UNITED STATES GOVERNMENT PRINTING OFFICE

OFFICE OF INSPECTOR GENERAL

Semiannual Report to Congress

April 1, 2007 through September 30, 2007

The U.S. Government Printing Office

For well over a century, the mission of the U.S. Government Printing Office (GPO) has been to fulfill the needs of the Federal Government for information products and to distribute those products to the public. GPO is the Federal Government's primary centralized 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 the Federal Government.

Under the Federal Depository Library Program, GPO distributes a broad spectrum of Government publications both in print and online formats to more than 1,250 public, academic, law, and other libraries across the country. In addition to distributing publications, 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 are born digital products and will be published directly to the Internet. GPO will never actually print those products. Such an evolution of creating and disseminating challenges GPO. But GPO is meeting those challenges by transforming from primarily a print format to an entity capable of delivering information products and services from a flexible digital platform. While introduction of digital technology may change the way GPO products and services are created and how they look or function, GPO will continue to satisfy the changing information 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 mission of the OIG at GPO is to provide leadership and coordination as well as evaluate GPO's internal control structure, and recommend policies, processes, and procedures that will 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 to help the GPO improve its efficiency and effectiveness as it undertakes its era of unprecedented transformation. It offers an independent and objective way of keeping the Public Printer and Congress fully informed about problems and deficiencies along with any positive developments relating to the GPO's administration and operations. To meet those responsibilities, 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

This semiannual report of the U.S. Government Printing Office (GPO) Office of Inspector General (OIG) summarizes our work from April 1, 2007, through September 30, 2007. The audits, inspections, investigations, and other activities highlighted in this report demonstrate the OIG's ongoing commitment to promote integrity, accountability, efficiency, and effectiveness in GPO programs and operations.

During this reporting period, the OIG continued to review and assess its role within the Agency as it relates to the GPO Strategic Vision for the 21st Century. As a result of that review, the OIG updated its Strategic Plan and refocused OIG efforts on those areas of GPO operations that are most critical to the Agency's future success, while at the same time ensuring that the OIG maintains its independence and continues to carry out its legal duties and responsibilities.

The Office of Audits and Inspections (OAI) continued its focus on several technology-laden initiatives critical to the ongoing operations of GPO. After the Joint Committee on Printing (JCP) approved the project, the OIG began Independent Verification and Validation of GPO's Future Digital System (FDsys) – a program that this office will continue to monitor diligently to help ensure its success. The OIG also conducted the first assessment of GPO's compliance with the Federal Information Security Management Act (FISMA),[1] which resulted in several recommendations to help the Agency enhance its information security posture. The OAI also completed a contract claim review that questioned a contractor's claim of $587,934, including $347,247 in unallowed costs and $240,687 in unsupported costs.

In our efforts to review passport production programs and operations for the Department of State, the OAI is assessing the Agency's Secure Production Facility. An initial report is expected in the next reporting period. Additionally, the Office of Investigations (OI) completed two investigations concerning passport security. These investigations resulted in several management recommendations that will help improve passport production security.

[1] As a Legislative branch agency, GPO is not required to comply with FISMA. However, the Agency voluntarily chose to comply because FISMA is considered a Federal Government best practice for information security management.

The OI also continued its efforts to expose workers' compensation fraud. An investigation that the Department of Justice previously accepted for prosecution resulted in a conviction, a 12-month jail sentence, and an order of restitution in excess of $120,000.

The OIG will continue to work with GPO staff and management in identifying and resolving issues that promote efficiency and combat waste and fraud. With the appointment of a new Public Printer, the OIG looks forward to working with GPO management under a new administration.

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

Highlights of this Semiannual Report

During this reporting period, the OIG continued to direct 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 that resulted in criminal and administrative actions. We also continued to serve as consultants 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 5 reports with a total of 23 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency. Those reports had an associated dollar impact of $587,934. OAI also continued to work jointly with GPO management to close 14 open recommendations from previous reporting periods.

The Office of Investigations (OI) opened 15 new investigative cases in response to 394 new complaints or allegations and closed 18 matters. Through its investigative efforts during this period, OI recovered $1,625 and helped GPO realize cost savings of approximately $390,000 through the successful investigation of workers' compensation fraud. Finally, as a result of an OI workers' compensation fraud investigation, the subject was convicted and sentenced to 12 months in jail, placed on 24 months probation, and ordered to make restitution of $123,289 to the GPO.

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 also manages the budget and the administrative, human resources, and technology needs of the OIG. During the reporting period, OALC reviewed two search warrants, two administrative subpoenas, and assisted OI with several matters that the Department of Justice accepted for civil and criminal prosecution. In addition to its other duties throughout the reporting period, OALC also acted on a variety of matters as the OIG liaison to the GPO General Counsel and to the GPO Office of the Chief of Staff. Finally, the OALC participated actively in the Council of Counsels to the Inspector General (CCIG) and, along with the GPO Web Development and Creative Services Division, is working on a project to develop an informational CCIG website for the benefit of the entire IG community.

OIG Management Initiatives

Personnel Update

Alberto Rivera-Fournier joined the OIG as the Assistant Inspector General for Administration and Counsel to the Inspector General. Alberto comes to the OIG from the Federal Trade Commission where he worked as an attorney in the Bureau of Consumer Protection handling rulemakings and litigation. Before working at the FTC, Alberto was a Senior Attorney in the U.S. Office of Special Counsel, and also worked as Deputy General Counsel at the Puerto Rico Federal Affairs Administration. Alberto is a graduate of The George Washington University Law School and Wesleyan University.

Vera Garrant and Karl Allen joined the OAI as Supervisory Auditors. Both individuals bring a combination of over 45 years of audit experience to the GPO OIG from various Federal audit organizations.

