



UNITED STATES GOVERNMENT PRINTING OFFICE  
OFFICE OF INSPECTOR GENERAL

# Semiannual Report to the Congress

October 1, 2006 through March 31, 2007

## The U.S. Government Printing Office

For well over a century, the mission of the U.S. Government Printing Office (GPO) under Public Printing and Documents statutes of title 44 of the United States Code 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](http://www.gpoaccess.gov)).

Today about half of all Federal Government documents are born digital products and will be published directly to the Web. GPO will never actually print those products. Such an evolution of creating and disseminating seriously challenges GPO. But GPO is meeting the challenges by transforming from primarily a print format to an entity capable of delivering information products and services in 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 recommend policies that will prevent and detect fraud, waste, abuse, and mismanagement. The OIG also recommends policies that will promote economy, efficiency, and effectiveness in GPO's programs and operations.

The OIG is dedicated to acting as an agent of positive change designed 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 administration and operations of the GPO. To meet those responsibilities, the OIG conducts audits, evaluations, investigations, inspections, and other reviews.

# Contents

Message from the Inspector General .....	1
Highlights of this Semiannual Report.....	3
OIG Management Initiatives.....	3
Review of Legislation and Regulations .....	4
GPO Management Challenges.....	6
Office of Audits and Inspections.....	12
A. Summary of Audit and Inspection Activity .....	12
B. Audit Accomplishments – Audit and Inspection Reports.....	12
C. Financial Statement Audit Activity .....	15
D. Peer Review .....	15
E. Status of Open Recommendations.....	15
Office of Investigations.....	20
A. Summary of Investigative Activity.....	20
B. Types of Cases.....	20
C. Status of Action on Referrals.....	20
D. Investigative Accomplishments .....	21
E. Work-In-Progress .....	21
<b>Appendices</b>	
A. Glossary and Acronyms .....	23-24
B. Inspector General Act Reporting Requirements .....	25
C. Statistical Tables	
Table C-1: Audit Reports with Questioned and Unsupported Costs .....	26
Table C-2: Audit Reports with Recommendations for Funds That Can Be Put to Better Use.....	27
Table C-3: List of Audit and Inspection Reports Issued During Reporting Period .....	28
Table C-4: Investigations Case Summary.....	29
Table C-5: Investigations Productivity Summary.....	31



## Message from the Inspector General

I recently came across a fairly critical review of Inspectors General suggesting that while IGs do good work, the result of recent IG activity was “an unhealthy situation . . . in which the IG culture has undermined public management.” While it might be easy to dismiss such criticism out of hand as the author is a registered lobbyist for two firms that do business with the government, the author is also a professor of public management at Harvard University and his comments warrant consideration. The author opines that most IG reports:

- ♦ Favor punishment and are highly critical of agencies for being insufficiently punitive rather than urging management to do more to reward achievement.
- ♦ Focus on controls, as opposed to creativity, which inhibits creative and innovative problem solving.
- ♦ Focus on problems rather than accomplishments, which creates a culture that “demoralizes civil servants, whose sense of commitment to their agencies’ missions is a crucial driving force for better work.”

OIGs are duty bound to ferret out fraud, waste, abuse, and mismanagement as well as to provide leadership, coordination, and promote economy, efficiency, and effectiveness within our respective agencies. What the author observes is arguably the antithesis of our responsibilities.

While not everyone will agree with the author, his comments certainly caused me to pause and reflect on my own office and reminded me of the importance for regularly examining our own internal operations. In that regard, we should be looking for ways, both within the OIG and with our Agency, to reward achievement, seek creative and innovative solutions for solving problems, and ensure our work is meaningful and engenders a sense of commitment and purpose. Not only would our offices and agencies be better served by continuous improvement in those areas, so too would the American public as beneficiaries of such process improvement. At minimum, it is worthy of consideration.

This semiannual report of the U.S. Government Printing Office (GPO) Office of Inspector General (OIG) summarizes our work from October 1, 2006, through March 31, 2007. The audits, inspections, investigations,

and other activities highlighted in this report demonstrate the ongoing commitment of the OIG to promote integrity, accountability, efficiency, and effectiveness in the programs and operations of the GPO.

During this reporting period, GPO continued to make significant progress in its efforts to transform into a 21<sup>st</sup> century information processing and dissemination operation. And, the OIG continued to focus on several technology-laden initiatives critical to transformation efforts of GPO. In that regard, the OIG made its selection for a contractor who will perform Independent Verification and Validation of GPO's Future Digital System (FDsys). We are awaiting authorization from the Joint Committee on Printing (JCP) to finalize the procurement.

In our efforts to protect the public from fraud, waste, abuse, and mismanagement, the Office of Audits and Inspections completed a follow-on report of GPO's purchase card program. The audit identified internal control and other issues that, when corrected, will improve the program's overall effectiveness. Additionally, the Office of Investigations continued its efforts to expose workers' compensation fraud. An investigation resulted in orders for restitution in excess of \$900,000.

The cooperation between GPO managers and the OIG has enabled us to work together to resolve a variety of issues. I continue to be hopeful that the spirit of cooperation will improve. And, as we urge GPO management to be customer focused, involve people in decision making, and embrace continuous improvement, the OIG must not only reflect upon, but also engage in, continuous improvement. The dedication and commitment of the OIG staff will be a crucial driving force toward that effort.

