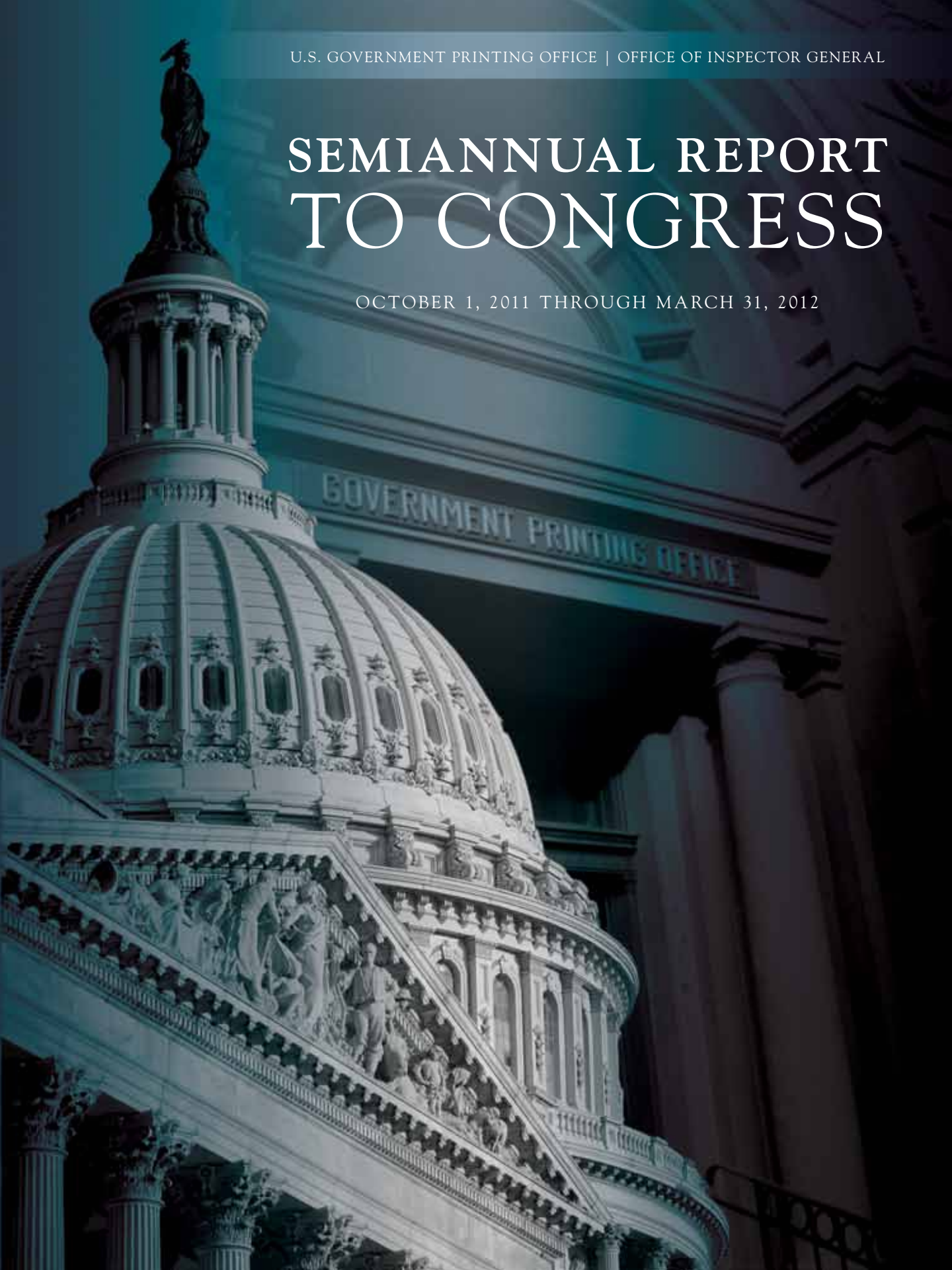


U.S. GOVERNMENT PRINTING OFFICE | OFFICE OF INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

OCTOBER 1, 2011 THROUGH MARCH 31, 2012



ABOUT THE 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 the production and distributing of information products and services for all three branches of the Federal Government, including U.S. passport for the department of State as well as the 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 (www.fdsys.gov) and through partnerships with approximately 1,200 libraries nationwide participating in the Federal depository Library Program.