Vera comes to the OIG from the Department of Health and Human Services OIG where she was the Director of the Planning, Reporting and Analysis Division in the Office of Management and Policy. Vera has over 21 years of Federal audit experience with several agencies including the Internal Revenue Service, the Defense Contract Audit Agency, the Department of Defense OIG, and the National Aeronautics and Space Administration (NASA) OIG. She is a graduate of New Hampshire College in Manchester, New Hampshire, and a Certified Public Accountant.

Karl joined us from the NASA OIG where he served as a Project Manager in the Financial and Institutional Audits Directorate. He served in a variety of positions at the NASA OIG for more than 16 years. Karl has 24 years of Federal audit experience with several agencies including the Department of Agriculture and was formerly with the GPO OIG from 1988 to 1990. He is a graduate of Rowan University in Glassboro, New Jersey, and is a Certified Public Accountant.

Kia Walters-Williams joined the OIG as Administrative Assistant. Kia comes to the OIG from the private sector, where she worked as a Route Coordinator at Lasership, a delivery company, for five years. Kia is a graduate of Meade Senior High School, at Fort Meade, Maryland.

Strategic Plan and Staff Training

During this reporting period, senior OIG staff updated the OIG Strategic Plan for 2007 through 2009. The plan discusses the vision, mission, goals, objectives, and strategies that will guide the OIG during the next three years and refocuses the OIG's efforts on those areas most critical to the Agency's future success. The updated strategic plan is on the OIG's website (www.gpo.gov/oig/strategic_plan.htm).

The OIG also had its first-ever training retreat for all OIG staff. The training focused on building effective team communication and working on understanding and accomplishing the OIG's Strategic Plan for 2007-2009.

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 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 29 Inspectors General (IGs) that the President appoints, and the ECIE comprises 33 IGs that agency directors appoint. The OIG at GPO is a member of the ECIE and participates regularly in its activities. During this reporting period, the co-Chair of the ECIE appointed the GPO IG to serve on the Legislative Committee of the PCIE/ECIE.

The Senate Appropriations Committee has previously acknowledged that a majority of legislative branch agencies have either a statutory or administrative IG to conduct and supervise audits and investigations relating to the programs and operations of their entity. The Committee recognized the benefits of coordination and formal communication between and among IGs through the PCIE and ECIE and urged that the legislative branch IGs communicate, cooperate, and coordinate with each other on an informal basis.

In response, legislative branch IGs now meet on a quarterly basis. During this reporting period, the GPO OIG hosted the meeting. The meetings have enabled improved communications and contact between the legislative branch IGs. In addition, the meetings have facilitated the development of a skills inventory to provide a resource for identifying available personnel to share resources, help identify cross-training needs, and perhaps facilitate coordination on future audits applicable throughout the legislative branch. Quarterly meetings will 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 Inspector General Act of 1978, as amended (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, the OIG continued discussions with GPO management regarding the process for establishing, updating, and communicating GPO directives to Agency employees. The OIG has urged management to maintain the legal integrity of the directives to ensure their effectiveness. GPO management has taken steps to address this concern. The OIG again urged GPO management to update several directives, including the directive regarding the GPO workers' compensation program.

While there were no legislative proposals relating to GPO programs and operations, at the request of the ECIE, the OALC provided additional comments to the ECIE legislative committee on two bills that would amend the IG Act. Those bills were House of Representatives Bill 928 and Senate Bill 1723 ("Improving Government Accountability Act").

GPO Management Challenges

GPO is well into its transformation efforts, 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 these programs and initiatives will continue. In our first semiannual report this fiscal year, 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 semiannual report and will continue to provide updates in future reports.

With the appointment of a new Public Printer, we remind management of the former Public Printer's comments that the challenges were "vital to GPO's continuous transformation" and that "it is critical that the next Public Printer incorporates all of these challenges and that the current progress being made on each of them continues. GPO cannot afford to reverse its course if it expects to be at the cutting edge of new technology and an industry leader in the digital age." We trust that the new Public Printer will continue the Agency's efforts in this regard.

While we have noted previously our concern about the Agency's acquisitions process, we acknowledge that the addition of a new Chief Acquisition Officer has brought about significant improvements. Assembling a highly professional and trained contracting workforce skilled at carrying out nontraditional acquisitions will continue to be key to the success of GPO.

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 for operation and maintenance. The estimates for building upkeep for Fiscal Year 2008 exceed $35 million. The Agency proposed to Congress a plan for relocating to new facilities specifically sized and equipped for future requirements and to more effectively 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's operations. While Members of Congress have expressed interest in this issue and urged the Agency to continue its efforts toward approval, there have been limited efforts in this regard. The OIG has not performed a review of the proposed move, but the information reviewed thus far supports significant cost savings. Accordingly, the OIG encourages management to continue making this matter a significant priority.

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 GPO's Strategic Vision for the 21st Century. We have urged business units to develop plans that cascade goals and objectives from the Agency's plan to help achieve employee buy-in and ensure that transformation efforts stay on track. In the absence of clearly articulated plans, senior management will have a difficult time determining whether the various business units are working together toward a common strategic goal.

During this reporting period, GPO Organizational Architects continued their efforts in implementing the provisions of the Government Performance Results Act (GPRA). Although not required to follow all of the mandates of GPRA, Congress has urged GPO to embrace its tenets. Indeed, the Organizational Architects have helped the Agency identify specific goals, objectives for each goal, and ways of measuring success. Although not necessarily constituting development of individual business unit plans (a strategy we continue to urge), identifying specific goals and objectives does help address the underlying issue—ensuring that business units work toward common goals and advance the GPO's Strategic Vision. We are encouraged that GPO management has made the effort a priority. Continued progress will help ensure that transformation efforts stay on track during this critical transition time.

