U.S. GOVERNMENT PRINTING OFFICE | OFFICE OF INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

APRIL 1, 2012 THROUGH SEPTEMBER 30, 2012

ABOUT THE GOVERNMENT PRINTING OFFICE...

Government Printing Office (GPO) continually strives to satisfy the requirements of Government and uphold its mission of Keeping America Informed.

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 provided with our compliments. It 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/.

MESSAGE FROM THE INSPECTOR GENERAL

This Semiannual Report to Congress covers the 6-month period ending September 30, 2012, and summarizes the most significant accomplishments of the GPO OIG.

During this reporting period, our office increased efforts to help GPO with its transformation to a digital platform. We reviewed GPO's Enterprise Architecture management maturity and FDsys Architecture management maturity. We conducted an internal control maturity assessment on the Inspectron software application used for tracking the production of e-Passports while in a work-in-progress status. We assessed GPO's response to a Distributed Denial of Service (DDoS) attack, and we reviewed the status of its Certification and Accreditation (C&A) activities. We continued to provide an assurance service necessary to support GPO's Public Key Infrastructure (PKI) Certification Authority (CA).

We identified and are in the process of implementing a number of proactive investigative initiatives. These initiatives are tests or examinations of systemic weaknesses or potential program vulnerabilities. They are based on fraud identified in a previous investigation or designed to detect violations that may have gone undetected. They may identify perpetrators, generate investigations, or result in a referral to the GPO management.

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.

I want to express my appreciation for the hard work performed by our dedicated OIG employees who strive to execute OIG's mission to improve the economy, effectiveness, and efficiency of GPO programs as well as prevent and detect criminal activity, waste, abuse, and fraud. During this reporting period, we issued 12 audit and other reports which, among other things, identified $3.8 million in questioned costs and funds that could be put to better use, identified funds that could be at risk, and made 27 recommendations for program improvement. Our investigative work led to one deferred prosecution, six debarments, and $52,840 in monetary funds at risk as the result of fraud.

I also thank the Acting Public Printer and other senior GPO officials and their staffs for not only their support of our work but also their receptiveness to our recommendations for improving GPO 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 1

Management Challenges 3

Transforming GPO into a Digital Platform 9

Operational and Financial Management 15

Print Procurement Programs 17

Program and Operational Integrity 19

Stewardship over Official Publications 23

Abbreviations and Acronyms 25

Glossary 27

Appendices 29

SELECTED STATISTICS

INVESTIGATIONS

Investigative cost-efficiencies, restitutions, fines and penalties	$52,840
Complaints opened	21
Complaints closed	16
Investigative cases opened	6
Investigative cases referred for prosecution	4
Investigative cases referred for administrative/civil action	10
Investigative cases accepted for prosecution	1
Investigative cases accepted for civil action	0
Investigative cases closed	8
Convictions/Deferred Prosecution	1
Debarments	6
Subpoenas issued	3

AUDITS AND INSPECTIONS

Audit and other reports issued	12
Questioned costs, funds put to better use, and other monetary impact	$3.8 million
Number of Recommendations Made	27

MANAGEMENT CHALLENGES

The Top Management Challenges OIG identified for GPO are discussed below. We updated the challenges since our March 31, 2012, Semiannual Report to Congress, to include current work and GPO's ongoing transformation.

For the period ending September 30, 2012, the OIG considers the following as the Top Management Challenges facing the GPO:

- Keeping focus on its mission of information dissemination
- Addressing emerging workforce skills
- Improving the Enterprise Architecture and Infrastructure to support enterprise-wide and FDsys transformation
- Securing information technology (IT) systems and protecting related information assets
- Managing Workers' Compensation Programs
- 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

Changes to the Top Management Challenges from the previous reporting period consist of the broadening of improving the Infrastructure for GPO's FDsys to improving the Enterprise Architecture and Infrastructure to support enterprise-wide and FDsys transformation.

KEEPING FOCUS ON ITS MISSION OF INFORMATION DISSEMINATION

Overview: The transformation of GPO has already begun. 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:

GPO is updating and revising its strategic plan to reflect the accomplishments from previous years as well as future year goals.

GPO continues its efforts to develop an organizational model where in some Business Units the chief executive officer focuses 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.

ADDRESSING EMERGING WORKFORCE SKILLS

Overview: As more and more Government information goes digital, GPO is likely to be confronted with a gap in workforce skills. GPO of today and tomorrow is

clearly being defined by digital technology, and digital technology itself has radically changed the way printing is performed. Such a change is especially true where the information products the House and Senate use are concerned.

GPO's digital systems support several key Federal publications—including the printing of the U.S. Budget and Federal Register as well as associated products. The Agency uses advanced authentication systems, supported by PKI, deemed essential components for assuring the digital security of congressional and Agency documents.

Another important product for which GPO is responsible is printing passports for the Department of State. 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, have transformed e Passports into the most secure and obtainable identification credential.

GPO has also developed a line of secure identification "smart cards" that help support credential requirements of the Department of Homeland Security for certain border crossing documents.

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.

A continued emphasis on a strategic vision may result in incorporating a workforce plan that includes an "as-is" inventory of the knowledge and skills of GPO employees and a "to-be" inventory that

identifies the knowledge and skills that GPO needs in the future.

IMPROVING THE ENTERPRISE ARCHITECTURE AND INFRASTRUCTURE TO SUPPORT ENTERPRISE-WIDE AND FDSYS TRANSFORMATION

Overview: GPO is the Federal Government's primary resource for producing, procuring, cataloging, indexing, authenticating, disseminating, and preserving the official information products of the Government in both digital and tangible formats. 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, title 44, chapter 36, 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.

Enterprise Architecture is the organizing logic for business processes, and IT infrastructure reflects the integration and standardization requirements of the company's operating model.

GPO's FDsys provides free online access to official information for the three branches of the Federal Government. FDsys comprises the following:

- Content Management System – FDsys provides online access to official Federal Government publications and securely controls digital content throughout its lifecycle to ensure content integrity and authenticity.
- Preservation Repository – The repository guarantees long-term preservation and access to digital Government content. To meet the critical need for permanent access to Government information, FDsys follows archival system standards.
- Advanced Search Engine – FDsys combines modern search technology with extensive metadata creation to ensure the highest quality search experience.

FDsys provides more than 680,000 Federal titles online from GPO servers and links to servers in other agencies. Each month, consumers download more than 13.1 million documents.

FDsys includes all known Government documents within the scope of GPO's FDLP. The library program consists of more than 1,200 designated Federal depository libraries throughout the United States and its territories and provides the American public with free access to Government publications in tangible and electronic collections.