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, to prevent and detect fraud, waste, and abuse in those programs and operations.

The GPO Inspector General Act of 1988, title II of Public Law 100-504 (October 18, 1988) establishes the responsibilities and duties of the Inspector General. 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 any problems or deficiencies relating to administering and operating GPO.



MESSAGE from the INSPECTOR GENERAL

This Semiannual Report to Congress covers the 6-month period ending March 31, 2012, and summarizes the most significant accomplishments of the GPO OIG. During this reporting period, our office continued to work extensively with GPO, Congress, and other Federal agencies by ensuring the integrity and efficiency of GPO programs and operations, safeguarding taxpayer investments in these programs, and investigating those allegedly abusing GPO programs.

Our accomplishments during this period are noteworthy. 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. During this reporting period, we issued 11 audit and other reports which, among other

things, recommended that \$3.3 million in funds be put to better use, identified funds that could be at risk, and made 65 program improvement recommendations. Our investigative work led to one conviction and identified \$405,691 in monetary fund's that could be at risk due to fraud.

We appreciate the interest and support shown GPO and the management team and look forward to working together to further reduce fraud, waste, and abuse; ensure that GPO programs and operations are efficient and cost effective; and help GPO respond to the demands of a challenging budget environment.

Michael A. Raponi
Inspector General



GOVERNMENT PRINTING OFFICE

CONTENTS

Selected Statistics	1
Management Challenges	3
Transforming GPO into a Digital Platform	7
Operational and Financial Management	9
Print Procurement Programs	11
Program and Operational Integrity	13
Stewardship over Official Publications	17
Abbreviations and Acronyms	21
Glossary	23
Appendices	25



SELECTED STATISTICS

INVESTIGATIONS

Investigative cost-efficiencies, restitutions, fines and penalties	\$405,691
Complaints opened	19
Complaints closed	15
Investigative cases opened	4
Investigative cases referred for prosecution/civil action	13
Investigative cases referred for administrative	17
Investigative cases accepted for prosecution	2
Investigative cases accepted for civil action	4
Investigative cases closed	13
Convictions	1
Debarments	16
Subpoenas issued	2

AUDITS AND INSPECTIONS

Audit and other reports issued	11
Funds recommended for better use or other	\$3.3 million
Number of Recommendations Made	65



MANAGEMENT CHALLENGES

As GPO has rethought and refocused efforts to carry out its mission, we realigned what the OIG considers the most serious management challenges facing the Agency at this time. For fiscal year (FY) 2012, we believe GPO faces the following major challenges:

- Keeping focus on its mission of information dissemination
- Addressing emerging workforce skills
- Improving the Infrastructure for GPO's FDsys
- Securing information technology (IT) systems and protecting related information assets
- Managing Workers' Compensation Programs
- Improving Print Procurement Programs

Keeping Focus on its Mission of Information Dissemination

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.

Addressing Emerging 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. Activities associated with creating congressional information databases comprise the vast majority of the work for the Congressional Printing and Binding Appropriation funds.

GPO's digital systems support several key Federal publications—including printing the U.S. Budget and the Federal Register, and associated products. The Agency uses advanced authentication systems, supported by public key infrastructure (PKI), which are 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. And 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 identification credential obtainable.

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. In addition, the secure credential unit is certified as the only Government-to-Government provider of credentials meeting the requirements of Homeland Security Presidential Directive-12 (HSPD-12).

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

Improving the Infrastructure for GPO’s FDsys

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

- A 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.
- A 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.
- An Advanced Search Engine – FDsys combines modern search technology with extensive metadata creation to ensure the highest quality search experience.

