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

Semiannual Report to Congress

April 1, 2013 Through September 30, 2013

About the Government Printing Office ...

GPO is the Federal Government's primary resource for producing, procuring, cataloging, indexing, authenticating, disseminating, and preserving the official information products of the U.S. Government in both digital and tangible formats. GPO is responsible for producing and distributing information products and services for all three branches of the Federal Government, including U.S. passports for the Department of State as well as official publications of Congress, the White House, and other Federal agencies. In addition to publication sales, GPO provides for permanent public access to Federal Government information at no charge through GPO's Federal Digital System (FDsys [www.fdsys.gov]) and through partnerships with approximately 1,200 libraries nationwide participating in the Federal Depository Library Program (FDLP).

And the Office of Inspector General ...

The Office of Inspector General (OIG) helps GPO effectively carry out its responsibilities by promoting economy, efficiency, and effectiveness in the administration of GPO programs and operations, designed to prevent and detect fraud, waste, and abuse in those programs and operations.

The GPO Inspector General (IG) Act of 1988, title II of Public Law 100-504 (October 18, 1988) establishes the responsibilities and duties of the IG. OIG, located in Washington, D.C., has 22 employees and is organized into 2 line elements—the Office of Investigations and the Office of Audits and Inspections. Through audits, evaluations, investigations, inspections, and other reviews, OIG conducts independent and objective reviews of Agency programs and helps keep the Public Printer and Congress informed of problems or deficiencies relating to administering and operating GPO.

Online Availability

This report is also available on our Web site: http://www.gpo.gov/oig/semi-annual.htm

To access other OIG reports, visit: http://www.gpo.gov/oig/.

A Message from the Inspector General

I am pleased to submit this Semiannual Report to Congress, which highlights the most significant activities and accomplishments of the OIG for the 6-month period ending September 30, 2013.

As always, the OIG team of dedicated and professional staff is committed to helping GPO—the accomplishments reported here are the direct results of the team's efforts.

We worked with GPO, Congress, and other Federal agencies to ensure the integrity and efficiency of GPO programs and operations, safeguarding taxpayer investments in those programs, and investigating anyone allegedly abusing GPO programs.

During this reporting period, we issued 15 audit and investigative reports and memoranda, which, among other things, recommended that $6.4 million in funds be put to better use, and made 5 program improvement recommendations. Our investigative work led to cost efficiencies totaling $282,633, and included 1 arrest, 3 referrals to management for potential debarment actions, and 12 referrals to management for potential personnel action, corrective action and/or information purposes. The OIG also conducted two peer reviews of other OIGs during this reporting period.

I thank the Public Printer and other senior GPO officials for their support of our work and their receptiveness for improving Agency programs and operations. We look forward to continuing our partnership with GPO and Congress in the months ahead to meet the many challenges GPO faces.

Michael A. Raponi
Inspector General

Contents

Selected Statistics

Audits and Inspections	
Audits and other reports issued	5
Funds put to better use	$6.4 million
Number of Recommendations Made	5

Investigations	
Investigative cost efficiencies, restitutions, fines, and penalties	$282,633
Arrests	1
Complaints opened	53
Complaints closed	47
Investigative cases referred for prosecution	3
Investigative cases referred for administrative/civil action	3
Investigative cases closed	3
Debarment Referrals	3

Management Challenges

The Reports Consolidation Act of 2000 requires that OIG identify and report annually on the most serious management challenges the Agency faces. To identify management challenges, we routinely examine past audit, inspection, and investigative work, as well as include in our reports where corrective actions have yet to be taken; assess ongoing audit, inspection, and investigative work to identify significant vulnerabilities; and analyze new programs and activities that could pose significant challenges because of their breadth and complexity.

During its last reporting period, OIG identified areas considered particularly vulnerable to management oversight, error, fraud, waste, or abuse. We presented six management challenges: (1) keeping focus on its mission of information dissemination, (2) addressing emerging workforce skills, (3) improving the enterprise architecture and infrastructure to support enterprise-wide and FDsys transformation, (4) securing IT systems and protecting related information assets, (5) managing workers' compensation programs, and (6) improving print procurement programs.

For each challenge, OIG presents the challenge and our assessment of GPO's progress in addressing the challenge.

Changes from Previous Reporting Period

No changes were made to the Top Management Challenges from the previous reporting period.

Challenge 1: Keeping Focus on Its Mission of Information Dissemination

Overview: The transformation of GPO has been underway for several years. The trend of producing Government documents through electronic publishing technology and providing the public with Government documents through the Internet has affected all

of the programs at GPO and reduced production, procurement, and sales of printed products. Those areas have historically provided GPO with a vital source of revenue.

Challenge: Making operational and cultural changes that will keep GPO relevant and efficient while at the same time meeting the needs of its customers.

GPO's Progress: Since GPO's enhanced strategic planning efforts, Business Units report quarterly progress on key efforts. For the fourth quarter of FY 2013, GPO reported completing 49 of 61 (80 percent) of the key efforts for the year. GPO continues to develop an organizational model where the chief executive officer and managing directors focus their efforts on organizational policy and long-range planning and the second in command serves as chief operating officer focusing on the day-to-day operations of the business.

Challenge 2: Addressing Emerging Workforce Skills

Overview: As more Government information goes digital, GPO is likely to be confronted with a gap in workforce skills. GPO of today as well as tomorrow is clearly being defined by digital technology, and digital technology itself has radically changed the way printing is performed.