A handwritten signature in black ink, reading "J. Anthony Ogden". The signature is written in a cursive, flowing style.

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

## Highlights of this Semiannual Report

During this reporting period, the OIG continued to direct its resources addressing 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 and administrative actions. We also continued to provide general and professional assistance and reviews of proposed legislation and regulations. The work of each of the OIG components is summarized below.

*The Office of Audits and Inspections (OAI)* issued five reports with a total of 30 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency. OAI also continued to work jointly with GPO management to close a significant number of open recommendations from previous reporting periods. OAI also received an unqualified opinion on a peer review the OIG at the National Science Foundation conducted.

*The Office of Investigations (OI)* opened 25 new investigative cases in response to 298 new complaints or allegations and closed 32 matters. Through its investigative efforts during this period, OI recovered \$947,742 and helped GPO realize cost savings of approximately \$656,400 through the successful investigation of workers' compensation fraud. Finally, as a result of a criminal conviction, the subjects of an OI investigation were ordered to make \$117,222 in restitution to GPO.

*The Office of Administration/Legal Counsel (OALC)* manages the OIG budget and human resources needs. OALC also provides legal advice and counsel on issues arising during the course of audits, inspections, and investigations, including opinions regarding legal accuracy and sufficiency of OIG reports. During the reporting period, OALC reviewed five administrative subpoenas and assisted OI with several matters accepted for civil and criminal prosecution by the Department of Justice (DOJ). In addition to its other duties throughout the reporting period, OALC also

acted on a variety of matters as OIG liaison to the GPO General Counsel and to the Office of the Chief of Staff.

## OIG Management Initiatives

### Personnel Update

Daniel Rose joined OAI as an Information Technology (IT) Specialist. Dan comes to the OIG from Science Applications International Corporation (SAIC), where he worked approximately two years as a Senior Systems Security Engineer and provided information assurance and certification/accreditation support services for the Defense Information Systems Agency. Before he worked for SAIC, Mr. Rose was a software engineer for SPARTA.

### 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 12805, May 11, 1992, 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 primarily comprises Inspectors General (IGs) that the President appoints, and the ECIE primarily comprises IGs that agency directors appoint. The OIG at GPO is a member of the ECIE and participates regularly in the activities of that Executive Council.

During the previous reporting period, the Senate Appropriations Committee acknowledges in Senate Report 109-267, Legislative Branch Appropriations (2007), 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 recognizes the benefits of coordination and formal communication between and among IGs through the PCIE and ECIE and urges in the report that the legislative branch IGs communicate, cooperate, and coordinate with each other on an informal basis.

In response to the Committee's request, legislative branch IGs began coming together as a group. During this reporting period, both the Library of Congress IG and House of Representatives IG hosted a meeting. The meetings have helped establish formal communications and contact between the legislative branch IGs. In addition, the IGs are beginning to develop an inventory of unique skills in each of the various legislative branch OIGs. While such an inventory will provide a resource for identifying available personnel if the opportunity presents itself to share resources, more importantly, the process will help identify cross-training needs and perhaps even facilitate coordination on future audits applicable throughout the legislative branch. Quarterly meetings will rotate among the IG offices of the legislative branch. Updates and the progress of those meetings will be provided Congress in our respective semiannual reports.

The 9th Annual PCIE/ECIE Awards Ceremony was held on October 24, 2006 at the Andrew W. Mellon Auditorium in Washington, DC. Supervisory Auditor Joseph Verch and Senior Auditor Patricia Mitchell, the GPO Travel Audit Program Team, received an Award for Excellence in recognition of outstanding work in recommending improvements in management controls and business processes related to all aspects of the GPO travel program. Congratulations to Joe and Patricia.



*From left to right: Supervisory Auditor, Joseph Verch receives a PCIE/ECIE Award for Excellence from ECIE Vice Chairman and Federal Reserve Board Inspector General Barry Snyder.*

## Review of Legislation and Regulations

The OIG, in fulfilling its obligations under the Inspector General Act of 1978, 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 this area.

During this reporting period, the OIG commented generally to GPO management on the process for establishing, updating, and communicating GPO directives to Agency employees. The OIG urged that management maintain the legal integrity of the directives to ensure their effectiveness. While simplifying directives may make them easier to read, the OIG expressed concern that oversimplifying GPO directives could diminish their legal effectiveness and enforceability. Additionally, the OIG again urged GPO management to update the directive regarding the GPO workers' compensation program. The OIG previously made several recommendations regarding the workers compensation directive. The recommendations will be evaluated in the pending audit of the GPO workers' compensation program. While there were no legislative proposals relating to GPO programs and operations, the OALC, at the request of the ECIE, commented to the ECIE legislative committee regarding two bills recently introduced that would amend the IG Act.





## GPO Management Challenges

As GPO management understands, aggressive transformation efforts also pose substantial and difficult risks that could affect a smooth and successful transformation process. The OIG previously provided management a list of issues most likely to hamper the Agency's transformation efforts if not addressed with elevated levels of attention and resources. We again update the management challenges in this semiannual report and will continue to provide updates in future reports.

The former Public Printer, in his last two reports to Congress, acknowledged that the challenges were "vital to GPO's continuous transformation." Moreover, he noted 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 concur with that assessment and note that management continues to make progress.