GPO relies extensively on computerized information systems and technology to support FDsys operations and its transformation. GPO anticipates a growing demand for content and use.

Areas within the Government that traditionally are most likely to cause delays or budget overruns include poorly defined project vision/goals, lack of accountability/ownership, unrealistic deadlines, poor communication of expectations, resource deprivation/competition, scope changes, uncertain dependencies, not understanding/defining project risk, and lack of stakeholder/user engagement throughout the project lifecycle. Those 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: Existing IT infrastructure may not be able to support the increased demand that GPO anticipates, including the ability to support more mobile applications to address the expanding market of e readers and smart phone users.

GPO's Progress:

Efforts to develop a fully mature Enterprise Architecture have been underway since 2008. GPO has developed and implemented an Enterprise Architecture policy, created the Enterprise Architecture Program Office, appointed a Chief Architect, uses an automated tool that contains reference models to assist in developing an Enterprise Architecture, and from 2008 to 2010 established an

Architect Review Board. In 2010, GPO performed a self-assessment using the Government Accountability Office's (GAO) framework and determined a maturity level of Stage 4 in the GAO framework. The highest level of maturity is Stage 6. Stage 4 represents completing and using an initial Enterprise Architecture version for targeted results.

We compared GPO's progress with GAO's framework. Based on both our audit and the GPO self-assessment in 2010, GPO had not fully expanded and evolved the Enterprise Architecture and its use for transformation and optimization.

We believe the maturity of GPO's Enterprise Architecture is less than what was reported in GPO's self-assessment in 2010.

We found similar results with the architecture maturity level of FDsys, which has not yet evolved to support transformation or optimization. In fiscal year (FY) 2012, FDsys was funded for development at approximately $4 million.

SECURING IT SYSTEMS AND PROTECTING RELATED INFORMATION ASSETS

Overview: GPO systems contain vital information that is central to the GPO mission and to the 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. In addition to the GPO Web site, the Agency routinely communicates with the public by way of Twitter, YouTube, and Facebook.

In past years, OIG has identified issues in the design and/or operations of GPO's IT. For example, issues have been noted in the areas of security management, access controls, segregation of duties, configuration management, and contingency planning. Generally,

the conditions existed as a result of resource constraints and competing priorities.

Challenge: Safeguarding information assets is a continuing challenge for Federal agencies, including GPO. Security challenges are increasing as employees increase the use of telework as well as a reliance on new ways of communicating. New forms of communication include social media technology, mobile applications, and hosting Web applications for other Federal agencies. GPO is challenged to evolve and adapt its information security controls to keep pace with the risks new technologies pose.

GPO's Progress:

GPO experienced an attack involving a Federal system and infrastructure, which demonstrated that a serious attack could be devastating. The attack prevented as well as impaired the normal authorized functionality of networks, systems, and/or applications by exhausting resources.

GPO is updating its incident handling directive and guidance and developing detailed and

standardized procedures using National Institute of Standards and Technology (NIST) Special Publication 800-61, "Computer Security Incident Handling Guide."

GPO is also conducting activities that will reflect the risk management framework approach established in NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems."

MANAGING WORKERS' COMPENSATION PROGRAMS

Overview: The Federal Employees' Compensation Act (FECA) Program provides wage-loss compensation and pays medical expenses for covered Federal civilian 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 the eligibility of injured workers to receive workers' compensation benefits. The Department of Labor provides direct compensation to medical providers, claimants, and beneficiaries. In addition to paying an administrative fee, GPO reimburses the Department of Labor for any workers' compensation claims.

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.

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 (CFR), Public Printing and Documents, to match GPO's costs and revenues through rates and prices charged customers. Recognizing this 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: Because the Department of Labor develops liability estimates for FECA and is out of the control of GPO, there is a risk that a relatively unexpected increase in the estimate could have significant unfavorable impact on GPO's financial management.

From a program perspective, 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 moving 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.

GPO's Progress:

GPO performs various activities involving its FECA program, such as actively servicing individual cases and verifying appropriate costs charged by the Department of Labor.

Monitoring FECA operations such as: (1) the marital status of claimants, (2) continued eligibility of the claimants dependents, (3) opportunities to bring claimants back on a modified, limited, or light duty assignment, (4) on a regular basis medical updates, and (5) the need for second medical opinions where the record indicates the claimant has some potential of eventually returning to work, could reduce GPO's risk to program volatility.

GPO could also mitigate risk by ensuring that its Business Unit supervisors understand their responsibilities under FECA and expand the use of IT to administer the program.

IMPROVING PRINT PROCUREMENT PROGRAMS

Overview: GPO is the principal agent for almost all Government printing. Title 44 requires that GPO must accomplish any printing, binding, and blankbook 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 due to inefficient printing by Executive Office agencies.

GPO's Progress:

GPO is working with OIG in two instances to determine if waivers were granted, exemptions were granted under specific legislation, print expenditures were most cost-beneficial to the Government, and documents were available through FDLP.

In April 2012, the JCP requested GAO to audit the total number of internal printing plants, the total amount of in-plant work produced, and the print procurement practices for all Federal departments and agencies. GPO is working with GAO on this request.

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.

Enhanced Architecture Maturity Could Better Guide GPO's Transformation

Throughout its 150-year history, GPO has transformed the way it publishes Government information to keep pace with the technology of the time. The trend toward producing Government documents through electronic publishing technology and providing the public with Government documents through the Internet has affected all of GPO's programs, ultimately reducing production, procurement, and sales of printed products. Those products have historically provided GPO with a vital source of revenue that supplements its annual budget. To help ensure that it stays relevant and efficient as well as meets the needs of customers, GPO is making strategic, operational, and cultural changes. GPO defines the transformation process as a move from being print centric to a model that includes content management systems, business information systems, and digital production systems.

OIG initiated an audit that would determine the extent to which GPO had assurance that its Enterprise Architecture was used to guide and constrain ongoing development and support of GPO's strategic transformation.

Efforts to develop a fully mature Enterprise Architecture have been underway since 2008. The Agency has developed and implemented an Enterprise Architecture policy, created the Enterprise Architecture Program Office, appointed a Chief Architect, and used automated tools containing reference models that assist in developing an Enterprise Architecture. During 2008 through 2010, GPO established an Architect Review Board. In 2010, GPO conducted a self-assessment using the GAO framework, which determined a maturity level of Stage 4. The highest level of maturity is Stage 6. Stage 4 represents completing and using an initial Enterprise Architecture version for targeted results.