Another important product for which GPO is responsible is producing blank e-Passports for the Department of State. As the next generation e-Passport is developed, GPO facilities will need modification and upgrades will be put into place to support installation of new e-Passport production lines. Although at one time passports were no more than conventionally printed documents, today the documents incorporate electronic devices (chips and antennae array) upon which important information such as biometric identification data are maintained. The data, along with other security features, transformed e-Passports into the most secure identification credential.

GPO has also developed a line of secure identification "smart cards" that help support credential requirements of the Department of Homeland Security and other agencies for certain border crossing documents. GPO is working closely with other Federal agencies to offer a wide range of smart card credential products and services in the areas of design, printing, manufacturing, and personalization to meet their requirements.

GPO is exploring new ways for users to interact with FDsys content by providing mobile-optimized access to FDsys and enabling direct interfacing with FDsys through Application Programming Interfaces.

Challenge: Developing effective strategies for addressing emerging issues related to potential labor and skills shortages as GPO continues its transformation to a digital-based platform.

GPO's Progress: GPO continues to further develop and update its workforce plan to better support transformation by adopting a more strategic view of human capital management and by having human resources officials work collaboratively with GPO managers. Human Capital reported working with senior GPO managers to prioritize training initiatives and ensure training was linked to the Agency's strategic plan.

Challenge 3: Improving the Enterprise Architecture and Infrastructure to Support Enterprise-wide and FDsys Transformation

Overview: GPO relies extensively on computerized information systems and technology to support its transformation. The Government classifies Enterprise Architecture as an

IT function and defines the term not as the process of examining the enterprise but as the documented results of that examination. Specifically, chapter 36, title 44 of the United States Code defines enterprise architecture as a "strategic information base" that defines the mission of an agency and describes the technology and information needed to perform that mission, along with descriptions of how the architecture of the organization should be changed in order to respond to changes in the mission. GPO's FDsys provides free online access to official information for the three branches of the Federal Government. FDsys includes all of the known Government documents within the scope of GPO's Federal Depository Library Program (FDLP).

GPO systems contain vital information central to the GPO mission and to effective administration of its programs. Providing assurances that IT systems will function reliably while safeguarding information assets—especially in the face of new security threats, IT developments, and telework requirements—will challenge Federal agencies for years to come. The GPO goal of using technology for creating and maintaining an open and transparent Government has added to the challenge of keeping information secure.

Challenge: Existing Enterprise Architecture and IT infrastructure needs to be able to support the changes and increasing demands that GPO anticipates, including more support for mobile applications addressing the expanding market of e-readers and smart phone users.

Safeguarding information assets is a continuing challenge for Federal agencies, including GPO. Compromise of GPO's data or systems could cause substantial harm to GPO, negatively impact operations, and lead to identity theft or other fraudulent use of information.

GPO's Progress: GPO continues its work related to Enterprise Architecture and IT Infrastructure. GPO reported progress with modernizing legacy applications, GPO's data center consolidation and modernization, and making strategic investments that will strengthen GPO operations. GPO continues to address security issues such as access and configurations. Challenges are made more difficult by the nature of major IT system developments, which typically occur over multiple years and are subject to changes in policy, priorities, funding, and innovations in technology.

Challenge 4: Managing Workers' Compensation Programs

Overview: The Federal Employees' Compensation Act (FECA) Program provides wage-loss compensation and pays medical expenses for covered Federal civilians and certain other employees who incur work-related occupational injuries or illnesses. It also provides survivor benefits for a covered employee's employment-related death.

The Department of Labor administers the FECA Program and makes all decisions regarding eligibility of injured workers to receive workers' compensation benefits. The Department of Labor also provides direct compensation to medical providers, claimants, and beneficiaries. In addition to paying an administrative fee, GPO reimburses the Department for any workers' compensation claims. It also reports that the FECA Program is susceptible to improper payments.

The accounting treatment for actuarial estimated long-term workers' compensation liabilities at GPO is based on application of Statements of Federal Financial Accounting Standards No. 5, "Accounting for Liabilities for the Federal Government," and Statement of Financial Accounting Standards No. 112, "Employers' Accounting for Postemployment Benefits." Application of those accounting standards to unfunded costs (that is, accrued

long-term workers' compensation benefits) conflicts with the legislative intent of title 44 of the Code of Federal Regulations, to match GPO's costs and revenues through rates and prices charged customers. Recognizing the unfunded actuarial estimated cost as an operating expense without any matching revenues could cause an imbalance in the GPO Revolving Fund not intended by legislation when establishing this self-sustaining revolving fund for GPO's operations.

Challenge: For financial reporting purposes, future compensation estimates are generated from application of actuarial procedures that the Department of Labor developed for estimating the liability for FECA benefits. The liability for future compensation benefits includes the expected liability for death, disability, medical costs for approved compensation cases, and a component related to injuries incurred but not reported. Liability is determined using historic data for benefit payment patterns related to a particular period to estimate the ultimate payments related to that period.

From a program perspective, GPO remains challenged in identifying the full extent of improper payments in the FECA Program. As highlighted in past OIG audits, GPO is challenged in managing its FECA Program to control costs. The FECA Program at GPO must be responsive and timely to eligible claimants while at the same time ensuring that it makes proper payments. The challenges facing GPO include timely moving of claimants off the periodic rolls when they can return to work or when their eligibility ceases, preventing ineligible recipients from receiving benefits and preventing fraud by service providers or individuals who receive FECA benefits while working.

Because the Department of Labor develops liability estimates for FECA and is out of GPO's control, GPO is challenged with managing the risk that a relatively unexpected increase in the estimate could have significant unfavorable impact on GPO's financial results.