In our last report, the OIG expressed concern with the Agency's acquisitions process. In this report, we raise that concern to a significant management challenge. We note below in more detail the importance of assembling a highly professional and trained contracting workforce skilled at carrying out nontraditional acquisitions.

We also note with interest the issue of a new facility for GPO. As previously reported, GPO 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 upkeep of the building 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. While the challenges associated with such a move will be significant for the Agency, Congress must still approve any relocation of GPO's operations. During a recent House Appropriations hearing, Members of Congress expressed interest in this issue and urged that the Agency continue to work closely with Congress toward approval. While the OIG has not performed a review of the proposed move, the information reviewed thus far supports significant savings in cost. 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 GPO's 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 made significant progress in implementing the provisions of the Government Performance Results Act (GPRA). While 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. While 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 advancing 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 its efforts to “right-size” the Agency workforce while at the same time attract 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 for ensuring that the Agency meets its ongoing workforce needs, in part by building a diverse, qualified applicant pool. In our last report, the OIG highlighted a need for a comprehensive telework program. Since that time, GPO established an Agency policy. While some issues still need resolving, establishing a telework program was an essential next step for successful long-term implementation and “buy-in” of the 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 requisite security requirements and understand the need for strict quality assurance and compliance in the passport production facility.

The results from the GPO Employee Survey released during this reporting period 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 these and other challenges as well as provides opportunities for improvement 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’s 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 already identified several vulnerabilities with the two projects and made recommendations 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 will continue IV&V efforts as the Oracle implementation continues. Other issues identified this year included customer billing. For example, KPMG LLP (KPMG), the Independent Public Accountant (IPA) conducting GPO’s annual financial statement audit, found several internal control issues related to customer billing in this year’s [FY 2006] audit. KPMG identified that some customers were duplicate billed by almost \$1 million in one instance and overbilled by approximately \$275,000 in another.

*4. Continuity of Operations.* An 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 (FPC) 65. GPO management must address this problem if it will 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 (FEMA) 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.

Although the Agency has taken these important initial steps, further steps must be taken to ensure a comprehensive COOP is in place. Steps include identifying, acquiring, and designating a backup facility for passport production. In addition, items such as identifying and pre-positioning minimum essential equipment and supplies at designated backup locations for critical Agency functions is also a critical requirement. Once it identifies the necessary facilities, supplies, personnel, and equipment, the Agency should run a real-time COOP exercise.

*5. Internal Controls.* GPO management is responsible for establishing and maintaining 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.

OIG audits during this reporting period again addressed issues with internal controls. For example, in a follow-on OIG audit of purchase cards we found that management and supervisory controls over GPO cardholder use and reporting of purchase card activities

need strengthening to ensure that purchase cards are used in an efficient and cost-effective manner by only authorized users and for legitimate GPO needs. We also found that controls related to the examination and payment process need improving to ensure that documentation supports purchase card transactions and that the transactions are properly reviewed and approved for payment by the appropriate authorities. In the audit, we identified several control problems related to purchase cards and recommended ways to strengthen controls over purchase card use and also ensure cards are used efficiently, cost effectively, for only documented GPO needs and in compliance with applicable laws, regulations, policies, and procedures.

The annual financial statement audit by KPMG identified several internal control issues and provided management with additional corrective actions. While GPO management recognizes the need to improve the current internal control environment if the Agency is to successfully implement its strategic vision, and has planned future initiatives in this area, management 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 Intelligence 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 had to re-examine its request for proposal (RFP) for production capability of smartcards. Although showing some progress in meeting unprecedented demand from the Department of State, the production of blank passports remains a significant concern from

a security and quality assurance perspective. A recent misprint resulted in the loss of numerous electronic passports at a significant cost to GPO. The issue highlights serious security and product integrity concerns and underscores the need for quality manage-

ment independent from production. The OIG will carefully review those issues in upcoming reporting periods. The passport production facility underwent an external physical security review and the results of that review will be forthcoming. Redesign of the production area to enhance security, while reported as underway in our last report, requires attention.

Although other concerns received significant attention, several matters must remain a priority for GPO management. Among those concerns are finalizing a Memorandum of Understanding with the Department of State, 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 focus on these during the next reporting period. SID also continues to advance its plan to provide Homeland Security Presidential Directive-12 (HSPD-12) credentialing services to Federal agencies. To realize the benefits from such an opportunity, management must continue to ensure the necessary procurement and related support to SID.

*7. Supporting Congressional Printing.* In recent months, the 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 include changes in staffing, reorganization of the workforce, use of “use-it-or-lose-it” leave during critical times, and various IT matters.

Indeed, GPO management took seriously the issues JCP raised and responded to their concerns. Some of the issues raised appear to be systemic, and GPO management must identify long-term solutions for the concerns of GPO’s principal customer. Moreover, the solutions must also employ strategies for continued process improvement

#### *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 becomes critical to the success of the GPO vision and mission. The 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 impact analysis. Legacy systems increasingly inhibit GPO 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 the Federal Information Security Management Act (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 and as well as personal information.

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 of GPO. The GPO 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 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 controls over its PKI Certificate Authority operations are fairly stated based on underlying principles and evaluation criteria. During FY 2007, the OIG is leading an assessment of GPO compliance with FISMA in order to identify gaps and deficiencies in the Agency's overall information security program as well as specific critical Agency systems. 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 the Digital Content Management System.