We compared progress at GPO with the GAO framework. Based on both our audit and the Agency's self-assessment, GPO did not fully expand the Enterprise Architecture and its use for transformation and optimization. We believe the maturity of GPO's Enterprise Architecture is less than what was reported in its 2010 self-assessment.

The results with the architecture maturity level of FDsys were similar to those of FDsys but has not yet, however, evolved to support transformation or optimization. In FY 2012, FDsys was funded at approximately $4 million for development.

Without a matured Enterprise Architecture, GPO assumes the risk that it will invest in IT that is duplicative, not well integrated, costly, not supportive of the Agency's strategic goals and mission, or not responsive to emerging technologies. Once complete, GPO will have a better vision of its transformation. For example, the "as-is" and "to-be" views of the performance, business, data, services, technology, and security architectures as well as well-defined plans for transitioning from the as-is to the to-be views, should be achieved. Also, GPO should be focused on continuously improving the quality of its suite of Enterprise Architecture artifacts and the people, processes, and tools used to govern their development, maintenance, and use.

From 2010 on we have expressed that progress was slowed as a result of the inactivity of the Architect Review Board in 2010. As board members were reassigned or left GPO, management did not identify replacement members and the board eventually discontinued its efforts and has not convened since the collapse.

Recommendation: For this audit, we recommended that the Chief Information Officer identify, develop, and implement a framework for evolving GPO's Enterprise Architecture and its use in supporting GPO's transformation and optimization. We also recommended that the Chief Information Officer reevaluate, modifying if necessary, GPO Directive 705.31, "GPO Enterprise Architecture Policy," and reestablish as well as reconvene the Architect Review Board. We further recommended that the Chief Technology Officer work with the Chief Information Officer to ensure FDsys architecture is aligned with the Enterprise Architecture.

Management agreed with the recommendations. In response to our recommendations, management reported that GPO will focus on complying with the spirit of the GAO maturity model as authority allows. Directive 705.31 will be updated to reflect a revised "right-sized" Enterprise Architecture approach, which takes into account cross-governmental Enterprise Architecture best practices such as those set forth by GAO and the Office of Management and Budget's (OMB's) Federal Enterprise Architecture Program Management Office but does not stipulate full compliance. Management also reported that FDsys technologies are aligned with the Enterprise Architecture Technical Reference Model. However, enhanced coordination that achieves more detailed design documentation would be helpful toward improving the baseline architectures. *(Enhanced Architecture Maturity Could Better Guide GPO's Transformation, Report No. 12-19, September 28, 2012)*

Internal Control Maturity Assessment–Inspectron Software Application

A genuine U.S. passport is a vital document, permitting its owner to travel freely into and out of the United States, prove U.S. citizenship, obtain further identification documents, and set up bank accounts, among other things. GPO has been producing U.S. passports since the 1920s. Beginning in early 2006, the Department of State began issuing passports with 64-kilobyte Radio Frequency Identification (RFID) chips that contain the name, nationality, gender, date of birth, and place of birth of the passport owner, as well as a digitized photograph of that person.

GPO uses the Inspectron software application for tracking production of e Passports while in a work-in-progress status. In general, work in progress consists of gluing adhesive tape strips to the inside cover of the passport, inserting and sewing pages into the cover, digital formatting and encoding of the RFID chip, separating joined passport covers and pages, and applying unique barcodes.

Based on guidance published by the Information Systems Audit and Control Association, the Committee of Sponsoring Organizations of the Treadway Commission, and the Software Engineering Institute of Carnegie Mellon University, we conducted an inspection to assess the design and effectiveness of the internal controls and operating efficiency and effectiveness of the Inspectron software application.

The audit revealed that internal controls were repeatable and processes produced projected outcomes. However, documentation supporting the application controls did not exist. We, therefore, believe that the internal control maturity level for the software application was assessed at a low maturity level.

Recommendation: For this audit, we recommended that the Director of Security and Intelligent Documents (SID) document tracking processes of the Inspectron software application and identify risks and any associated roles and responsibilities as well as periodically review and evaluate controls after the process has been documented. Management agreed with the recommendations. *(Internal Control Maturity Assessment – Inspectron Software Application, Report No. 12-09, April 16, 2012)*

Audit of Computer Security–Handling a Denial of Service Incident

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.

In March 2012, GPO was the victim of a DDoS attack requiring an immediate shift of its full attention to detecting, analyzing, containing, and recovering from the attack. The hacker attacked a Web site that GPO hosted—bringing it down by overloading it with traffic. We believe the attackers were protesting Online Piracy legislation. The hacker's attack essentially swamped the Web site with false users. The attacks primarily comprised multiple individuals and/or groups using a High Orbit Ion Cannon (HOIC). An HOIC is an increasingly popular attack tool that can simultaneously target up to 256 Web addresses. An HOIC tool uses "booster" scripts in attempts to randomize characteristics of Hypertext Transfer Protocol requests in order to evade detection as an attacker. The booster scripts—which are already circulating widely among hacker circles—allowed the attack the advantage of stealth.

OIG's involvement entailed a two-pronged approach. The first approach involved a criminal investigation, and the second was an audit that assessed actions GPO took in response to the DDoS incident in March 2012 as well as actions taken when explicitly accepting the risk to Agency operations by authorizing the hosted Web site to operate.

We identified several areas where controls could be strengthened that would further mitigate future risks. For example, GPO should strengthen its information security policies and procedures related to a DDoS incident so that it fully addresses the standards and guidance the NIST issues. We also note in the report that some additional steps could be taken to strengthen actions associated with handling an incident. While GPO took some action before the GPO-hosted Web site became operational, we note as well that not all elements of the C&A process were completed before authorizing the Web site to operate. The impact of a DDoS attack could completely disrupt and/or cripple GPO's ability to fulfill its mission until the network can be restored.

Recommendation: For this audit, we recommended that the Chief Information Officer continue working toward the goal of becoming Federal Information Security Management Act of 2002 (FISMA)-compliant by updating the Agency's incident handling directive and guidance as well as developing detailed and standardized procedures using NIST Special Publication 800-61. We also recommended that the Chief Information Officer conduct C&A activities that reflect the risk management framework approach established in NIST Special Publication 800-37. As a legislative branch, GPO is not required to comply with FISMA but voluntarily follows the spirit of the law.