GPO's Progress: In a recent report, GPO agreed to strengthen FECA case management by: (1) ensuring GPO case files are complete, with sufficient initial medical evidence that will substantiate claims, obtain medical updates when required, obtain updated Form CA-1032s, and assign employees to limited duty consistent with the claimant's medically defined work limitation, and (2) once the required claim information is obtained, implement aggressive case management.

GPO also agreed to analyze in sufficient detail and develop a policy that provides consistent application of accounting standards promulgated by either the Federal Accounting Standards Advisory Board (FASAB) or the Financial Accounting Standards Board (FASB) in order to address the volatility of the FECA liability.

Challenge 5: Improving Print Procurement Programs

Overview: GPO is the principal agent for almost all Government printing. Title 44 requires that GPO accomplish any printing, binding, and blank-book work for Congress, executive branch offices, the Judiciary—other than the Supreme Court of the United States—and every Executive Office, independent office, and establishment of the Government. The only exceptions include: (1) classes of work that the Joint Committee on Printing (JCP) considers urgent or necessary to be completed elsewhere, (2) printing in field printing plants operated by an Executive Office, independent office, or establishment, and (3) procurement of printing by an Executive Office, independent office, or establishment from allotments for contract field printing, if approved by the JCP.

Challenge: GPO's identification of title 44 violations and working with executive branch agencies to prevent a loss of documents for the FDLP as well as preventing potential higher printing cost as a result of inefficient printing by Executive Office agencies.

GPO's Progress: GPO is working collaboratively with OIG on a current audit to estimate the cost of products an audit client obtained from sources other than GPO, whether those products met the criteria for inclusion in FDLP, and whether those products should have been cataloged and indexed.

Challenge 6: Uncertainties Related to Sequestration and Future Budgetary Caps

As part of the Budget Control Act of 2011, across-the-board cuts, also known as sequestration, were included for the purpose of compelling Congress to act on deficit reduction and reaching a budget compromise. With no compromise, the cuts were set to initially begin on January 1, 2013, but that date was postponed by 2 months by the American Taxpayer Relief Act of 2012. On March 1, 2013, the President issued a sequestration order canceling $85 billion in budgetary resources across the Federal Government for FY 2013. Those across-the-board budget reductions remained in effect for FY 2013 and will also result in lowering discretionary caps and sequestration of mandatory spending in the years 2014 through 2021.

The short-term impact of the sequestration or GPO's budget is a reduction of funds to the Office of Superintendent of Documents: Salaries and Expenses appropriation and a reduction to the Congressional Printing and Binding appropriation.

Challenge: While the size of the cut to GPO's appropriation may be reduced, what remains uncertain is the extent to which the impact on Federal agencies will result in reduced orders for printing and related information product services to GPO.

GPO Progress: GPO scenario managers place a high priority on managing the fiscal impact of sequestration and related budget constraints to ensure the continued provision of mission-critical products and services for Congress, Federal agencies, and the public. GPO successfully achieve positive monthly financial results throughout the year and avoided furloughing employees.

Transforming GPO into a Digital Platform

OIG Strategic Goal 1:
Assist GPO in meeting its strategic management goals related to transforming itself into a digital information platform and provider of secure documents to satisfy changing customer requirements in the present and in the future.

OIG conducts audits and investigations that focus on the effectiveness and efficiency with which GPO manages its assets. GPO is increasingly dependent on IT to efficiently and effectively deliver its programs and provide meaningful and reliable financial reporting.

Controls Over Information Security Management

One of the more significant dangers GPO faces is a cyber attack on its IT infrastructure, whether by terrorists seeking to destroy unique databases or criminals seeking economic gain.

OIG contracted with CliftonLarsonAllen LLP to assess GPO compliance with the Federal Information Security Management Act (FISMA) as it relates to continuous monitoring of the Passport Printing and Production System (PPPS). The objective was to assess the effectiveness of GPO's continuous automated monitoring controls over PPPS and whether GPO has an effective vulnerability scanning process for its networks and databases including a corrective action process for correcting known vulnerabilities.

The audit determined that during the past year, GPO's Office of Information Technology and Systems and Office of Security and Intelligent Documents made marked efforts to continuously monitor PPPS, including proactively testing various components of this multiplatform system. As part of its ongoing monitoring program, GPO periodically performed network scanning, targeted PPPS scans, and annually recertified and reaccredited this application.

Although vulnerability tests were periodically performed, additional work was still needed to ensure controls were in place and operating effectively.

Recommendation: We recommended that the Chief Information Officer and the Managing Director of the Office of Security and Intelligent Documents continue strengthening IT controls over PPPS. Management agreed with the recommendations and stated that it plans to implement these and other steps (PPPS Compliance with FISMA as it Relates to Continuous Monitoring, Report No.13-17, September 18, 2013).

Federal Public Key Infrastructure Compliance Report and WebTrust for Certification Authority

GPO operates as a Certification Authority (CA) known as the GPO Public Key Infrastructure (PKI) Certification Authority (GPO-CA) in Washington, D.C.

- PKI is a set of hardware, software, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
- In cryptography, CA is an entity that issues digital certificates.
- A digital certificate or identity certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

GPO implemented GPO-CA in support of meeting customer expectations regarding electronic information dissemination and e-Government, both of which require digital certification that documents within GPO's domain are authentic and official. PKI facilitates trusted electronic business transactions for Federal organizations and nonFederal entities.