*9. Customer Service.* As GPO moves closer to its goal of transforming to a 21<sup>st</sup> century information and 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. Acquisition.* GPO is currently in the implementation planning phase of FDSys, which is envisioned as being 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 this approximately \$29 million system is critical to the Agency's future as a 21<sup>st</sup> century information processing and dissemination operation.

In our previous semiannual report, the OIG stated that we are increasingly 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, we are elevating our concern to a management challenge for GPO management to consider as they review the organizational and staffing issues confronting the Agency. We concur with management's decision during the last reporting period to separate Acquisition Services from Customer Services and having this group report directly to the Deputy Public Printer. While we note that management hired a Technical Procurement Manager to focus on complex acquisitions, we also believe that the Agency needs to move out in recruiting a Chief Acquisition Officer experienced in the FDSys-type of acquisitions.



GOVERNMENT PRINTING OFFICE

710

## Office of Audits and Inspections

OAI, as required by the Inspector General Act of 1978, as amended, conducts independent and objective performance and financial audits relating to GPO operations and programs, and oversees the annual financial statement audit performed by an independent public accounting firm under contract. In addition, OAI 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 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. Those reports made a total of 30 recommendations for improving GPO operations, including strengthening of internal controls throughout the Agency. OAI also continued to work with GPO management to close open recommendations carried over from previous reporting periods. As of March 31, 2007, 31 recommendations remain open. The number of open recommendations has decreased significantly from the 54 open as of the completion of the last semiannual reporting period. Based on our assessment of management's ongoing actions related to COOP and Oracle implementation, we believe that a significant number of these remaining open recommendations from previous periods will be closed during the next reporting period.

This reporting period also saw GPO receive an unqualified opinion on its FY 2006 financial statements audit. This audit, performed under contract with KPMG, is overseen by OAI as the Contracting Officer's Technical Representative (COTR). OAI also earned an unqualified opinion on a peer review of the office's

operations that the OIG for the National Science Foundation conducted.

### B. Audit Accomplishments – Audit and Inspection Reports

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

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

The OIG is conducting ongoing IV&V activities associated with GPO's 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). In advance of IOC implementation, GPO initiated early implementation start-up projects to become familiar with Oracle technology and work process dependencies as well as develop successful project skills and user requirements. The OIG initiated IV&V activities beginning with two of the early implementation projects. The objective of IV&V is to provide GPO with an independent assessment of project status, satisfy user needs, and project cost effectiveness. To conduct IV&V, the OIG contracted with a nonprofit, scientific research and engineering corporation that operates in the public interest.

The OIG issued a sensitive report summarizing vulnerabilities identified during the IV&V activities. That report includes recommendations to GPO management for strengthening controls and mitigating risks associated with those vulnerabilities. Management concurred with each of the recommendations and proposed responsive corrective actions. We considered management's actions and proposed actions responsive to the recommendations.

#### 2. Assessment Report 07-02 (Issued November 27, 2006)

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

GPO implemented 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 recently became cross-certified with the Federal Bridge Certificate Authority (FBCA), whose certification provisions require that the GPO PKI undergo a compliance review. To satisfy this compliance requirement, the OIG tasked an IPA firm to conduct a WebTrust assessment of its Certification Authority (CA). 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 assertions related to the adequacy and effectiveness of controls over its CA operations is fairly stated based on underlying principles and evaluation criteria.

GPO management performed a pre-assessment designed to identify gaps and deficiencies between the current GPO PKI environment and the required criteria of the WebTrust Program for CA. During the final WebTrust phase, controls were tested to gather support for an opinion regarding compliance with applicable WebTrust principles and criteria for certification. As a result of work performed in the final WebTrust phase, 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. Assessment Report 07-03 (Issued November 29, 2006)**

#### *Report on GPO PKI Certification Practices Statement Compliance with the Federal Common Policy Framework*

As part of GPO's application to the Federal Identity Credentialing Committee (FICC) Shared Service Provider (SSP) Subcommittee in which it seeks to obtain certification and accreditation as a qualified bidder for providing managed PKI services, GPO must submit a report from its PKI compliance auditor that the GPO Certificate Practices Statement (CPS)

complies with the Government's *X.509 Certificate Policy for the Common Policy Framework (CCP)*. To satisfy that requirement, the OIG contracted with an IPA firm licensed by the AICPA to provide PKI-related assurance services. Between October 30, 2006, and November 17, 2006, the IPA examined GPO's CPS version 1.7 to determine whether GPO's assertions regarding controls over its Certification Authorities were fairly stated based on underlying principles and evaluation criteria. The IPA issued an unqualified opinion that GPO's CPS complied, in all material respects, with the CCP as of November 10, 2006.

### **4. Audit Report 07-04 (Issued March 30, 2007)**

#### *Follow-On Report on GPO Purchase Card Program*

The General Services Administration (GSA), through a contract with the Bank of America, provides GPO with purchase cards for employees to make purchases for official Government use. The purchase card program is intended to provide the Government with financial and cash management control over low-dollar, high-volume procurements. GPO employees use the purchase cards for various purposes, including purchasing supplies and services, emergency requirements, or to support production and field activities. Use of purchase cards by GPO has experienced steady growth since its inception in FY 1997 when 47 cardholders charged \$130,788 to 94 cardholders charging \$1,322,758 during the first 7 months of FY 2006 (as of April 30, 2006).