2. Management of Human Capital. We previously highlighted challenges GPO faces in "rightsizing" the Agency 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 the transformation of the GPO workforce and must advance creative solutions for ensuring that the Agency meets its ongoing workforce needs, in part by building a diverse, qualified applicant pool.

The OIG previously highlighted the need for a comprehensive telework program. Since that time, GPO established an Agency policy successfully implementing a telework program. The telework program will also help address certain critical continuity of operations (COOP) issues.

With an increased demand for passport production, Human Capital must also address current and ongoing needs of plant operations to ensure that a reliable workforce is in place that can meet security requirements and understand the need for strict quality assurance and compliance in the passport production facility. Workforce issues affecting plant operations will be particularly important in the next six months with respect to the plan to have a Secure Production Facility (SPF) fully operational by April 1, 2008. Accomplishing that milestone will require the execution of a plan designed to hire, train, and place on-site, approximately 50 personnel to staff the SPF by March 1, 2008. We have initiated an audit to review the various issues related to the planning for the SPF.

The results from the GPO Employee Survey released in 2006 showed 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 these 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. While investment in the integrated system presents opportunities for enhanced efficiency and cost savings, it also presents significant risk in the event the system does not meet user requirements. GPO must ensure implementation happens 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 GPO implementation of the Oracle E-Business suite. The objective of IV&V is to provide GPO with an independent assessment of project status, satisfaction of user needs, and project cost effectiveness. To that end, the IV&V identified several vulnerabilities with the two projects and the OIG recommended that GPO management strengthen controls to mitigate the risks associated with those vulnerabilities. Management concurred with each of the recommendations and proposed responsive corrective actions. We are also continuing IV&V efforts for the second release of Oracle, which will include implementations related to inventory and procurement.

Finally, the OIG continues to provide oversight of the activities of KPMG LLP (KPMG), the Independent Public Accountant (IPA) conducting the GPO's annual financial statement audit. KPMG is currently in the process of auditing the FY 2007 financial statement.

4. Continuity of Operations. 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 included several recommendations including, most fundamentally, that GPO adopt the planning requirements and critical elements identified in Federal Preparedness Circular 65. Management must address the problem to be able to continue its essential functions and 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 addresses 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 establishes the appropriate response in the event of an emergency and addresses all known or anticipated categories of emergencies.

Further steps to enhance the Agency's COOP posture were taken during this reporting period, including identifying the location of the SPF and obtaining congressional approval to equip, staff, and activate the facility by April 1, 2008. In addition, the Agency conducted several, real-time COOP exercises which successfully tested alternate production facilities and notification procedures for essential GPO personnel.

5. Internal Controls. GPO management establishes and maintains a system of internal controls to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. In addition, 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.

In addition, the annual financial statement audit by KPMG addresses internal control issues and provides management with recommended corrective actions. While management recognizes the need for improving the current internal control environment to successfully implement its strategic vision, and has planned future initiatives in this area, Agency action is even more important because of upcoming changes that elevate even further the importance of a sound internal control program.

Of particular importance is the implementation of Statement on Auditing Standards (SAS) No. 112, "Communicating Internal Control Related Matters Identified in an Audit." SAS 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."

6. Security and Intelligent Documents. Management considers Security and Intelligent Documents (SID) the most important business unit for the future of GPO. Since our last report, SID continued its business development addressing Government credentials and re-examined its request for proposal for production capability of smart cards.

Although showing progress in meeting unprecedented demand from the Department of State (DOS), the production of 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 issues in upcoming reporting periods. The passport production facility underwent an external physical security review and we report the results herein. Redesign of the production area to enhance security, while reported as underway in our last report, still requires significant attention.

GPO has launched its e-Credentials program to serve customers in the DOS, Department of Defense, Coast Guard, and others. The Department of Homeland Security (DHS) Customs and Border Patrol (CBP) recently selected GPO to design, produce, and issue hundreds of

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.

thousands of secure Trusted Traveler cards. DHS/CBP has challenged GPO to create one of the most secure identity cards issued by the Federal Government. The Trusted Traveler security goals, shared among the governments of the U.S., Canada, and Mexico, are to protect North America from external threats, and to prevent and respond to internal threats.

Additionally, GPO and the Social Security Administration (SSA) will launch a pilot project using GPO equipment and processes to deliver 1000 Federal Information Processing Standards-201[2] cards. Evaluation results will determine if SSA proceeds with a follow-on project to personalize the FIPS-201 cards at quantities and timeframes to be determined. To realize the benefits from such opportunities, management must continue to ensure the necessary procurement and related support to SID. The OIG will work with SID to develop adequate oversight of these projects.

Although other concerns received significant attention, several matters must remain a priority for management. Among those concerns are finalizing a Memorandum of Understanding with the DOS, addressing technology as well as data security related to the electronic passport, inventory volume and storage of blank passport books, and understaffing in the SID business unit. Although we note progress regarding certain COOP vulnerabilities, critical issues must still be addressed and the OIG will continue to focus on these issues during upcoming reporting periods.

As GPO considers deploying its own Homeland Security Presidential Directive 12 (HSPD-12) infrastructure and issuance of identity credentials to GPO employees and contractors, it must consider several control objectives critical to meeting the security, efficiency, fraud prevention, and privacy protection goals of HSPD-12. Those control objectives include separation of duties in the registration and credential issuance processes; use of original identity source documents; use of appropriate background investigations; and, use of smart cards as person-identity-verification credentials. The OIG will monitor Agency efforts regarding internal deployment of HSPD-12 and conduct audits as necessary to ensure compliance with FIPS-201.