GPO's PKI is cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification requires that GPO PKI undergo an annual independent compliance assessment. To satisfy that requirement, OIG contracted with Ernst & Young LLP (E&Y) to conduct an annual WebTrust examination. The review represents an evaluation of whether GPO's assertions related to the adequacy and effectiveness of controls over GPO-CA operations are fairly stated based on underlying principles and evaluation criteria.

Once again, we commend the management of GPO-CA for passing such a rigorous assessment. E&Y's opinion for the period July 1, 2012, through June 30, 2013, was that the GPO Principal Certification Authority Certificate Practices Statement conformed in all material respects to GPO-CA and the Federal PKI common policies, and GPO fairly stated management's assertion in all material respects based on the American Institute of Certified Public Accountants Trust Services Criteria for Certification Authorities.

Recommendation: The report did not contain any recommendations. (Federal PKI Compliance Report, Report No. 13-19, September 6, 2013, and WebTrust for Certification Authority, Report No. 13-18, September 6, 2013).

Operational and Financial Management

OIG Strategic Goal 2:

Promote economy, efficiency, and effectiveness in GPO operations by helping GPO managers ensure financial responsibility.

Establishing and maintaining sound financial management is a top priority for GPO because managers need accurate and timely information to make decisions about budget, policy, and operations. GPO prepares annual financial statements that must be audited by an independent entity.

Financial Accounting: Volatility of the Federal Employees' Compensation Act Actuarial Liability Estimate

The audit presents the results of our review of GPO's workers' compensation actuarial liability estimate, focusing on the discount rate model used to estimate the liability. Our objective was to determine whether opportunities existed to address the volatility associated with accounting for the FECA actuarial liability estimate.

The Department of Labor determines actuarial liabilities of agencies for future workers' compensation benefits for civilian Federal employees, as FECA mandates. The actuarial liability for future workers' compensation includes the expected liability for death, disability, medical, and miscellaneous costs for approved cases as well as an estimate for cases incurred but not reported. The Department of Labor follows accounting standards promulgated by the FASAB. Since October 1999, FASAB has been recognized as the standard-setting body for Federal Government entities. Those standards are also referred to as Federal Generally Accepted Accounting Principles (GAAP) or Federal GAAP.

GPO accounts for future workers' compensation costs not yet paid and reports the liability in its consolidated financial statements. GPO follows accounting standards promulgated by the FASB. FASB sets financial reporting standards for privately owned

entities in the United States. Those standards are also known as Commercial GAAP. As FASAB permits, GPO can follow either FASAB or FASB accounting standards.

The audit identified opportunities for addressing the volatility associated with accounting for the FECA actuarial liability estimate. The FECA actuarial liability estimate is reported in GPO's Consolidated Balance Sheets and any increase or decrease in the liability is reported in the Agency's Consolidated Statements of Revenues, Expenses, and Changes in Retained Earnings. With the exception of the FECA actuarial liability, GPO's consolidated financial statements are prepared in accordance with accounting standards promulgated by FASB (Commercial GAAP). The Department of Labor calculates the actuarial liability as prescribed by FASAB standards (Federal GAAP), which uses the Office of Management and Budget (OMB) economic assumptions for 10-year Treasury notes and bonds. Conversely, under FASB standards or Commercial GAAP, the current market rate is used to discount the payments to recognize the amount that could be paid currently to settle the liability. Combining accounting standards in such a manner is not consistent with generally accepted accounting practices. As of June 2013, GPO was still analyzing the switchover to accounting for the FECA actuarial liability using Commercial GAAP.

Reporting the actuarial liability in accordance with Commercial GAAP could increase volatility as well as negatively impact annual financial results. For example, using Commercial GAAP to report the liability would have resulted in a net income of approximately $1.4 million compared with a higher reported net income in FY 2011 of approximately $5.6 million. In FY 2012, however, a lower net income of approximately $2.8 million was reported compared with approximately $6.7 million that would have been reported following Commercial GAAP—differences of $4.2 million and $3.9 million for 2011 and 2012 respectively.

Recommendation: We recommended the Chief Financial Officer analyze in sufficient detail and develop a policy that provides consistent application of accounting standards promulgated by either the FASAB or the FASB. Management concurred with the recommendation. (Financial Accounting: Volatility of the Federal Employees' Compensation Act Actuarial Liability Estimate, Report No.13-14, August 7, 2013).

Print Procurement Programs

OIG Strategic Goal 3:

Strengthen GPO's print procurement programs that support other Government entities by providing quality and timely assessments.

Report of Structured Query Language Injection Incident

GPO's print procurement process relies on major legacy applications to generate random and rotating potential vendor lists for solicitations based upon order specifications, allow print procurement customers to place orders directly with a GPO contractor, format payment files to produce checks, provide order entry capability, order status, contractor performance history, quality records, exception reports, and order-tracking. One of the more significant dangers GPO faces is a cyber security attack on its IT infrastructure, whether by terrorists seeking to destroy unique databases or criminals seeking economic gain. If an incident were to occur, GPO could experience anywhere from minor delays to major service disruptions.

An OIG investigation revealed that GPO may have been a victim of a Structured Query Language (SQL) injection scan during the period January through July 2013. SQL injection is a type of security exploit in which the attacker adds SQL code to a Web form input box to gain access to resources or make changes to data. Most Web forms do not have mechanisms in place that block input other than names and passwords. Unless such precautions are taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways. SQL Injection allows an attacker the capability of creating, reading, updating, altering, or deleting data stored in the back-end database.