During this reporting period, the OIG performed a second audit evaluating the effectiveness of GPO's purchase card program. The objectives of this audit were to (1) determine whether purchase cards are used efficiently and cost effectively, and (2) evaluate the effectiveness of the examination and payment process for purchase card transactions. The OIG found that management and supervisory controls over GPO cardholder use and reporting of purchase card activities need strengthening to ensure that purchase cards are used in an efficient and cost-effective manner, by only authorized users, and for legitimate GPO needs. In addition, controls related to the examination and



payment process need improving. Improving controls will ensure that purchase card transactions are supported by documentation and are properly reviewed and approved for payment by the appropriate authorities. The audit specifically identified that:

- (1) Unauthorized personnel in GPO's Central Office have used purchase cards;
- (2) Cardholders purchased goods and services that were neither required by nor applicable to the needs of the cardholder's branch, division, or office;
- (3) Cardholders were not always maintaining required records such as invoices, receipts and purchase logs to support purchases being made;
- (4) GPO employees were incurring state and local sales taxes on purchases made with purchase cards that were otherwise tax-exempt;
- (5) GPO purchase cards were being used for making recurring, large-dollar charges to the same vendors, potentially circumventing established procedures for congressional review and approval;
- (6) Procedures related to the review and approval of monthly bank statements detailing the charges made by cardholders were not always being followed; and
- (7) Two GPO cardholders were having monthly bank statements sent to home addresses, and in some instances purchased goods were delivered to home addresses.

The OIG recommended to GPO management that it strengthen management and supervisory controls over GPO purchase card use as well as ensure that cards are used efficiently, cost effectively, for only documented GPO needs, and in compliance with applicable laws, regulations, policies and procedures. Management concurred with each of the recommendations and will implement corrective actions.

## 5. Assessment Report 07-05 (Issued March 31, 2009)

### *Report on Peer-to-Peer File Sharing*

GPO Policy 825.29A, *Internet and E-Mail Policy, Section 7b (12)*, prohibits the "unauthorized acquisition, using, reproducing, transmitting, or distributing of any controlled information. Such information includes computer software and data that contains privacy information, or is copyrighted or trademarked, or material with other intellectual property rights (beyond fair use)." Peer-to-Peer (P2P) file sharing has been a way of sharing files since mid-1999, and since that time its use has grown dramatically.

Although it can be used for legitimate purposes, such as software collaboration, P2P file sharing is often used for the inappropriate or illegal exchange of files. P2P file sharing has even been used to post sensitive Federal Government documents to the Internet. P2P software is easy to use and acquire. To potentially acquire illegally distributed copyrighted as well as inappropriate or offensive material, users need only install no-cost P2P client software and enter a search string. Illegal file exchange through P2P networks has become so common that organizations such as the Recording Industry Association of America have pursued legal action against users of P2P software.

An OIG assessment of P2P file sharing found that GPO's Internet and e-mail policies establish the foundation for monitoring and prohibiting P2P activities. However, the OIG identified a P2P file distribution protocol being used within the GPO network domain. Use of P2P file-sharing software can increase GPO's IT risks in several ways. Some P2P client software has known vulnerabilities that can easily be exploited remotely and thus compromise the system on which the software is installed. Improper configuration of P2P software makes it possible for a user to inadvertently share all files on a computer and network drives with other P2P users. Additionally, illegally distributing copyrighted material to or from GPO computers could embarrass the Agency or potentially involve it in litigation with copyright holders. We recommended in our report that GPO management

further strengthen controls over P2P. Management concurred with our recommendations and proposed responsive corrective actions.

### **C. Financial Statement Audit Activity**

Section 309, title 44 of United States Code requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. Under a multiyear contract, KPMG was retained to conduct this audit. 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 for the KPMG auditors administrative support and coordination with GPO management.

During this reporting period, KPMG completed the FY 2006 audit of GPO's consolidated financial statements. KPMG issued an unqualified opinion, stating that GPO's financial statements were presented fairly, in all material respects, in conformity with generally accepted accounting principles. KPMG identified several reportable conditions, including (1) controls surrounding the billing process should be strengthened, (2) certain reconciliation controls should be strengthened, (3) controls over recording and reporting environmental liabilities should be improved, and (4) general controls for IT should be improved. KPMG made recommendations for addressing each condition. GPO management concurred with those recommendations and has either planned or initiated responsive corrective actions.

### **D. Peer Review**

During this reporting period, the National Science Foundation conducted a review of OAI's audit operations. The peer review was in accordance with the guidelines that the PCIE and ECIE establish. The objective of the peer review was to determine whether the internal quality control system was adequate as designed as well as complied with, and provided reasonable assurance that applicable auditing standards, policies, and procedures were met.

The National Science Foundation issued an unqualified opinion, stating that the OAI's system of quality control in effect for the year ending March 31, 2006, met the quality control standards the Comptroller General of the United States established for a Federal Government audit organization and that the quality control conformed to applicable auditing standards, policies, and procedures.

### **E. Status of Open Recommendations**

GPO management officials continued to make significant progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. Specifically, GPO management worked to close a significant number of open recommendations. For 31 recommendations remaining open, a summary of the finding and recommendations, along with the status of actions for implementing the recommendation and OIG comments, appear below.