7. Supporting Congressional Printing. In our last reporting period, we noted that the JCP had 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-it-or-lose-it" leave during critical times, and various IT matters.

During this reporting period, GPO management took primary steps to address these problems, including establishing a Data Operations Center to provide IT support for Plant Operations and increased personnel to meet Congressional printing demand. The OIG will continue to monitor the situation to make sure long-term solutions and strategies are implemented to meet timely Congressional printing demands.

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 the GPO vision and mission. Acquisition, implementation, and sustaining engineering issues associated with IT&S, including security issues, provide GPO with new and emerging management challenges.

Noteworthy challenges for IT&S include establishing a top level Enterprise Architecture and support for a number of significant initiatives, including the Future Digital System (FDsys), e-passport systems, rollout of GPO's Public Key Infrastructure (PKI), network management, and the continued implementation of the Oracle financial management system. To create a plan for mitigating risks to GPO from aging legacy systems, IT&S initiated a legacy application and business

[2] Federal Information Processing Standards Publication 201 (FIPS-201) is a United States Government standard that specifies Personal Identity Verification requirements for Federal employee and contractor access to Federal facilities and information systems. FIPS–201 was developed to satisfy the technical requirements of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

impact analysis. Legacy systems increasingly inhibit GPO's ability to respond to customer needs and must be replaced or worked around.

In addition, because GPO is a provider of services to agencies of the executive branch who must comply with FISMA, GPO has chosen to substantially comply with the principles of the Act. Complying with FISMA presents additional challenges to IT&S, including protection of sensitive Agency information as well as personal information. During FY 2007, the OIG conducted an assessment of GPO compliance with FISMA to identify gaps and deficiencies in the Agency's overall information security program as well as specific critical Agency systems. We will conduct a follow-on FISMA assessment in FY 2008. We also conducted an annual assessment of the GPO enterprise network infrastructure to evaluate the level of security controls in place that help protect GPO's 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 GPO PKI is cross-certified with the Federal Bridge Certification 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 GPO revenue-generating activities.

To partially meet PKI certification provisions, the OIG conducts periodic compliance reviews that determine whether GPO's 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 also lead IV&V activities associated with the ongoing implementation of the Oracle financial management system and implementation of FDsys.

9. Customer Service. As GPO moves closer to its goal of transforming to a 21st Century information processing and dissemination operation, its customer services must reflect and advance that transformation. To ensure success in the future, GPO 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 have to. Transformation of the traditional GPO customer relationship requires a continuing evolution toward state-of-the-art customer relations management.

10. Acquisitions. GPO is implementing a phase of its new FDsys, which is envisioned to be a world-class system that will preserve and provide permanent public access to information published by all branches of 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 the system implementation is consistent with the FDsys project plan and cost plan, and whether the delivered system meets GPO requirements.

The OIG remains concerned with the Agency's ability to efficiently and effectively acquire the high-technology goods and services necessary to transform the Agency. Acquisitions such as the 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. With respect to the Agency's contracting workforce, management has taken steps such as separating Acquisition Services from Customer Services and hiring a Chief Acquisition Officer. Further emphasis should be focused on ensuring that GPO contracting staff obtains the appropriate training and qualifications necessary for conducting the types of complex acquisitions that the Agency will require during its transformation.

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


GOVERNMENT PRINTING OFFICE

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 performed by an IPA firm under contract. 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) promulgated by the Comptroller General of the United States.

When requested, OAI provides accounting and auditing assistance to the OIG OI for both civil and criminal investigations. Furthermore, OAI refers any irregularities and other suspicious conduct detected during audits, inspections, or assessments to OI for investigative consideration.

A. Summary of Audit and Inspection Activity

During this reporting period, OAI issued five new audit and assessment reports. These 5 reports made 23 recommendations for improving GPO operations, including strengthening of internal controls throughout the Agency. The reports also had an associated dollar impact of $587,934.

OAI continued to work with GPO management to close open recommendations carried over from previous reporting periods. As of September 30, 2007, a total of 33 recommendations remain open. The number of open recommendations decreased significantly from the 47 open as of the completion of the last semiannual reporting period. Based on our assessment of management's ongoing actions, including those specifically related to Oracle implementation, we believe that a significant number of remaining open recommendations from previous periods will be closed during the next reporting period.

B. Audit Accomplishments – Audit and Inspection Reports

1. Assessment Report 07-06 (Issued May 9, 2007)

Report on GPO Oracle Release 2 Project – Review of Statement of Work

The OIG continues to conduct IV&V activities associated with GPO implementation of the Oracle E-Business suite. GPO is implementing certain licensed modules of the Oracle E-Business suite in a series of Incremental Operating Capabilities (IOC). The objective of IV&V is to provide GPO with an independent assessment of project status, satisfaction of user needs, and project cost effectiveness.

To conduct IV&V activities, the OIG contracted with a nonprofit, scientific research and engineering corporation that operates in the public interest. To date, the OIG has conducted IV&V activities on several early implementation Oracle start-up projects. As part of this review, the OIG tasked the contractor to evaluate the Agency's draft Statement of Work (SOW) to obtain the services of a project integrator for the Oracle Release 2 project. Specifically, the contractor was tasked to evaluate the SOW to determine whether (1) the relevant sections necessary for a SOW of the size and scope of the Oracle Release 2 project were present; and (2) existing sections were fully articulated with the information required to enable full offeror scoping and Government bid evaluation.

The OIG issued a sensitive report which concluded that the draft SOW needed additional detail to ensure successful performance by an integrator, including additional detail to adequately scope the work to be performed. Although formal recommendations were not made to GPO, comments and recommendations intended to strengthen the SOW were provided to management and the GPO Oracle Project team.