Management reported that it will update procedures to include more of the suggested guidance from the NIST SP 800-61 document. Management also reported there are serious financial and resource implications for GPO pertaining to aligning its C&A activities to reflect the risk management framework approach established in NIST. Management further stated that it will conduct a cost-benefit analysis and

coordinate with the Acting Public Printer and other senior officials to determine if the recommendation can be implemented within the fiscal and resource constraints of GPO. *(Audit of Computer Security – Handling a Denial of Service Incident, Report No. 12-13, June 28, 2012)*

Federal PKI Compliance Report and WebTrust for Certification Authority

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

- PKI is a set of hardware, software, people, 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 the 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 non-Federal entities.

GPO's PKI is cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification requires that the 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.

We commend management of the GPO-CA once again for passing such a rigorous assessment. E&Y's opinion for the period July 1, 2011, through June 30, 2012, is that the GPO Principal Certification Authority Certificate Practices Statement conformed in all material respects to the GPO-CA and Federal PKI common policies (Federal PKI Compliance Report, Report No. 12-23, September 18, 2012) and GPO management's assertion is fairly stated in all material respects based on the AICPA Trust Services Criteria for Certification Authorities. *(WebTrust for Certification Authority, Report No. 12-22, September 18, 2012)*

Recommendation: The report did not contain any recommendations.

Audit of GPO's Suitability Process for Passport Production

SID produces electronic passports (e-Passports), which individuals can use as identification documents. Passport production is a critical homeland security concern, given that possession of an American passport can help travelers bypass some of the stringent reviews conducted of anyone entering the U.S. from abroad.

OIG conducted an audit to determine if opportunities existed that would enhance controls over GPO's internal processes and standards for personnel suitability determinations for personnel with access to SID passport production facilities.

We concluded that controls over the personnel suitability processes could be further strengthened for passport production. Specifically, SID could strengthen its process to include the following actions: (1) determine the required clearances and levels of clearances for positions requiring access to the passport facilities; (2) periodic monitoring of employees with a National Agency Check with Inquiries and Credit Check (NACIC) clearance; (3) annotate position descriptions for employees having access to SID to reflect the sensitivity level of the position; and (4) strengthen controls over monitoring the status of reinvestigations. Strengthening controls should mitigate the risk of providing an avenue for potential unscrupulous activities to take place.

Recommendations: For this audit, we recommended that the SID Managing Director determine

the proper risk level and position classification for employees with access to SID passport production facilities, and, if needed, complete the appropriate background investigations for the classification established. We also recommended that the Chief Human Capital Officer coordinate with the SID Managing Director and annotate position descriptions with the sensitivity level of the position. We further recommended that the Director of Security require that employees and contractors with access to SID passport production facilities inform management if any employee or contractor is arrested or charged with any offenses, with the exception of minor traffic infractions that do not involve drugs or alcohol; and to periodically monitor cleared employees and contractors for adverse changes.

Management agreed with the recommendations. The Managing Director of SID will work with the Chief Human Capital Officer to incorporate changes resulting from a review of SID's position classifications and ensure that position descriptions note any security clearance requirements. The Director of Security Services will update GPO Directive 825.2B, "Personnel Security Program," dated February 25, 2010, to include self-reporting requirements for personnel assigned to SID (and GPO personnel assigned to support SID operations) and those having executive privileges and/or unescorted privileges to SID operations. The Director will also conduct and coordinate an awareness campaign and training events. The Director of Security Services will initiate a new program for performing periodic criminal checks on SID and GPO personnel who support SID operations and those with executive privileges and/or unescorted privileges to SID operations. Every 5 years, designated employees or contractors will be fingerprinted and subjected to background checks and monitoring for adverse changes. The directive will be updated to include that change. The Managing Director of SID and the Chief Human Capital Officer will in tandem review position descriptions and associated sensitivity levels. *(Audit of GPO's Suitability Process for Passport Production, Report No. 12-17, September 18, 2012)*

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.

Operational Enhancements Could Further Improve the Congressional Billing Process

The Committee on House Administration requested that OIG determine whether GPO properly billed the Congressional Printing and Binding (CP&B) appropriation for congressional products delivered to the Committee on Foreign Affairs and whether opportunities existed that would enhance controls over billing charges. The Committee questioned a report of billing charges associated with 24 jackets (sometimes referred to as work orders) from November 2005 through March 2008 for congressional hearings. The Committee also questioned billing charges associated with 30 jackets billed in April and July 2011 for congressional hearings. The Committee reported instances of billing for the same jackets twice, overcharging by using an incorrect number of billable pages, incorrectly charging the page rate rather than a flat rate, and billing for work associated with another congressional committee.

While the audit was in progress, we received additional information about incomplete billing charges associated with pre-press printing (letterheads and envelopes). We incorporated a review of those billing charges into our audit. Pre-press costs are incurred when a customer sends GPO a file that needs to be manipulated to make the file ready for printing. For example, pre-press work could include revising the user-supplied typeface.

OIG conducted an audit to determine if opportunities existed that would enhance controls over the accuracy of billing charges for congressional products.

While in the audit report we note a reduction from 2005 to 2011 in the number of duplicate billing charges, errors associated with billing the incorrect congressional committee, and billing charges based on the number of printed pages instead of the billing rate associated with posting electronic files online, opportunities existed for enhancing controls over the accuracy of billing charges for congressional products.

Of the approximately $3.45 million in billing charges to the CP&B appropriation from FY 2006 through FY 2011 for products the Committee on Foreign Affairs requested, we calculated that about 95.4 percent (or approximately $3.29 million) of the charges were accurate. Conversely, approximately 4.6 percent (or $159,529) of the billing charges were not accounted for accurately.

GPO notified the Senate Rules and Administration Committee and the Committee on House Administration pre-press billing that charges beginning in May 2009 through May 2012 had not been billed. We confirmed that approximately $2.2 million worth of pre-press billing charges were not billed during that period.

We also note in the report that although GPO has a designated single point of contact for congressional committees to discuss billing matters, it was not always apparent. Since 2005, the Committee on Foreign Affairs had been contacting a variety of individuals in the Official Journals of Government and Finance and Administration business units to discuss billing discrepancies.

Recommendations: For this audit, we recommended that the Chief Financial Officer establish a performance measure for billing accuracy, and establish and implement a formal process for periodically assessing and monitoring the accuracy of billing charges that will ensure controls are operating as designed and achieving the intended purpose.

We also recommended that the Managing Director of Official Journals of Government work with the Chief Financial Officer to reiterate within GPO and ensure that each congressional committee is aware of the single point of contact in GPO with whom they can discuss billing matters.