#### **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 weaknesses identified in the business processes used for producing blank passports that are relevant to all documents and operations within GPO's 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 four of the eight open recommendations. Management is working on implementing corrective actions for the remaining four 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 a 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 our 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 GPO's enterprise network. Those recommendations should reduce the risk of compromise to GPO data and systems. Based upon 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

Corrective actions for the three remaining recommendations are in progress. The OIG is working with GPO management and monitoring implementation of the remaining three 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 to mitigate the risks associated with those vulnerabilities. The vulnerabilities identified during the assessment included: (1) top management support was not aligned with program execution; (2) inadequate functional and technical staffing existed; (3) the program lacked a methodology for organizational restructuring; (4) the program did not have targeted performance metrics; and (5) the program lacked an effective method of managing the progress of the program.

#### 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

We closed one recommendation from this report relating to the appointment of an Executive Steering Committee to oversee the Oracle Program. Management satisfied this recommendation by

appointing an Executive Sponsor along with assigning responsibilities to the Planning and Strategy Board and Operating Committee. Implementation of the remaining 12 recommendations was delayed pending hire of an Oracle Program Manager, which occurred in March 2007. With the new manager now on board, we anticipate progress during the next reporting period toward closing the remaining open recommendations.

#### **4. Inspection Report 06-04 (Issued March 31, 2006)**

*Inspection of GPO's Continuity of Operations Plan*

##### **Finding**

The objective of the inspection was to evaluate GPO's existing processes, procedures, and authorities against Federal Government best practices for maintaining essential functions in the event of a disaster or other significant adverse event. We evaluated GPO's COOP plan against the FEMA FPC-65, "Federal Executive Branch Continuity of Operations." FPC-65 is the model for best practices within the Federal Government. *Because of the sensitive but unclassified nature of the inspection, we are limiting our discussion of findings for purposes of this report. Further details regarding the inspection's findings can be obtained by contacting the OIG.*

##### **Recommendation**

The OIG made 18 recommendations that should improve GPO's plans and procedures for reasonably ensuring a viable COOP capability in the event of a disaster or other significant adverse event. GPO management concurred with each recommendation.

##### **Management Comments**

GPO management concurred with each recommendation and initiated responsive corrective actions. The actions management took and plans generally provide the initial framework for establishing and maintaining

a viable COOP plan in the event of a disaster or significant adverse event. GPO has a comprehensive draft COOP plan based on the FEMA template of key COOP components. The draft plan addresses essential functions, interoperable communications, delegations of authority, testing, training, and exercises. The Agency has also developed an OEP as a companion to the COOP. The OEP establishes the appropriate response in the event of an emergency and addresses all known or anticipated categories of emergencies.

##### **OIG Comments**

During this reporting period, five of the 17 open recommendations were closed. The OIG is working with GPO management to monitor implementation of the remaining 12 open recommendations.

HOUSE LIBRARY

PROPERTY OF THE

U. S. GOVERNMENT

HEARINGS

SENATE

HEARINGS

COMMITTEE

RECORD

HOUSE LIBRARY

106TH CONGRESS

1st SESSION

COMMITTEE ON APPROPRIATIONS

H. OF R.

SENATE LIBRARY

SENATE LIBRARY



UNITED STATES  
GOVERNMENT  
PRINTING OFFICE

## 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, GPO management, or other GPO employees. Special Agents in OI are Federal Criminal Investigators (job series 1811). Investigators are also designated as Special Police Officers in accordance with subsection 317, title 44 of the United States Code. Investigations that uncover violations of Federal law or GPO rules or regulations may result in administrative sanctions or civil or criminal prosecution, or both. OI also issues Management Implication Reports that identify issues uncovered during an investigation that it believes warrant prompt attention by GPO management. Prosecutions may result in court-imposed prison terms, probation, fines, or restitution.

### A. Summary of Investigative Activity

During this reporting period and in response to 298 new complaints or allegations, OI opened 25 investigative cases and closed 32 matters. Thirty-one of the investigative matters are on-going. OI works with GPO offices throughout the country. During this reporting period, OI issued three administrative subpoenas.

### B. Types of Cases

The OI's investigative workload includes the following major categories:

#### Office of Workers' Compensation Program (OWCP)

The OI investigates GPO employees who have allegedly submitted false claims and made false statements to facilitate receiving workers' compensation benefits. We are working on ten investigations involving alleged OWCP fraud.

#### Procurement Fraud

OI investigates allegations of statutory violations involving GPO contract service providers defrauding

the Government in connection with GPO's procurement of printing goods and services. These violations include, but are not limited to, false claims, false statements, wire and mail fraud, product substitution, and Small Disadvantaged Business Program violations. OI has eight open cases involving procurement fraud.

#### Employee Misconduct

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

#### Miscellaneous

OI investigates miscellaneous administrative allegations and other types of investigations that do not fall into one of the above categories, for example theft of Government property or illegal hacking. OI has seven open cases involving miscellaneous matters.

### C. Status of Action on Referrals

OI's investigative efforts result in both external and internal referrals for action. A summary of the status of outstanding referrals by the OI follows.

#### External

We referred five investigative matters to the Department of Justice for prosecution. Prosecutorial actions are pending on two matters referred from previous reporting periods. Those two matters are:

- ♦ The Department of Justice accepted for criminal prosecution one OWCP investigation.
- ♦ The Department of Justice accepted for civil action one matter dealing with fraud.