2. Assessment Report 07-07 (Issued September 17, 2007)

Report on WebTrust Assessment of GPO's Certification Authority – Attestation Report

GPO implemented its PKI to support its "born digital and published to the Web" methodology and meet GPO customer expectations that documents are official and authentic. The GPO PKI also directly supports the GPO mission related to electronic information dissemination and e-Government. The GPO PKI is cross-certified with the Federal Bridge Certification Authority, whose certification provisions require that the GPO PKI undergo an annual compliance review.

To satisfy this compliance requirement, the OIG tasked an IPA firm to conduct a WebTrust assessment of the GPO PKI Certification Authority (CA) for the period of August 1, 2006 through June 30, 2007. The IPA assessed the CA in accordance with the American Institute of Certified Public Accountants (AICPA) "WebTrust Principles and Criteria for Certificate Authorities." The assessment represents an evaluation of whether GPO management assertions related to the adequacy and effectiveness of controls over its CA operations are in all material respects fairly stated. The IPA firm issued an attestation report that expresses their opinion that the assertions of GPO management regarding its CA operations are fairly stated. This opinion is contained in the final report, which is considered sensitive.

3. Audit Report 07-08 (Issued September 19, 2007)

Report on Audit of Revised Settlement Proposal by [GPO Contractor]

In accordance with Section 49.107 of the Materials Management Acquisition Regulation (MMAR), the OIG performed an audit of the revised settlement proposal a GPO contractor submitted. The settlement proposal was for a requirements contract awarded to provide the production of various laser Government forms, letters, notices, court documents, requests for information, and newsletters, requiring such operations as outputting of static and variable data from furnished electronic media, other printing of static information, binding, packing, mailing, and distribution. GPO terminated the contract for convenience in May 2006. In July 2006, the contractor submitted a settlement proposal to GPO for $1,312,747. Subsequent to GPO's counterproposal, the contractor submitted a revised proposal for $587,934.

The OIG audit of the revised settlement proposal questioned the contractor's entire claim of $587,934, including $347,247 in unallowed costs and $240,687 in unsupported costs. The report, which was advisory in nature, was submitted to the GPO Contracting Officer for use in negotiating a settlement or issuing a unilateral determination regarding the contractor's proposal. A decision by the GPO Contracting Officer was pending at the completion of this reporting period.

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

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

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.[2] Although a legislative branch agency, GPO has recognized the need to be FISMA compliant due to the services the Agency provides, including services to executive branch agencies.

The OIG contracted with a consulting firm to perform a baseline assessment of GPO's FISMA compliance and to evaluate the design and effectiveness of the controls over GPO's information security program, policies, and practices. The assessment was performed using the most recent applicable FISMA requirements and guidelines published by the Office of Management and Budget and the National Institute of Standards and Technology. Significant emphasis was placed on evaluating the GPO systems used for providing services to client agencies.

The OIG issued a sensitive report concluding that although the Agency has taken steps to comply with FISMA, additional progress is needed to fully comply. The report contains 11 recommendations which, if implemented, will help move GPO toward FISMA compliance.

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

Report on Perimeter Security Assessment of a GPO Building

The Federal Protective Service (FPS), an organization within the Department of Homeland Security, provides law enforcement and security services to the U.S. General Services Administration for federally owned and leased facilities. Although GPO is a legislative branch agency and not subject to FPS recommendations, the OIG considers FPS recommendations related to building security to be best practices for the protection of Federal facilities and GPO should follow them whenever possible and practical.

At the OIG's request, the FPS conducted a physical security assessment of a GPO Building. The assessment was conducted in accordance with the standards detailed in the "Department of Justice Vulnerability Assessment of Federal Facilities," dated June 28, 1995. The standards in the report establish facility security levels and minimum physical security safeguards required for all Federal facilities to protect against acts of terrorism and other forms of violence. The FPS evaluated the perimeter security of a GPO Building against Interagency Security Committee (ISC), Security Design Criteria. The ISC Security Design Criteria was developed to ensure that security becomes an integral part of the planning, design, and construction of new Federal office buildings and major modernization projects.

The FPS methodology for assessing security in this 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 12 recommendations intended to enhance security of this GPO Building.

C. Financial Statement Audit Activity

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees.[3] KPMG LLP (KPMG) is conducting this audit under a multiyear contract for which the OAI provides oversight as its Contracting Officer's Technical Representative (COTR). The oversight ensures that the audit complies with government auditing standards. OAI also assists with facilitating the external auditor's work as well as reviewing the work performed. In addition, OAI provides administrative support to the KPMG auditors and coordinates the audit with GPO management.

[2] 44 U.S.C. § 3541 *et seq.*

[3] 44 U.S.C. § 309(e).

KPMG issued an unqualified opinion on GPO's FY 2006 consolidated financial statements, stating that its financial statements were presented fairly, in all material respects, in conformity with generally accepted accounting principles. KPMG identified several reportable conditions, including (1) strengthening controls surrounding the billing process, (2) improving certain reconciliation controls, (3) improving controls over recording and reporting environmental liabilities, and (4) improving general information technology controls. KPMG made recommendations addressing each condition and GPO management concurred with the recommendations.

KPMG is currently auditing the Agency's FY 2007 consolidated financial statements and assessing the status of the FY 2006 findings to determine whether they will need to be reported again in the FY 2007 audit report, along with any new findings and recommendations.