Management agreed with our recommendations. The Chief Financial Officer will implement a quarterly review procedure in FY 2013 to statistically sample CP&B billings to determine the accuracy of the charges and establish guidelines for measuring performance accuracy. The Chief Financial Officer will also coordinate with the Managing Director of Official Journals of Government to identify a GPO single point of contact for billing matters and subsequently notify the appropriate individuals. *(Operational Enhancements Could Further Improve the Congressional Billing Process, Report No. 12-16, September 21, 2012).*

Audit of Controls over GPO's Fleet Credit Card Program

GPO administers 19 fleet credit cards used to purchase fuel and authorized maintenance on its 39 GPO-owned and 3 leased vehicles. US Bank issued 17 of the cards and the General Services Administration (GSA) issued 2.

We conducted an audit to determine if controls over fleet credit cards were adequate and if the expenses were allowable and appropriate.

The audit revealed that there was an absence of key controls related to reviewing, approving, and reconciling monthly charges, separation of duties, and periodic assessments. Fleet cardholders did not receive training, and documentation for charges was not always maintained or readily available. In addition, payments were made for unauthorized premium grades of fuel. GPO drafted but did not finalize a management directive that primarily discussed processes and procedures for the fleet card. The absence of a strong internal control infrastructure to oversee the Fleet Credit Card Program exposes GPO to increased risk of potential loss of assets through improper purchases.

Recommendation: For this audit, we recommended that the Director for Acquisition Services complete and implement a written management directive and standard operating procedures that address goals and objectives for the Fleet Credit Card Program.

Management agreed with the recommendation. The Director for Acquisition Services plans to mitigate the risk of potentially improper purchases by completing and implementing a written management directive and standard operating procedures that provide goals and Fleet Credit Card Program objectives and corresponding procedures. The Director for Acquisition Services will include instructions in the guidelines similar to those on the GSA Web site that provide guidance for using fleet cards. *(Audit of Controls over GPO's Fleet Credit Card Program, Report No. 12-18, September 28, 2012)*

PRINT PROCUREMENT PROGRAMS

OIG STRATEGIC GOAL 3:

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

Fabricated Government Bills of Lading

An OIG investigation revealed that one vendor submitted an invoice in the amount of $479,933 using fabricated Government Bills of Lading as proof of delivery in order to initiate payment.

In December 2010, GPO placed an order on behalf of the Defense Logistics Agency (DLA) for production of the DLA Customer Assistance Handbook. The order consisted of two parts: 40,000 copies of a 338-page perfect-bound handbook and 80,000 copies of a 338-page spiral-bound handbook. All materials were required to be delivered to DLA in February 2011. After receiving the delivery, DLA reported they were shorted several thousand copies.

GPO's Financial Management Division processed the invoice but later suspended the payment after receiving information that the order was incomplete.

Current procedures require that vendors submit a receipt and/or shipping documents that equal the quantity ordered and the quantity billed. Government bills of lading and commercial bills of lading must be signed by the carrier and indicate the actual pickup date. Straight bills of lading are not considered adequate shipping documentation.

Evidence of shipment or delivery is also required. Vendors must submit as receipts copies of the shipping documents when delivery or shipping is required by a specific date. Receipts or shipping documents must show a purchase order number, the jacket number, print order number (when appropriate), and quantity represented by the receipt.

Receipts or shipping documents must total to the quantity ordered and quantity billed, and the carrier must sign bills of lading, indicating the actual pickup date. Straight bills of lading are not considered adequate shipping documentation. They must be commercial carrier airway or freight bills. *(Report of Investigation No. 12-0001-I)*

Outcome: The vendor provided the remainder of the shipment in November 2011 and beginning in April 2012 and ending in April 2015, the owner, Government account executive, and vendor were debarred from doing business with GPO as contractors, subcontractors, or contractor's representatives.

Vendor Misrepresentation of Print Capabilities

GPO reported that a vendor provided false information regarding existence of a registered printing company. Our investigation found the vendor registered five fictitious companies and one additional company with the only capability of performing copy work. Because the vendor had misrepresented its capabilities, GPO ended up awarding 229 contracts and paid $538,546 in related work. The vendor admitted it used the address of another business when registering one of the companies and admitted another company was a fictitious division. *(Report of Investigation No. 10-0036-I)*

Outcome: Beginning in July 2012 and ending in July 2015, the vendor and all of its registered

companies were debarred from doing business with GPO as contractors, subcontractors, or contractor's representatives.

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.

GPO Parking Program—Program Integrity

At the request from the Acting Public Printer, OIG initiated an audit of GPO's Employee Parking Program to determine whether controls were in place that would ensure employees were following parking policies and only authorized employees were parking in GPO parking facilities.

In addition to our audit, we investigated allegations that one employee allowed a co-worker to copy her GPO parking permit allowing the employee to park in the GPO parking lot for approximately 2 years without paying while at the same time receiving transit benefits.

In another investigation, we investigated an allegation that one employee parked in a GPO parking lot without having enrolled in the program or paying parking fees.

An OIG audit identified opportunities to further strengthen controls in the GPO Parking Program. We identified opportunities for further strengthening controls over the Parking Program. For example, our audit substantiated concerns that some employees were not abiding by the requirements of the program. In fact, the audit revealed that for an average of about 4 years 19 employees did not pay for parking—7 years in 1 case. The employees stated that they believed parking fees were being deducted from their biweekly earnings and that they had not reviewed their Leave and Earning Statements to confirm that parking fees were deducted. Those 19 employees failed to pay parking fees totaling $54,230. We note in the report that of 3,656 (22 percent) permits issued, 94 could not be accounted for since the permits were acquired in FY 2006. In addition, 115 permits were not properly secured. Nearly 47 percent of the program records tested were either inaccurate, incomplete, or both.

This issue not only raises security concerns but loss of revenue. Permits were not always displayed on all parked vehicles. We note in the report that on 3 separate occasions, 10 parked vehicles did not have permits. Four of the illegally parked vehicles were vehicles of non-GPO employees. We could not determine ownership for three vehicles.

We did not audit temporary permit receipts because some of the associated documents were shredded when the Parking Program was transferred to the Office of Security Services.

We believe that the weaknesses in the parking program can be attributed to two key components of the internal control system: control activities and monitoring. Internal control weaknesses in Agency programs expose GPO to fraudulent, improper, and abusive loss of assets. We note in the report that control activities such as reconciliations were not performed between parking fees received and parking permits issued. Also, the Agency did not develop

standard operating procedures for the program. In addition, neither monitoring nor internal evaluations were performed.