We notified Information Technology & Security (IT&S), who has primary responsibility at GPO for IT security. IT&S was not aware of the incident and had not identified any related security exploits. In response to our notification, IT&S blocked the reported Internet Provider (IP) addresses, reviewed sensor logs, firewall logs, Web server logs, and daily logs for the suspected IP address.

In February 2013, OIG reported possible risks associated with this major application. At that time, we recommended that IT&S conduct risk assessments that included, at a minimum, assessment of the sensitivity of data, threats, vulnerabilities, and effectiveness of current/proposed safeguards, and document the risk assessments.

Management stated that the recommendations were reasonable activities generally requiring long-term remediation actions and requiring a significant investment by GPO. Management either concurred or partially concurred with the recommendations. Partial concurrence was based on budgetary limitations.

Outcome: The prior recommendation remains open. Therefore, we did not make a recommendation in our current referral to GPO. *(Audit of Computer Security: GPO's Risk Acceptance Process for Major Legacy and Minor Applications, Report No.13-05, February 13, 2013, and Case No. 13-0053-C).*

Vendor Falsifies Documents

An OIG investigation revealed that a vendor doing business with GPO for approximately 25 years, falsified five documents. The vendor submitted four invoices using the identical verification of shipment document for each of the four invoices. The vendor admitted

falsifying the four documents. Two of those invoices were submitted before the purchase order was complete, resulting in premature payment. The stated number of items on each invoice was incorrect. Furthermore, the vendor submitted a false weekly compliance report, stating that several jobs jackets were completed when, in fact, they were not.

Outcome: In August 2013, the OIG referred the vendor to GPO for suspension and/or debarment after our investigation revealed the vendor willfully falsified documents. The GPO Suspending and Debarring Official (SDO) suspended both company and its owner/operator from doing business with GPO until GPO renders a final decision. (*Case No. 13-0005-I*).

Vendor Violated Terms of Certificate of Independent Price Determination

An OIG investigation developed evidence demonstrating that a vendor, a self-identified Bona Fide Agency, violated the Certificate of Independent Price Determination (CIPD). GPO includes a covenant against contingency fees in all of its contracts with vendors, with the caveat that if the contingency fee is charged by a business legitimately involved with securing business (a bona fide agency), and then the fees are allowable. The vendor established itself as a bid service agency more than 30 years ago. The CIPD states:

a. The prices in the offer have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror competitor relating to: (i) those prices; (ii) the intention to submit an offer; or (iii) the methods or factors used to calculate the prices offered.

b. The prices in the offer have not been and will not be knowingly disclosed by the offeror, directly or indirectly, to any other offeror or competitor before bid opening or contractor award unless otherwise required by law; and

c. No attempt has been made or will be made by the offeror to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.

The investigation disclosed that despite the vendor's claims of implementing a system of firewalls to protect client information and prevent sharing of bid information, the system did not work. The result was a breakdown of the principle of independent bid development, which resulted in the development of collusive bids—a violation of the CIPD.

Outcome: In August 2013, the OIG referred the vendor to GPO for suspension and/or debarment after our investigation revealed the vendor violated all three tenets of CIPD. A decision by the GPO SDO is currently pending. (*Case No. 10-0024-I*).

Vendor Arrested for Defrauding GPO

An OIG investigation revealed a vendor submitted eight invoices to GPO for which the contracted items were not delivered. The vendor was paid in excess of $20,000 before it was discovered key elements of his invoices were falsified.

Outcome: OIG Special Agents arrested the vendor, and the criminal matter is currently pending in the District of Columbia Superior Court. *(Case No. 12-0006-I)*.

Program and Operational Integrity

Strategic Goal 4:
Reduce improper payments and related vulnerabilities by helping GPO managers reduce payment errors, waste, fraud, and abuse in the major GPO programs and operations while continuing to ensure that programs serve and provide access to their intended parties.

Audit of GPO's Federal Employees' Compensation Act Case Management

The FECA Program provides workers' compensation coverage to approximately 193 GPO employees for work-related injuries and illnesses. In FY 2012, the FECA Program at GPO paid approximately $7 million in wage loss compensation to claimants. The Program affects the budget of GPO. The Department of Labor's Office of Workers' Compensation Programs estimated that future actuarial liabilities for GPO FECA compensation payments to those receiving benefits as of FY 2012 could total more than $70 million.

OIG conducted the audit to determine whether GPO could enhance its case management efforts and reduce overall FECA costs. The audit revealed that as GPO continues its efforts to improve FECA operations and management of individual claims, enhanced management of case files could reduce costs as well as risks of abuse and fraud. Management of the FECA Program could be affected by limited and necessary data.

Of the 193 case files, 38 (19 percent) were missing initial medical evidence. Initial medical evidence is necessary to establish a causal relationship for a claim. We noted that of 159 case files where medical updates were required, 132 (83 percent) lacked updated medical reports. The lack of medical reports hampered a specialist's ability to return medically able employees to work. Our review disclosed that of 105 case files requiring "Latest Earnings and Dependency Information" forms (Form CA1032), 104 (99 percent) did not include the proper form. The CA1032 identifies whether a claimant is receiving additional income, potentially identifying whether work capacity exists, and changes in dependency information. Although GPO does not require that workers' compensation specialists obtain updated CA1032s, adopting such a practice could aid specialists in returning beneficiaries to work, and therefore reduce costs.

Until GPO ensures that case files are complete, with sufficient initial medical evidence to substantiate claims, obtains medical updates when required, obtains updated CA1032s, and assigns employees to limited duty consistent with the claimant's medically defined work limitation, GPO runs the risk of paying questionable costs for benefits. Based on case review, of the 193 claims, 150 made up $6.4 million in annual compensation payments—funds that could have been put to better use due to missing or insufficient documentation. If not checked, we estimate payments for the claims during the next 5 years could reach as much as $32 million.