D. Secure Production Facility

GPO is the sole source for the production, storage, and delivery of all U.S. passports for the DOS. The Agency produces the passports at one facility located in Washington, DC. GPO is in the process of establishing an alternate passport production facility outside of the Washington, DC, area to ensure continued passport production in the event of a disruption. GPO refers to that facility as the Secure Production Facility (SPF) and plans for it to be operational by April 1, 2008, at an estimated cost of $41 million.

The OIG is in the process of performing an audit evaluating Agency planning for the SPF. The specific audit objectives are to determine if GPO planning is sufficient to ensure that the SPF is delivered on schedule, meets GPO requirements, and meets applicable Federal facility requirements.

In July 2007, the OIG issued a status memorandum to GPO senior management on this assignment's progress. In that memorandum, we state that based on the limited work performed to that point, the OIG had not identified any issues that would indicate the proposed facility would not meet the needs of the GPO for an alternate facility for passport production. The facility has perimeter security, sound structure, and transportation and communication capabilities that meet Agency needs.

With respect to project management, GPO had recently appointed a Project Manager in order to consolidate responsibility for the project with one individual who had already begun taking steps for ensuring the project proceeds on schedule. We brought to management's attention one issue concerning the opportunity to possibly leverage state funding and financial incentives to assist with workforce development for employers, including Federal Government agencies, relocating to or operating in the state. We anticipate issuing a report on this audit during the next semiannual reporting period. This report will address issues such as schedule, cost, requirements, and human capital.

E. TeamMate Audit Software Implementation

The OAI has taken the initial steps during this reporting period to begin implementation of PricewaterhouseCoopers (PWC) TeamMate software. TeamMate is a powerful electronic work paper package that has revolutionized the audit documentation process. TeamMate will be used by OAI 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 designed by PWC to be used for all types of audits, including: compliance, contract, controls, efficiency and regulatory reviews, financial, government, IT, investigations, procedural, and security. TeamMate automates the entire work paper process, including preparation, review, report generation, and global issue tracking. During this period, the software and associated licenses were purchased and installation began. We anticipate conducting staff training and initially implementing TeamMate for assignments during the next reporting period.

F. Future Digital System (FDsys)—Independent Verification and Validation

The FDsys will be a comprehensive information life cycle 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 be composed of approximately 6 solution clusters (Content Management, Content Preservation, Content Access, Content Delivery, Content Submission, and Infrastructure), which are comprised of 25 or more functional areas.

FDsys is being developed by a joint GPO and Harris Corporation (Harris) team. A multiyear, multirelease integration effort will be used to design, procure, develop, integrate, and deploy selected technologies and components of FDsys. Harris will create the system design and development, integrate various components, technology, and applications that support functional FDsys functional clusters, and deliver a world-class information lifecycle management system.

The OIG is responsible for IV&V work associated with developing and implementing FDsys. We have contracted with American Systems to conduct the IV&V. American Systems has extensive IV&V experience in the Federal sector. IV&V work will determine whether system implementation is consistent with the FDsys project plan and cost plan, and whether the delivered system meets GPO's 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.

G. Status of Open Recommendations

GPO management officials made significant progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. GPO management closed 14 open

recommendations during this period. For the 33 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. Inspection Report AI0502 (Issued March 31, 2005)

Blank Passport Product Integrity and Security Review

Finding

The inspection revealed several weaknesses in the business processes used for producing blank passports. Those weaknesses included missing critical core competencies, deficient processes, and infrastructure issues that require GPO management attention. The OIG also found significant deficiencies regarding manufacture of blank passports, security of component products, and related internal controls that require GPO management review and reengineering.

Recommendation

The OIG recommended that GPO improve the business processes used for producing blank passports that are relevant to all documents and operations within GPO's Security and Intelligent Documents (SID) operation. GPO's implementation of the recommendations should lead to an improved level of security and integrity for the entire SID business line.

Management Comments

GPO management generally concurred with the report's recommendations and continues to implement actions that will correct the conditions.

OIG Comments

GPO management provided documentation during this reporting period that closed two of the four open recommendations. Management is working on implementing corrective actions for the remaining two open recommendations.

2. 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, the OIG closed one recommendation upon issuance of the final report.

Management Comments

GPO management concurred with each of the report's recommendations and initiated responsive corrective actions.

OIG Comments

GPO management provided documentation during this reporting period that closed one of the three open recommendations. Corrective actions for the two remaining recommendations are in progress. The OIG is working with GPO management and monitoring implementation of the remaining two open recommendations.

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

GPO Oracle Program Stakeholder Analysis

Finding

The assessment identified several vulnerabilities associated with GPO's Oracle Program and made recommendations that would 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 the 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

GPO management concurred with each of the report's recommendations and agreed to take corrective actions throughout implementation of the project.

OIG Comments

GPO management provided documentation during this reporting period that was sufficient to close 4 of the 12 recommendations that remained open from the previous reporting period. Management is continuing to work on implementing corrective actions for the remaining eight open recommendations. We anticipate progress during the next reporting period toward closing the remaining open recommendations.

4. 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 included 21 recommendations to GPO management for strengthening controls and mitigating risks associated the vulnerabilities.

Management Comments

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

OIG Comments

Each of the 21 recommendations remains open as of the close of this reporting period. A majority of the recommendations were made to improve future Oracle implementations.

Office of Investigations (OI)

The 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, GPO management, or other Agency employees. Special Agents in OI are Federal Criminal Investigators (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 also issues Management Implication Reports that identify issues uncovered during an investigation it believes warrant prompt attention by GPO management.

A. Summary of Investigative Activity

During this reporting period and in response to 394 new complaints or allegations, OI opened 15 investigative cases. It closed 18 cases. Twenty-eight of the investigative matters are on-going. During this reporting period, OI obtained two search warrants and issued two administrative subpoenas during the course of investigative efforts.