Recommendations: For this audit, we recommended that the Director of Security Services and the Chief Financial Officer continue to work toward developing and maintaining a parking program in accordance with GPO policies by strengthening key controls. The key controls include reconciling parking fees received with parking permits issued, developing and documenting standard operating procedures, monitoring and conducting internal evaluations of the Parking Program, and collecting from employees the unpaid parking fees totaling $54,230.

Management agreed with all of the recommendations. GPO has developed standard operating procedures, is planning to reissue parking permits, has redesigned permits with additional security features for better control, has implemented a review process that will monitor withholdings for all parking program participants, and has initiated collection action against those employees who parked without paying. (GPO Parking Program: Opportunities Exist to Further Strengthen Controls, Report No. 12-14, July 25, 2012)

In December 2011, the OIG received an allegation that one GPO employee allowed a co-worker to make a copy of her GPO parking permit. We were told the employee had been parking with the copied parking permit for approximately 2 years. It was further reported that while parking on the GPO parking lot one of the employees was receiving transit benefits.

After arresting both employees, one employee admitted, in a letter signed in June 2012, that she used a copy of a co-worker's parking pass that she made without the co-worker's consent. The employee admitted to copying the pass during 2010. The employee admitted that she did not pay the biweekly fees associated with parking on a GPO lot during this period. Charges against the second employee were dropped as a result of the confession. The employee also received transit benefits, while parking on the

GPO parking lot. (Report of Investigation 12-0003-I)

Outcome: OIG confiscated the parking permit in January 2012. The employee entered into a deferred prosecution agreement to defer prosecution of this case for a period of 4 months. If the employee performs 32 hours of verified community service and pays $2,150 in restitution, the United States will dismiss the case.

In March 2012, the OIG received an allegation that one employee parked on a GPO parking lot without being enrolled in the program or paying parking fees. Our investigation revealed an employee parked in a GPO parking lot from July 2005 until February 2012 without paying any parking fees. A review of the employee's records disclosed the absence of any parking applications or allotment forms for the period. We confirmed allotments were not deducted from the employee's salary. This case was outside the scope of our audit work because the employee did not submit or participate in the GPO Parking Program. (Report of Investigation 12-0005-I)

Outcome: We issued a Report of Investigation to GPO that identified $4,498 worth of improper benefits received.

Opportunities for Improved Safeguards Over Tuition and Student Loan Reimbursements

GPO offers its employees a variety of training and educational opportunities to complement work experiences and achieve better organizational and individual performance. Under certain circumstances, GPO provides tuition reimbursement to its employees. GPO may also repay portions of student loans of employees it seeks to recruit and retain.

During FY 2011, 1 employee received a student loan reimbursement in the amount of $10,000, and 10 employees received reimbursements totaling $20,899 under the Tuition Reimbursement Program. Within the 3-year retention period of FY 2008 through FY 2011, eight employees were considered active participants in the Student Loan Reimbursement Program. GPO did not pay any tuition or student loan reimbursements during FY 2012. Because of budget constraints, both programs were temporarily suspended toward the beginning of the third quarter in FY 2011.

In July 2010, OIG received a hotline complaint alleging that a former employee was reimbursed $2,070 for tuition and book costs but separated from GPO before fulfilling the service agreement. We substantiated the allegation and reported the results in July 2011. As a result of this hotline complaint, OIG initiated an audit to determine the extent to which GPO safeguards its Tuition Reimbursement and Student Loan Reimbursement programs against employees not fulfilling service agreements.

The audit revealed that one employee receiving student loan reimbursements separated without fulfilling their service agreement and did not repay GPO the $10,000 owed and GPO could not produce copies of signed service agreements for two employees before they each received reimbursements. One of those employees separated without repaying GPO the $10,000 owed, and the employee who received tuition reimbursement separated without fulfilling the service agreement and did not repay GPO $779 owed.

We identified opportunities that would improve controls over college or university course selection. Courses should relate to the performance of an employee's duties or anticipated duties. We determined that of the 10 employees who participated in the Tuition Reimbursement Program, 6 were attending courses unrelated to job functions or reported to be pursuing college degrees contradicting GPO policy.

We believe that the lack of standard operating procedures and failure to monitor the program were major contributing factors to those conditions. Consequently, debts totaling $20,779 were not discovered and collected before the departures of the three employees. In addition, it is unclear what benefit GPO received from six employees attending courses unrelated to their job duties, totaling $4,955.

Recommendations: For this audit, we recommended that the Chief Human Capital Officer review the records involving the two former employees who received a student loan reimbursement without satisfying the 3-year work requirement before separating from GPO and initiate action to collect the funds from those employees. We also recommended that GPO review the records involving the former employee who received tuition reimbursement but did not satisfy the 6-month work requirement before separating from GPO and initiate action to collect the funds from that employee.

We also recommended that when the Tuition Reimbursement and Student Loan Reimbursement Programs are reactivated management should develop standard operating procedures for the programs. Management should also reiterate to Business Unit Heads course reimbursement requirements and restrictions as Directive 625.6a, Chapter 11,"Nominations for Outside Training," specifies. We further recommended that the Chief Human Capital Officer ensure that service agreements are processed before reimbursement of tuition and student loan repayment by effectively monitoring the

process and that Separation Clearance and Property Return Checklists are properly completed at the time an employee separates from GPO.

Management agreed with all of the recommendations. The Chief Human Capital Officer is working with the Office of Finance and Administration to collect the money the three former employees owe the Government. The Chief Human Capital Officer also stated that GPO would implement standard operating procedures, reiterate reimbursement requirements to Business Unit Heads, and ensure service agreements are executed for all student loan and tuition reimbursements when those programs are reactivated. Finally, the Chief Human Capital Officer stated that the Agency will issue appropriate checklists to departing employees and ensure that the checklists are completed. *(Opportunities Exist for Improved Safeguards over Tuition and Student Loan Reimbursements, Report No. 12-15, July 13, 2012)*

Violation by an Employee of Workers' Compensation

OIG received allegations that from November 2008 through July 2011 a GPO employee submitted a total of 200 transactions for the purchase of prescribed medications while at the same time there were no transactions that indicated a physician had seen the employee or that any physician had billed the Department of Labor for payment. In a joint investigation with the Department of Labor's OIG, we determined that the employee claimed and received $45,058 in prescription compensation for medications that were prescribed for conditions not accepted under the employee's compensation claim. (Investigation No. 11-0015-I)

Outcome: The Department of Labor's Office of Workers' Compensation Program established an overpayment in the amount of $45,058 and will pursue collection.