Recommendations: We recommended that the Chief Human Capital Officer further strengthen FECA case management by: (1) ensuring GPO case files are complete, with sufficient initial medical evidence that will substantiate claims, obtains medical updates when required, obtains updated CA1032s, and assigns employees to limited duty consistent with the claimant's medically defined work limitation, and (2) once the required claim information is obtained, implement aggressive case management as identified in GPO Directive 665.5B, dated September 3, 2008. Management concurred with the recommendation.

Procurement of Law Enforcement Credential Stock

OIG was contacted regarding alleged Department of Defense personnel improperly procuring security-enhanced law enforcement credential stock and laminating film from GPO. The credential stock and laminate were subsequently used to issue credentials to non-law enforcement personnel who then allegedly used the credentials improperly.

Our investigation revealed current standard operating procedures did not include verification of appropriate employee status of agencies who request secure credentials.

Recommendations: We recommended that the Managing Director, Security and Intelligent Documents, implement a process that will strengthen controls, such as requiring presentation of current credentials or using peer-to-peer confirmation through another law enforcement agency. Management concurred with the recommendation.

Employee Misconduct: Parking Program

An OIG investigation determined that four GPO employees violated the Parking Program's "Rules Governing Use of Permits" after it revealed that on four separate occasions, those employees were improperly sharing parking permits. GPO Directive 850.1G, *GPO Parking Directive and Administration* states, "Permits are not transferable and cannot be loaned or given to any employee other than a member of the carpool to which it is issued."

Outcome: The Acting GPO Employee Relations Manager recommended issuing each employee a Letter of Warning for their deliberate and repeated violations of the GPO Directive.

Vendor Violated Contract Terms

An OIG investigation revealed that a vendor violated its contract when it: (1) did not pay 46 of its security guards the required health and welfare benefits, totaling $282,633, (2) routinely worked its security guards in excess of 12 consecutive hours in 75 separate instances, and (3) did not provide properly certified security guards in Cardiopulmonary Resuscitation and First Aid during more than 60 percent of the hours worked, totaling approximately $1.2 million worth of ineligible payments.

The contract was for security services provided at the GPO Passport Facility located at the John C. Stennis Space Center in Mississippi.

Outcome: As a direct result of the OIG investigation, the vendor made full restitution to its employees in the amount of $282,633. In September, OIG referred the vendor to GPO for suspension and/or debarment based upon the OIG calculation of $1.4 million in monetary impact to GPO, and that the vendor willfully violated the terms of the contract and failed to take corrective action until presented with the possibility of civil litigation being initiated by the U.S. Attorney's Office. *(Case No. 10-0038-I).*

Federal Depository Library Program (FDLP) Planned October 2013 Conference

In June 2013, OIG received allegations of misuse of GPO funds regarding the planned October 2013 Depository Library Council Meeting and Federal Depository Library Conference. It was alleged that 15 people would be flown in to Washington, D.C., 2 days before the event for their own personal benefit and not out of business necessity and that a wine and cheese reception would be held as part of the conference "against advice."

Outcome: The OIG investigation revealed travel invitations had been issued for members of the Council who would be traveling to Washington, D.C. We discovered that each individual

invitation stipulated travel was only authorized for departure from the city of origin the day before the commencement of the conference and required returning the last day of the conference. Those invited were required to use the GPO travel agent to ensure adherence with pre-negotiated Government rates. If the traveler chose to book the travel themselves, they would be responsible for any difference in airfare between the actual cost and the Government rate. A block of hotel rooms had been reserved in Washington, D.C., and those rooms were being paid through a GPO purchase order from the GPO. The availability of those rooms coincided with the travel invitation; if a traveler desired to come early or stay later, there would have been no way to charge that expense to GPO and would have necessitated the traveler to make his or her own personal payment arrangements.

Our review disclosed a reception was planned. Federal policy concerning alcoholic beverages states, except where the head of the responsible agency has granted an exemption in writing for the appropriate official use of alcoholic beverages, all persons entering in or on Federal property are prohibited from being under the influence or using alcoholic beverages. We were advised that GPO senior management did not approve consumption of alcohol during the upcoming Conference and that the reception would be cancelled.

In August 2013, the OIG referred the complaint to GPO management and requested that GPO follow the guidance provided under Section 3003 of the Consolidated and Further Continuing Appropriations Act of 2013 that details conference spending reporting requirements to the OIG. (*Case No. 13-0040-C*).

Select Other Investigative Matter

We reported previously that OIG received allegations that several managers suspected they had been retaliated against for whistleblowing. We referred the allegations to the Office of General Counsel for further assessment. Subsequently, the Office of General Counsel reported that the Director of Equal Employment Opportunity (EEO) informed him that the employees are pursuing EEO complaints and that they will be investigated fully by an independent contractor.

During this reporting period, the EEO investigation was completed and two of the complainants are currently awaiting hearings at the EEO Commission, while the third complainant is pending a final agency decision from GPO. After the conclusion of the EEO process, OIG will evaluate the results and determine if further action—either on the part of GPO or OIG—is warranted. *(Case No. 12-0009-I).*

Referrals to and Requests for Information from Other Agencies

During the reporting period, the OIG referred 14 hotline complaints to other OIGs and responded to 2 requests for information from other agencies.