B. Types of Cases

The OI investigative workload includes the following major categories:

Workers' Compensation Fraud

The OI investigates GPO employees who allegedly submitted false claims or made false statements to receive workers' compensation benefits. We are working on seven investigations involving alleged workers' compensation fraud.

Procurement Fraud

The OI investigates allegations involving GPO contract service providers defrauding the Government in connection with GPO's procurement of goods and services. These violations generally include, but are not limited to, false claims, false statements, wire and mail fraud, product substitution, and Small Disadvantaged Business Program violations. OI has five open cases involving procurement fraud.

Employee Misconduct

The OI investigates allegations involving GPO employee misconduct. Allegations generally include, but are not limited to, misuse of Government computers, theft, assaults, drug violations, gambling, kickbacks, and travel voucher fraud. OI has 11 open investigations involving misconduct.

Miscellaneous

The OI investigates miscellaneous administrative allegations and other types of investigations that do not fall into one of the above categories. Examples of such investigations include theft of Government property or illegal hacking. 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 seven investigative matters to the Department of Justice (DOJ) for prosecution. Prosecutorial action is pending in one matter referred in a previous reporting period and accepted for civil prosecution

Internal

Five investigative matters referred to GPO management for action remain pending. In addition, GPO management resolved seven investigative cases from previous reporting periods. Agency action in response to the investigation findings included one suspension, five letters of warning, and one termination from GPO employment.

OI investigative findings were also forwarded to the appropriate Agency official for suspension, debarment, or other administrative actions against Agency contractors. As a result of OI investigative efforts this reporting period, the Agency issued two debarments and four letters of warning.

D. Investigative Accomplishments

Management Implication Reports (MIR)

During this reporting period, OI issued two MIRs to GPO management regarding the security of passport production.

The first MIR concerned visitor access policy. The OIG recommended that the Agency review its visitor access policy to restrict access to "official" visitors only. The agency concurred with all recommendations set forth in that MIR.

The second MIR concerned the shipping and storage procedures of the security material used to create the passports. Due to damaged shipments received by GPO, the OIG recommended that security and storage procedures for the material be strengthened. As of the end of the reporting period, the agency has not responded to our recommendations addressed in that MIR.

Workers' Compensation Fraud

An investigation into workers' compensation fraud that was accepted for criminal prosecution by the DOJ was resolved during this reporting period. The employee was convicted, sentenced to 12 months imprisonment, two-years probation, and ordered to make restitution to the GPO in the amount of $123,289.29.

OI's continued pro-active, investigative approach and its working relationship with GPO's Health Unit and the Office of Workers' Compensation has resulted in maintaining agency Sick Injured Administrative costs under $20,000 per month.

OI's investigative efforts also found that one workers' compensation claimant had died; however, the death was not reported to the Department of Labor. As a result, the GPO will save $18,000 per year ($180,000 in actuary amount over 10 years) in compensation payments.

A previous reporting period investigation of a GPO employee of alleged workers' compensation fraud resulted in the forfeiture of $34,623.00 of the employee's compensation. Final recovery is pending any appeal of the forfeiture.

An OI investigation into violations of the workers' compensation program resulted in the employee being removed from the periodic rolls because an independent medical examination determined that he was no

longer injured. As a result, the agency will save $21,000 per year ($210,000 in actuary amount over 10 years) in compensation payments.

Employee Misconduct

An OI investigation involving allegations of pornography and other offensive materials, including child pornography, resulted in the employee being terminated from GPO employment for violations of agency regulations on the use of government computers and the Internet. Information regarding this matter was referred to the Maryland State Police for any investigative measures they deem necessary.

A prior reporting period investigation regarding an alleged assault by a GPO Police Officer resulted in the officer receiving a letter of warning.

An OAI referral to the OI regarding an employee who submitted false travel vouchers and time and attendance forms resulted in the employee: (1) receiving a Letter of Warning; (2) being placed on travel restriction for up to six months; (3) being ordered to take a training class on submitting travel vouchers; and (4) being ordered to pay restitution in the amount of $6,511.27.

Procurement Fraud

An OI investigation of a GPO contractor and accepted by DOJ for civil prosecution is still 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.

A previous reporting period investigation of a GPO Region 5 contractor that allegedly submitted false claims/statements resulted in the debarment of the contractor and its officers from future GPO contracts.

An ongoing prior reporting period investigation of a contractor regarding alleged contract fraud, false statements, product substitution, and subcontracting resulted in a final recovery of $1,625.

As a result of OI investigative efforts, the Agency issued two debarments and four letters of warning to agency printing contractors.

Miscellaneous

OI investigated several GPO Persistent Uniform Resource Locators (Internet commands that redirect users to specific websites) that linked to pornographic, online casino, and pharmaceutical websites. Through the course of the investigation, OI determined that the perpetrators were from various foreign nations and, therefore, was unable to pursue any judicial proceedings.

E. Work-In-Progress

Several significant OI matters remain pending as of the end of this reporting period. Disposition and results of those investigations will be detailed in future reports.

APPENDIX A: GLOSSARY AND ACRONYMS

Glossary

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

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

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

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

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

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

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

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

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

Material Weakness – A significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

Questioned Cost - A cost the IG questions because of an alleged violation of a law, regulation, contract, cooperative agreement, or other document governing the expenditure of funds; such cost is not supported by adequate documentation; or the expenditure of funds for the intended purposes was determined by the IG to be unnecessary or unreasonable.

Recommendation - Actions needed to correct or eliminate recurrence of the cause(s) of the finding(s) identified by the IG to take advantage of an opportunity.

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

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

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

Unsupported Costs - Questioned costs not supported by adequate documentation.

Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
COOP	Continuity of Operations
COTR	Contracting Officers Technical Representative
DHS/CBP	Department of Homeland Security Customs and Border Patrol
DOJ	Department of Justice
DOS	Department of State
ECIE	Executive Council on Integrity and Efficiency
FDLP	Federal Depository Library Program
FDsys	Future Digital System
FIPS-201	Federal Information Processing Standard Publication 201
FISMA	Federal Information Security Management Act
FSA	Financial Statement Audit
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GPO	U.S. Government Printing Office
GPRA	Government Performance Results Act
HSPD-12	Homeland Security Presidential Directive-12
IG	Inspector General
IG Act	Inspector General Act of 1978
IOC	Incremental Operating Capabilities
IPA	Independent Public Accountant
IT&S	Information Technology and Systems
IV&V	Independent Verification and Validation
JCP	Joint Committee on Printing
MMAR	Materials Management Acquisition Regulation
OAI	Office of Audits and Inspections
OEP	Occupant Emergency Plan
OI	Office of Investigations
OIG	Office of Inspector General
PCIE	President's Council on Integrity and Efficiency
PKI	Public Key Infrastructure
SAS	Statement on Auditing Standards
SID	Security and Intelligent Documents
SOW	Statement of Work
SPF	Secure Production Facility
SSA	Social Security Administration

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 13–15
Section 5 (a)(2)	Recommendations for Corrective Actions	13–15
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	17
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)	13–15
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 total dollar value recommendations that funds be put to better use	29
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 Inspector General 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	$347,247	$240,687	$587,934
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	$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 for Funds That Can 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 Oracle Release 2 Project—Review of Statement of Work (Assessment Report Number 07-06, issued 05/09/07)	$0
Report on WebTrust Assessment of GPO's Certification Authority—Attestation Report (Assessment Report Number 07-07, issued 09/17/07)	$0
Report on Audit of Revised Settlement Proposal by [GPO Contractor] (Audit Report Number 07-08, issued 09/19/07)	$587,934
Report on GPO's Compliance with the Federal Information Security Management Act (Assessment Report Number 07-09, issued 09/27/07)	$0
Report on Perimeter Security Assessment of Government Printing Office (GPO) Building 4 (Assessment Report Number 07-10, issued 09/28/07)	$0
Total	$587,934

Table C-4: Investigations Case Summary

Cases Open at Beginning of Reporting Period	31
Total New Hotline / Other Complaints Received during SAR Period	394
Cases Opened by OI	15
Cases Closed during Reporting Period	18
No Formal Investigative Action Required	379
Cases Open at End of Reporting Period	28
• Cases Referred to GPO Management	5
• Cases Referred to Other Agencies	1
• Cases Referred to Office of Audits and Inspections	0

Current Case Openings by Allegation	28	
• Contract and Procurement Fraud	5	18%
• Employee Misconduct	11	39%
• Workers' Compensation Fraud	7	25%
• Miscellaneous	5	18%

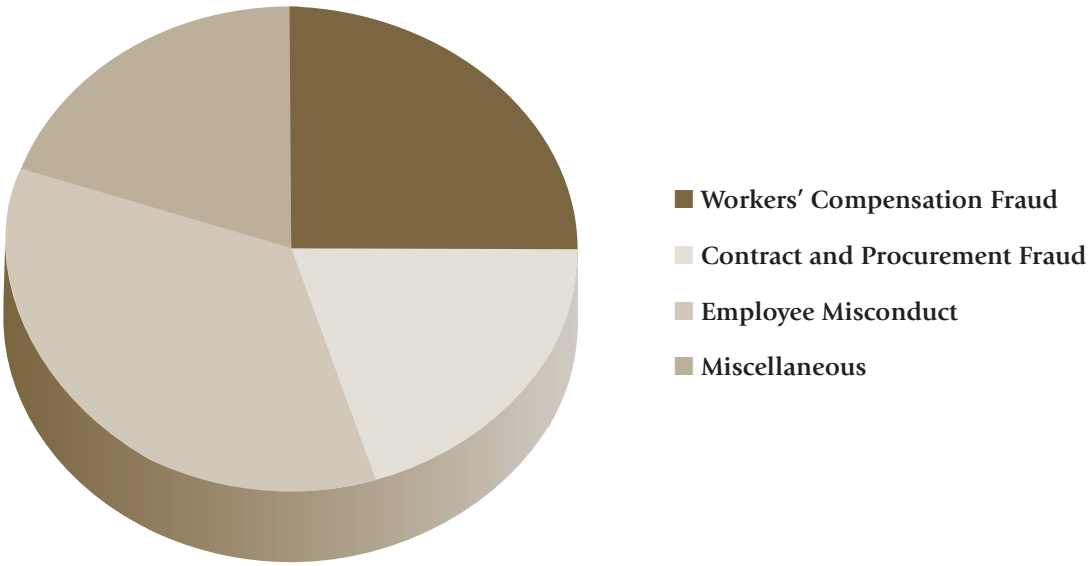

Table C-5: Investigations Productivity Summary

Arrests	0
Total Cases Presented to Prosecuting Authorities	8
Criminal	8
Criminal Declinations	7
Convictions	1
Guilty Pleas	0
Probation (days)	730
Jail Time (days)	365
Restitutions	$129,800
Civil	0
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	$1,625
Total Agency Cost Savings Through Investigative Efforts	~ $390,000
Total Administrative Referrals	5
Contractor Debarments	2
Contractor Suspensions	0
Contractor Other Actions	4
Employee Suspensions	1
Employee Terminations	1
Employee Warned/Other Actions	5
Other Law Enforcement Agency Referrals	**1**

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