#### Internal

A total of four investigative matters referred to GPO management for action remain pending. In addition, GPO management resolved 12 investigative cases from previous reporting periods. Agency action in

response to the investigation findings included two suspensions, nine verbal warnings, and one resignation in lieu of adverse personnel action.

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 letters of warning.

#### **D. Investigative Accomplishments**

- ◆ An OI investigation into the theft of approximately 4,430 printer ink cartridges valued at \$111,000 resulted in one of the individuals pleading guilty to theft of Government property. One individual was sentenced to 5 months in jail, 180 days of home detention, 3 years supervised probation, and ordered to pay \$111,025 in restitution to GPO. The other individual pled guilty to trafficking in stolen property and was sentenced to 2 years probation as well as ordered to make restitution of \$6,197 to GPO. Both individuals resigned from GPO before their convictions.
- ◆ An OI investigation into allegations of sexual harassment and abuse of a contractor employee by a supervisory GPO employee resulted in the GPO employee resigning his position in lieu of adverse personnel action by the Agency.
- ◆ An OI investigation of a contractor opened in a previous reporting period and accepted by the Department of Justice is still pending. The contractor is alleged to have filed false claims and statements in connection with contracts valued at approximately \$438,000.
- ◆ Efforts in OWCP fraud investigations have led to an actual cost savings of \$656,400 for the Agency. One OI investigation resulted in ordering restitution totaling \$947,000 in fraudulent OWCP claims.
- ◆ An investigation into Federal Employee Compensation Act (FECA) fraud and accepted for criminal prosecution by the Department of Justice remains pending. The employee pleaded guilty. Sentencing is scheduled for the next reporting period. This matter has already resulted in savings of \$2,250 per year. Final disposition could result in cost savings of \$60,000 per year.
- ◆ An investigation into a GPO employee's use of a Government vehicle for personal use resulted in the employee receiving a 30-day suspension.
- ◆ As a result of an OI investigation into certification of fraudulent firearms qualifications scores of Federal police officers, two employees received verbal warnings.
- ◆ An OI investigation into alleged travel voucher and overtime fraud resulted in the issuance of seven verbal warnings to GPO employees.
- ◆ As a result of OI investigative efforts, the Agency issued two letters of warning to agency printing contractors.

#### **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.





Congressional Record

VOL 107  
PART 13  
1967 to 1967

70th CONGRESS  
1st SESSION  
JULY 25, 1967  
TO  
OCTOBER 1, 1967

Congressional Record

VOL 103  
PART 11  
1955 to 1956

83rd CONGRESS  
1st SESSION  
JULY 2, 1955  
TO  
OCTOBER 1, 1955

Congressional Record

VOL 107  
PART 10  
1962 to 1967

89th CONGRESS  
1st SESSION  
JULY 17, 1966  
TO  
JULY 25, 1967

Congressional Record

VOL 112  
PART 21  
1969 to 1969

91st CONGRESS  
2d SESSION  
OCTOBER 20, 1968  
TO  
OCTOBER 22, 1968

Congressional Record

VOL 103  
PART 10  
1955 to 1955

84th CONGRESS  
1st SESSION  
JULY 26, 1957  
TO  
AUG 2, 1957

## 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.

**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

<b>CFO</b>	Chief Financial Officer	<b>IG Act</b>	Inspector General Act of 1978
<b>CIO</b>	Chief Information Officer	<b>IOC</b>	Incremental Operating Capabilities
<b>COOP</b>	Continuity of Operations	<b>IT&amp;S</b>	Information Technology and Systems
<b>COTR</b>	Contracting Officers Technical Representative	<b>IV&amp;V</b>	Independent Verification and Validation
<b>CPS</b>	Certificate Practices Statement	<b>JCP</b>	Joint Committee on Printing
<b>ECIE</b>	Executive Council on Integrity and Efficiency	<b>MMAR</b>	Materials Management Acquisition Regulation
<b>FDLP</b>	Federal Depository Library Program	<b>OAI</b>	Office of Audits and Inspections
<b>FDsys</b>	Future Digital (content) System	<b>OEP</b>	Occupant Emergency Plan
<b>FICC</b>	Federal Identity Credentialing Committee	<b>OI</b>	Office of Investigations
<b>FISMA</b>	Federal Information Security Management Act	<b>OIG</b>	Office of Inspector General
<b>FSA</b>	Financial Statement Audit	<b>OWCP</b>	Office of Workers' Compensation Program
<b>FY</b>	Fiscal Year	<b>P2P</b>	Peer-to-Peer
<b>GAO</b>	Government Accountability Office	<b>PCIE</b>	President's Council on Integrity and Efficiency
<b>GAGAS</b>	Generally Accepted Government Auditing Standards	<b>PKI</b>	Public Key Infrastructure
<b>GPO</b>	U.S. Government Printing Office	<b>RFP</b>	Request for Proposal
<b>GSA</b>	General Services Administration	<b>SA</b>	Special Agent
<b>HSPD-12</b>	Homeland Security Presidential Directive-12	<b>SAIC</b>	Science Applications International Corporation
<b>IG</b>	Inspector General	<b>SID</b>	Security and Intelligent Documents
		<b>SSP</b>	Shared Services Provider