Stewardship Over Official Publications

OIG Strategic Goal 5:
Increase the efficiency and effectiveness with which GPO managers exercise stewardship over official publications from all three branches of the Federal Government.

Commercial Printing and Dissemination of Government Information

OIG is engaged in a long-term audit project to assess GPO's monitoring of key aspects of public printing and document retention requirements as prescribed in title 44 of the United States Code as it relates to National Institutes of Health, VA, and the Department of State.

Abbreviations and Acronyms

CA	Certification Authority
CICIE	Council of the Inspectors General on Integrity and Efficiency
CIPD	Certificate of Independent Price Determination
EEO	Equal Employment Opportunity
E&Y	Ernst & Young LLP
FASB	Financial Accounting Standards Board
FASAB	Federal Accounting Standards Advisory Board
FBCA	Federal Bridge Certificate Authority
FDLP	Federal Depository Library Program
FDsys	Federal Digital System
FECA	Federal Employees' Compensation Act
FISMA	Federal Information Security Management Act
GAAP	Generally Accepted Accounting Principles
GPO	Government Printing Office
IG	Inspector General
IT	Information Technology
IT&S	Information Technology & Security
JCP	Joint Committee on Printing
OIG	Office of Inspection General
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PPPS	Passport Printing and Production System
SDO	Suspending and Debarring Official
SQL	Structured Query Language
VA	Department of Veterans Affairs

Glossary

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 is completed by the time agreement is reached.

Management Implication Report
A report to management issued during or at the completion of an investigation identifying systemic problems or advising management of significant issues that require immediate attention.

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

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

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

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.

Appendix A

Index of Reporting Requirements under the IG Act of 1978

Reporting	Requirement	Page
Section 4(a)(2)	Review of Legislation and Regulation	None
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	All
Section 5(a)(2)	Recommendations with Respect to Significant Problems, Abuses, and Deficiencies	All
Section 5(a)(3)	Prior Significant Recommendations on Which Corrective Action Has Not Been Completed	21
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	24
Section 5(a)(5) and Section 6(b)(2)	Summary of Instances Where Information Was Refused	None
Section 5(a)(6)	List of Audit Reports	7-16
Section 5(a)(7)	Summary of Significant Reports	All
Section 5(a)(8)	Statistical Tables on Management Decisions on Questioned Costs	22
Section 5(a)(9)	Statistical Tables on Management Decisions on Recommendations That Funds Be Put to Better Use	22
Section 5(a)(10)	Summary of Each Audit Report over Six Months Old for Which No Management Decision Has Been Made	21
Section 5(a)(11)	Description and Explanation of Any Significant Revised Management Decision	None
Section 5(a)(12)	Information on Any Significant Management Decisions with Which the Inspector General Disagrees	None

Requirement under the Dodd-Frank Wall Street Reform Act of 2010

Section 3(d)	Peer Review	25-26

Appendix B

Final Reports Issued and Grouped by OIG Strategic Goal				
Report Name	**Number of Recommendations**	**Questioned Costs ($)**	**Funds Put To Better Use ($)**	**Other Monetary Impact ($)**
Transforming GPO into a Digital Platform				
WebTrust for Certification Authority, Report No. 13-18, September 6, 2013	0	0	0	0
Federal PKI Compliance Report, Report No. 13-19, September 6, 2013	0	0	0	0
PPPS Compliance with FISMA as it Relates to Continuous Monitoring, Report No.13- 17, September 18, 2013	2	0	0	0
Operational and Financial Management				
Financial Accounting: Volatility of the Federal Employees' Compensation Act Actuarial Liability Estimate, Report No.13-14, August 7, 2013	1	0	0	0
Program and Operational Integrity				
Audit of GPO's Federal Employees' Compensation Act Case Management, Report No. 13-13, September 23, 2013	2	0	$6.4 million	0
Management Implication Report— Procurement of GPO Law Enforcement Credential Stock, Implication Report No.13-01, September 10, 2013	0	0	0	0

Appendix C

Unresolved Audit Recommendations More Than 6 Months Old OIG Negotiating with Agency

Date Issued	Name of Audit	Report Number	Number of Recommendations	Costs ($)
Nov. 16, 2011	Audit of Selected Aspects of GPO Time and Attendance and Payroll Administration	12-01	2	0

Appendix D

Prior Recommendations on Which Corrective Action Has Not Been Completed in More Than 1-Year

Date Issued	Name of Audit	Report Number	Number of Recommendations	Monetary Impact ($)
Jan. 11, 2010	GPO FISMA	10-03	9	0
Nov. 16, 2011	Audit of Selected Aspects of GPO Time and Attendance and Payroll Administration	12-01	3	$372,717
Dec. 16, 2011	Independent Auditor's Report—US GPO FY 2011	12-02	5	0
Feb 14, 2012	Final Report FY 2011 Management Advisory Comments	12-07	4	0
Mar. 30, 2012	Maintaining Effective Control Over Employee Overtime	12-08	1	0
Apr. 16, 2012	Internal Control Maturity Assessment— Inspectron Software Application	12-09	2	0
Mar. 1, 2012	Consolidated Financial Statement Audit GPO Business Information System (GBIS)	12-10	4	0
Mar. 1, 2012	Consolidated Financial Statement Audit General Support System (GSS)	12-11	2	0
Jun. 28, 2012	Audit of Computer Security Handling a Denial of Service Incident	12-13	1	0

Appendix E

Audit Reports with Recommendations That Funds Be Put To Better Use, Questioned Costs, and Other Monetary Impact

