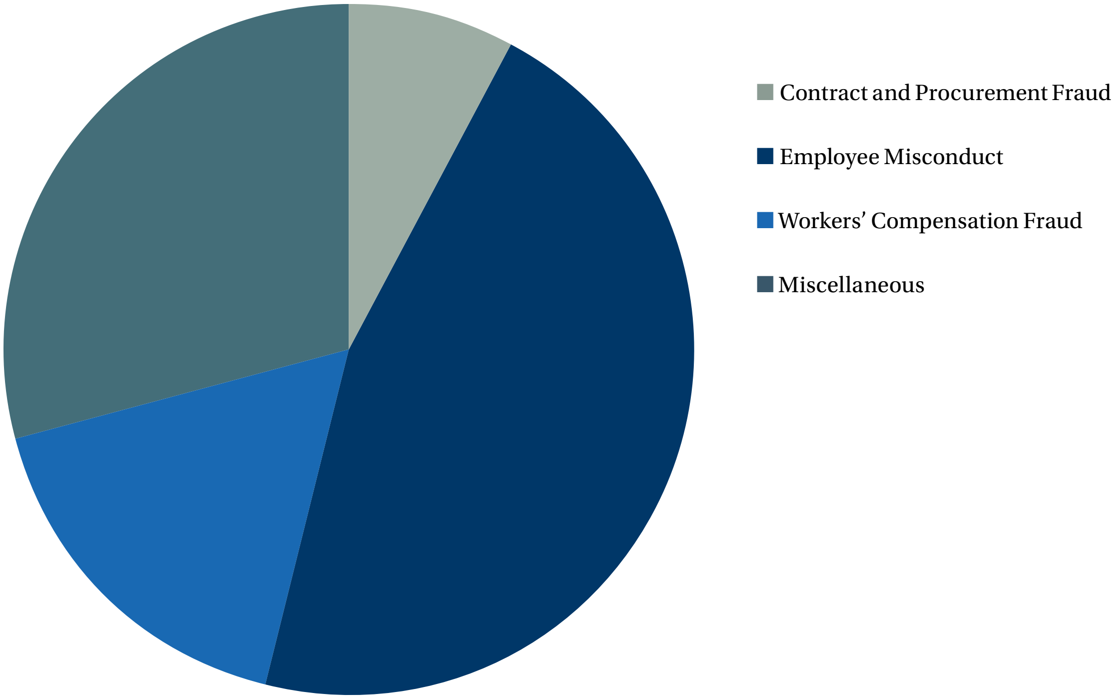


Table C-5: Investigations Productivity Summary

Arrests	0
Total Cases Presented to Prosecuting Authorities	5
Criminal	5
Criminal Declinations	1
Convictions	0
Guilty Pleas	0
Probation (days)	0
Jail Time (days)	0
Restitutions	$0
Civil	0
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	$0
Total Agency Cost Savings Through Investigative Efforts	$0
Total Administrative Referrals	3
Contractor Debarments	0
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions	0
Employee Terminations	0
Employee Warned/Other Actions	0
Other Law Enforcement Agency Referrals	0

U.S. GOVERNMENT PRINTING OFFICE
Keeping America Informed | www.gpo.gov

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