## 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	4
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	6-10
Section 5(a)(2)	Recommendations for Corrective Actions	6-10
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	15-17
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	20-21
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 for Funds That Can Be Put To Better Use)	12-15
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned and unsupported costs	26
Section 5(a)(9)	Statistical table showing the total number of audit reports and the dollar value of recommendations for funds that can be put to better use	27
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	\$0	\$0	\$0
Subtotals	\$0	\$0	\$0
Reports for which a management decision made during reporting period			
1. Dollar value of disallowed costs	\$0	\$0	\$0
2. Dollar value of allowed costs	\$112,927	\$63,935	\$176,322
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 <ul style="list-style-type: none"> <li data-bbox="142 900 706 967">♦ Dollar value of recommendations agreed to by management</li> <li data-bbox="142 996 706 1064">♦ Dollar value of recommendations not agreed to by management</li> </ul>	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 Early Oracle Implementation: Independent Verification and Validation (IV&V) (Assessment Report Number 07-01, issued 11/20/06)	\$0
Report on WebTrust Assessment of GPO's Certification Authority—Attestation Report (Assessment Report Number 07-02, issued 11/27/06)	\$0
Report on GPO PKI Certification Practices Statement Compliance with the Federal Common Policy Framework (Assessment Report Number 07-03, issued 11/29/06)	\$0
Follow-On Report on GPO Purchase Card Program (Audit Report Number 07-04, issued 03/30/07)	\$0
Report on Peer-to-Peer (P2P) File Sharing (Assessment Report Number 07-05, issued 03/31/07)	\$0
Total	\$0

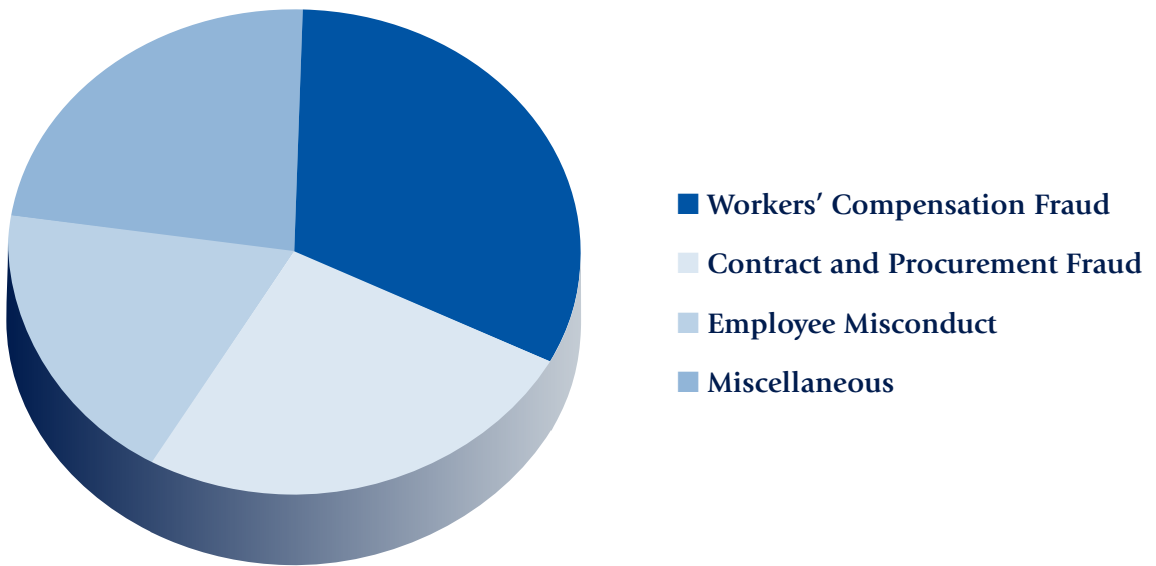
**Table C-4: Investigations Case Summary**

---

Cases Open at Beginning of Reporting Period	38
<hr/>	
Total New Hotline / Other Complaints Received during SAR Period	298
<hr/>	
Cases Opened by OI	25
<hr/>	
Cases Closed during Reporting Period	32
<hr/>	
No Formal Investigative Action Required	273
<hr/>	
Cases Open at End of Reporting Period	31
<hr/>	
♦ Cases Referred to GPO Management that remain pending	4
<hr/>	
♦ Cases Referred to Other Agencies	0
<hr/>	
♦ Cases Referred to Office of Audits and Inspections	2
<hr/>	



Current Case Openings by Allegation	31	
◆ Contract and Procurement Fraud	8	26%
◆ Employee Misconduct	6	19%
◆ Workers' Compensation Fraud	10	32%
◆ Miscellaneous	7	23%



**Table C-5: Investigations Productivity Summary**

Arrests	1
Total Cases Presented to Prosecuting Authorities	5
Criminal	5
Criminal Declinations	5
Convictions	2
Guilty Pleas	3
Probation (days)	1,825
Jail Time (days)	1,825
Restitutions	\$117,222
Civil	0
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	\$947,782
Total Agency Cost Savings Through Investigative Efforts	~ \$656,400
Total Administrative Referrals	5
Contractor Debarments	0
Contractor Suspensions	0
Contractor Other Actions	2
Employee Suspensions	1
Employee Terminations	0
Employee Warned/Other Actions	11
<b>Other Law Enforcement Agency Referrals</b>	<b>0</b>





**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**