Description	Number of Reports	Funds Put to Better Use, Questioned Costs, and Other Monetary Impact ($)
Reports for which no management decisions were made by beginning of reporting period	0	0
Reports issued during reporting period:		
Audit Report - Audit of GPO's Federal Employees' Compensation Act Case Management, Report No. 13-13, September 23, 2013	1	$6.4 million
Subtotal	**1**	**$6.4 million**
Reports for which management decision was made during reporting period:		
1. Dollar value of recommendations not agreed to by management		
2. Dollar value if recommendations agreed to by management	1	$6.4 million
Reports for which management decision was made by end of reporting period	0	0
Report for which no management decision was made within 6 months of issuance	0	0

Appendix F

Investigations Case Summary	
Item	**Quantity**
Total New Hotline/Other Allegations Received during Reporting Period	53
Preliminary Investigations (Complaints) Closed	47
Complaint Referrals to Other Agencies	16
Complaint Referrals to OAI	0
Investigations Opened by OI during Reporting Period	6
Investigations Open at Beginning of Reporting Period	28
Investigations Closed during Reporting Period	3
Investigations Open at End of Reporting Period	31
Referrals to GPO Management (Complaints and Investigations for corrective action or information purposes)	12

Current Open Investigations	**Number**	**Percent**
Procurement/Contract Fraud	17	54.8
Employee Misconduct	8	25.8
Workers' Compensation Fraud	2	6.5
Information Technology/Computer Crimes	1	3.2
Proactive Initiatives	2	6.5
Other Investigations	1	3.2
Total	**31**	**100**

Appendix G

Investigations Productivity Summary	
Item	**Quantity**
Arrests	1
Total Presentations to Prosecuting Authorities	3
Criminal Acceptances	1
Criminal Declinations	2
Indictments	1
Convictions	0
Guilty Pleas/Deferred Prosecution Agreements	0
Probation (months)	0
Jail Time (days)	0
Civil Restitutions	0
Civil Acceptances	0
Civil Agreements	0
Civil Declinations	2
Amounts Recovered Through Investigative Efforts	$0
Total Agency Cost Savings Through Investigative Efforts	$282,633*
Total Administrative Referrals	12
Contractor Debarments	0
Contractor Suspensions	2
Contractor Other Actions	0**
Employee Suspensions	1
Proposed Employee Suspensions	0
Employee Terminations	1***
Subpoenas	0

* Amount realized during the previous reporting period, amount accounted for this reporting period
** Show Cause Letter, Letter of Demand, etc.
*** Resignation in lieu of further disciplinary action

Appendix H

Peer Review Reporting

The following meets the requirement under Section 989C of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Public Law 111-203) that IGs include peer review results as an appendix to each semiannual report. Federal audit functions can receive a rating of "pass," "pass with deficiencies," or "fail." Federal investigation functions can receive a rating of "compliant" or "noncompliant."

Peer Review of GPO-OIG Audit Function

The Library of Congress OIG conducted the most recent peer review of the GPO Office of Audit and Inspections in March 2011.

The Library of Congress OIG reported that the system of quality control for the audit function in effect for the 2 years ending September 30, 2010, was suitably designed and complied with, and provided OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards. The peer review gave GPO OIG a rating of "pass."

The Peer Review Report is available on the GPO OIG Web site at http://www.gpo.gov/pdfs/ig/audits/GPO-AuditPeerReviewReport.pdf

Peer Review of GPO-OIG Investigative Function

The National Science Foundation OIG conducted the most recent peer review of the investigative function at GPO in March 2011.

The National Science Foundation OIG reported that the system of internal safeguards and management procedures for the investigative function for the year ended 2010 complies with the quality standards established by the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and the Attorney General guidelines. The safeguards and procedures provide reasonable assurance of conforming to professional standards in the conduct of its investigations. There were no outstanding recommendations from this peer review.

The Peer Review Report is available on the GPO OIG Web site at http://www.gpo.gov/pdfs/ig/investigations/InvestigationsPeerReview.pdf

Peer Reviews of other OIGs

GPO OIG conducted a peer review of the Architect of the Capitol OIG's Office of Investigations in accordance with in the Quality Standards for Investigations and the Quality Assessment Review Guidelines established by the CIGIE and the Attorney General's Guidelines for OIGs with Statutory Law Enforcement Authority, as applicable. In our opinion, the system of internal safeguards and management procedures observed during the review was "compliant" with the quality standards established by the CIGIE and the applicable Attorney General guidelines. The safeguards and procedures provide reasonable assurance of the Architect of the Capitol OIG's Office of Investigations conformed with professional standards in the planning, execution, and reporting of its investigations.

The GPO OIG also conducted a peer review of the Federal Communications Commission OIG's system of quality control for the year ended March 31, 2013, in accordance with generally accepted government auditing standards and guidelines

established by the CIGIE. In our opinion, the Federal Communications Commission OIG system of quality control was suitably designed and complied with to provide the Federal Communications Commission OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Therefore, we issued a peer review report with a rating of "pass." As is customary, we also issued a letter that sets forth findings that were not considered to be of sufficient significance to affect our opinion expressed in our report.

Report Fraud, Waste, and Abuse

Report violations of law, rules, or agency regulations, mismanagement, gross waste of funds, abuse of authority, danger to public health and safety related to GPO contracts, programs, and/or employees.

U.S. Government Printing Office
Office of Inspector General
P.O. Box 1790
Washington, DC 20013-1790
Email: gpoighotline@gpo.gov
Fax: 1 (202) 512-1030
Hotline: 1 (800) 743-7574