Allegations of Workplace Violence

OIG reviewed allegations that a GPO employee posed a threat to other employees and/or GPO. OIG conducted a threat assessment of the situation to identify if the employee exhibited threatening and/or violent behaviors toward other employees or GPO. (Management Implication Report No. 12-21, September 18, 2012)

Outcome: Based on statements the employee and other employees made, we determined the allegations had some merit and the employee posed some degree of a threat to other employees and GPO. GPO acted to mitigate the threat.

Select Other Investigative Matters

Several complaints resulted in referrals to GPO management for disposition.

- OIG received information that an employee received a recruitment bonus in which he was overpaid $750. The employee refused to remit the $750 because he claimed he never received the full amount of his bonus, even though GPO records revealed he signed for the bonus and it was cashed or deposited. Further investigation and additional interviews confirmed the employee received a check for $750 and processed it through his GPO Federal Credit Union bank account. The employee later returned the $750 when presented with evidence that he signed for and deposited the check.
- OIG received information that a print vendor submitted three invoices for $567 with the same date and the same shipping receipt. A review of invoices in the GPO's OnBase contract database revealed that in May 2012 the vendor submitted 116 invoices in which no jackets were invoiced multiple times. An interview with the vendor resulted in the vendor crediting the overbilled amount to GPO.
- OIG received allegations that several GPO managers suspected that they had been retaliated against for whistleblowing. We referred the allegations to GPO's Office of General Counsel for further assessment. GPO's Office of General Counsel will report the results when it completes the assessment.

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.

Independent Audit of Harris Corporation–FDsys Master Integrator

In 2004, GPO initiated the FDsys project to replace GPO Access as an improved means of providing public access to electronic documents for all three branches of the Federal Government. GPO awarded the FDsys Master Integrator contract to Harris Corporation Government Communication Systems Division of Melbourne, Florida (Harris).

Harris was required to design, develop, and then integrate the various FDsys components, technology, and applications. Initially, GPO planned for the basic FDsys functionality to be operational by July 2007, at a cost of $16 million. However, it was not until December 2010 that GPO announced FDsys as its official system of record for online Government information, 3 years behind schedule, with less functionality than originally planned, and at a higher cost than planned. We conducted an audit in 2011 to determine if GPO effectively administered the FDsys Master Integrator contract with Harris Corporation. The report was published in August 2011.

As a follow-on audit, the OIG contracted with the Defense Contract Audit Agency (DCAA) to determine whether the direct materials, direct labor, travel, and other direct costs of approximately $15 million charged by Harris were allowed. DCAA determined that the Harris-claimed direct costs were allocable and allowable as adjusted by the audit.

DCAA, however, questioned $1,178,814 of claimed costs for payments exceeding contract funding limits, overtime costs not approved as required by the contract, and unreasonable costs related to field premiums and cost of living allowance (COLA). *(Independent Audit of Harris Corporation – FDsys Master Integrator, Report No. 12-24, September 21, 2012)*

Recommendation: For this review, we recommended the Director for Acquisition Services recover questioned costs of $1,178,814.

ABBREVIATIONS AND ACRONYMS

AICPA	American Institute of Certified Public Accountants
C&A	Certification and Accreditation
CA	Certification Authority
CFR	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COLA	Cost of Living Allowance
CP&B	Congressional Printing and Binding
DCAA	Defense Contracting Audit Agency
DLA	Defense Logistics Agency
DDoS	Distributed Denial of Service
E&Y	Ernst & Young LLP
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
FY	Fiscal Year
GAO	Government Accountability Office
GPO	Government Printing Office
GSA	General Services Administration
HOIC	High Orbit Ion Cannon
IG	Inspector General
IT	Information Technology
JCP	Joint Committee on Printing
NACIC	National Agency Check with Inquiries and Credit Check
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SID	Security and Intelligent Documents
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification

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 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.

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

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

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

Unsupported Costs
Questioned costs not supported by adequate documentation.

APPENDICES

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	32
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	36
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	9-23
Section 5(a)(7)	Summary of Significant Reports	All

Index of Reporting Requirements under the IG Act of 1978 (continued)

REPORTING	REQUIREMENT	PAGE
Section 5(a)(8)	Statistical Tables on Management Decisions on Questioned Costs	33
Section 5(a)(9)	Statistical Tables on Management Decisions on Recommendations That Funds Be Put to Better Use	33
Section 5(a)(10)	Summary of Each Audit Report over Six Months Old for Which No Management Decision Has Been Made	32
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	37

APPENDIX B

Statistical Reports

Final Reports Issued and Grouped by OIG Strategic Goal

REPORT NAME	NO. OF RECOMMENDATIONS	QUESTIONED COSTS ($)	FUNDS PUT TO BETTER USE ($)	OTHER MONETARY IMPACT ($)
Transforming GPO into a Digital Platform				
Audit of Computer Security – Handling a Denial of Service, Report No. 12-13, June 28, 2012	2	0	0	0
WebTrust for Certification Authority, Report No. 12-22, September 18, 2012	0	0	0	0
Federal PKI Compliance Report, Report No. 12-23, September 18, 2012	0	0	0	0
IInternal Control Maturity Assessment – Inspectron Software Application, Report No. 12-09, April 16, 2012	2	0	0	0
Enhanced Architecture Maturity Could Better Guide GPO's Transformation, Report No. 12-19, September 28, 2012	3	0	0	0
Operational and Financial Management				
Operational Enhancements Could Further Improve the Congressional Billing Process, Report No. 12-16, September 21, 2012	3	0	$2,521,007	0
Audit of Controls over GPO's Fleet Credit Card Program, Report No 12 18, September 28, 2012	1	0	$4,751	0
Program and Operational Integrity				
GPO Parking Program: Opportunities Exists to Further Strengthen Controls, Report No. 12 14, July 25, 2012	5	0	$72,810	0
Opportunities Exist for Improved Safeguards over Tuition and Student Loan Reimbursements Report No. 12-15, July 13, 2012	5	0	$27,028	0
Audit of GPO's Suitability Process for Passport Production, Report No. 12-17, September 18, 2012	5	0	0	0
Management Implication Report, Workplace Violence, Report No. 12 21, September 18, 2012	0	0	0	0
Stewardship over Official Publications				
Independent Audit of Harris Corporation – FDsys Master Integrator, Report No. 12-24, September 21, 2012	1	$1,178,814	0	0

APPENDIX C

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

DATE ISSUED	NAME OF AUDIT	REPORT NUMBER	# OF RECOMMENDATIONS	COSTS ($)
9/30/09	FDsys IV&V – Ninth Quarter Report on Risk Management, Issues, and Traceability	09-12	1	0
11/16/11	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 Over 1-Year

DATE ISSUED	NAME OF AUDIT	REPORT NUMBER	NO. OF RECOMMENDATIONS	MONETARY IMPACT ($)
11/20/06	Early Oracle Implementation: Independent Verification and Validation (IV&V)	07-01	12	0
3/28/08	FDsys Independent Verification and Validation (IV&V) - First Quarter Observations and Recommendations	08-04	1	0
11/04/08	FDsys Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability	09-01	2	0
12/24/08	FDsys Independent Verification and Validation (IV&V) - Fifth Quarter Report on Risk Management, Issues, and Traceability	09-03	1	0
3/20/09	FDsys IV&V — Sixth Quarter Report on Risk Management, Issues, and Traceability	09-07	1	0
3/31/09	Oracle E-Business Suite Release 2 IV&V — Technical	09-08	3	0
9/30/09	FDsys Independent Verification and Validation — Seventh Quarter Report on Risk Management, Issues, and Traceability	09-12	6	0
12/2/09	Final Assessment Report on FDsys IV&V 9th Quarter Report on Risk Management, Issues, and Traceability	10-01	3	0
1/12/10	GPO FISMA	10-03	9	0
12/16/10	OIG Final Report on Audit of GPO's Ethics Program	11-01	2	0
12/6/10	Final Report on Audit of Control and Accountability of Laptop Computers	11-02	7	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 AND OTHER MONETARY IMPACT ($)
Reports for which no management decisions were made by beginning of reporting period	0	0
Reports issued during reporting period	5	
Audit Report – Operational Enhancements Could Further Improve the Congressional Billing Process, Report No. 12-16, September 21, 2012		$2,521,007
Audit Report – GPO Parking Program: Opportunities Exists to Further Strengthen Controls, Report No. 12-14, July 25, 2012		$72,810
Audit Report – Opportunities Exist for Improved Safeguards over Tuition and Student Loan Reimbursements, Report No. 12-15, July 13, 2012		$27,028
Audit of Controls over GPO's Fleet Credit Card Program, Report No. 12-18, September 28, 2012		$4,751
Independent Audit of Harris Corporation – FDsys Master Integrator, Report No. 12 24, September 21, 2012		$1,178,814
Subtotals	5	$3,804,410
Reports for which a management decision was made during reporting period		
1. Dollar value of recommendations not agreed to by management		
2. Dollar value of recommendations agreed to by management		$3,804,410
Reports for which no management decision was made by end of reporting period	0	0
Reports for which no management decision was made within 6 months of issuance	0	0

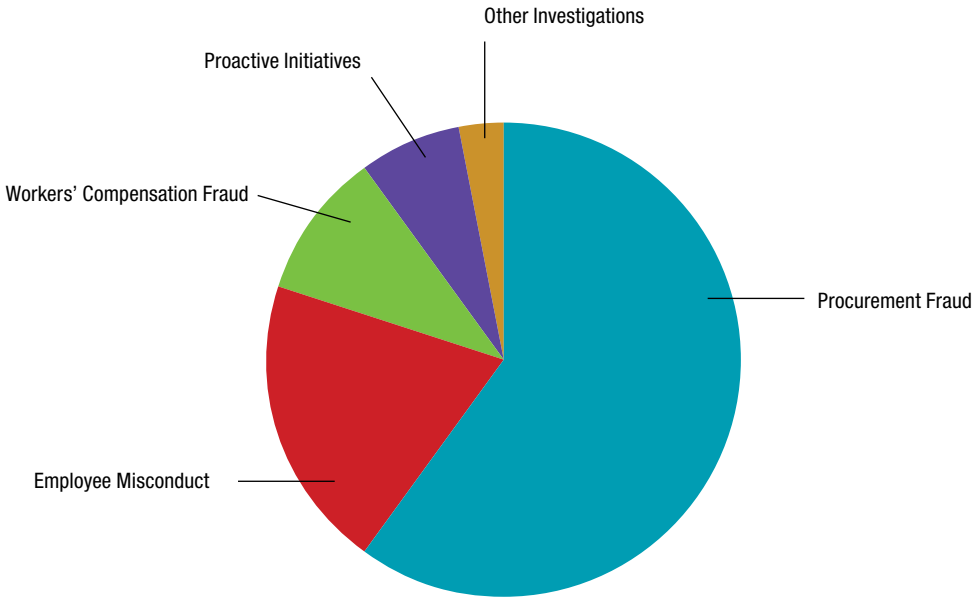
APPENDIX F

Investigations Case Summary

ITEM	QUANTITY
Total New Hotline/Other Allegations Received during Reporting Period	21
Preliminary Investigations (Complaints) Closed to the File	4
Complaint Referrals to Other Agencies	2
Complaint Referrals to OAI	1
Investigations Opened by OI during Reporting Period	6
Investigations Open at Beginning of Reporting Period	32
Investigations Closed during Reporting Period	8
Investigations Open at End of Reporting Period	30
Referrals to GPO Management (Complaints and Investigations)	10

CURRENT OPEN INVESTIGATIONS BY ALLEGATION	NUMBER	PERCENT
Procurement Fraud	18	60
Employee Misconduct	6	20
Workers Compensation Fraud (OWCP)	3	10
Proactive Initiatives	2	7
Other Investigations	1	3
Total	30	100

CURRENT OPEN INVESTIGATIONS BY ALLEGATION



APPENDIX G

Investigations Productivity Summary

ITEM	QUANTITY
Arrests	2
Total Presentations to Prosecuting Authorities	4
Criminal Acceptances	1
Criminal Declinations	1
Indictments	0
Convictions	0
Guilty Pleas/Deferred Prosecution Agreements	1
Probation (months)	0
Jail Time (days)	0
Civil Restitutions	0
Civil Acceptances	0
Civil Agreements	0
Civil Declinations	3
Amounts Recovered Through Investigative Efforts	$52,840
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	10
Contractor Debarments	6
Contractor Suspensions	0
Contractor Other Actions	2*
Employee Suspensions	2
Proposed Employee Suspensions	0
Employee Terminations	1**
Subpoenas	3

*Proposed Debarment

**Proposed Termination

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 Inspectors General 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 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 the 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. These 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

The GPO OIG conducted a peer review of Peace Corps OIG's audit organization for the year ended September 30, 2010, in accordance with generally accepted government auditing standards and guidelines established by the CIGIE. In our opinion, the system of quality control for the audit organization of the Peace Corps OIG was suitably designed and complied with to provide the Peace Corps 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.

NOTES

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