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

FDsys includes all known U.S. 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 U.S. Government publications in tangible and electronic collections.

Content is entered into the system, authenticated, and cataloged according to GPO metadata standards and best practices in document creation and management. Content can include a variety of formats – text and associated graphics, video and sound, and other forms of content. Those documents are then available for Web searching and viewing, downloading, and printing.

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

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-reader and smart phone users.

GPO executives and project managers may face challenges in managing system infrastructure developments and other related technology initiatives to accomplish them on time and within budget, and to ensure these initiatives function as designed.

Areas within the U.S. 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 life cycle.

These challenges are made more difficult by the nature of major IT system infrastructure developments, which typically occur over multiple years and are subject to changes in policy, priorities, funding, and innovations in technology.

Securing IT Systems and Protecting Related Information Assets

GPO systems contain vital information that is central to the GPO’s 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 GPO Web site, the Agency routinely communicates with the public routinely 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 due to resource constraints and competing priorities.

Challenge: Safeguarding information assets is a continuing challenge for Federal agencies, including GPO. Security challenges are increasing with employees' increased use of telework and reliance on new ways of communicating such as social

media technology, and mobile applications. The GPO is challenged to evolve and adapt its information security controls to keep pace with the risks new technologies pose.

Managing Workers' Compensation Programs

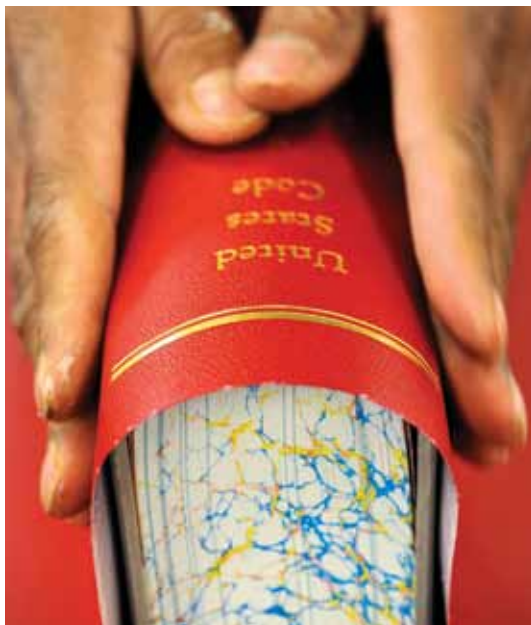
The Federal Employees' Compensation Act (FECA) Program provides wage loss compensation and pays medical expenses for covered Federal civilian and certain other employees who incur work related occupational injuries or illnesses. It also provides survivors benefits for a covered employee's employment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

The Department of Labor (DOL) administers the FECA Program and makes all decisions regarding the eligibility of injured workers to receive workers' compensation benefits. DOL provides direct compensation to medical providers, claimants, and beneficiaries. In addition to paying an administrative fee, GPO reimburses DOL for any workers' compensation claims.

For financial reporting purposes, future workers' compensation estimates are generated from the

application of actuarial procedures that DOL developed for estimating the liability for FECA benefits. The liability for future workers' 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 (SFFAS) No. 5, "Accounting for Liabilities for the Federal Government," and Statement of Financial Accounting Standards (SFAS) No. 112, "Employers' Accounting for Postemployment Benefits." Application of those accounting standards to "unfunded costs: (i.e., accrued long-term workers' compensation benefits) conflicts with the legislative intent of title 44 of the Code of Federal Regulations (44 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, can cause an imbalance in the GPO Revolving Fund not intended by legislation establishing this self sustaining revolving fund for GPO's operations.

Challenge: Because the FECA liability estimate is developed by DOL and out of the control of GPO, there is a risk that a significant, unexpected increase in the estimate could have a 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 ensuring 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 and by individuals who receive FECA benefits while working.

Improving Print Procurement Programs

GPO is the principal agent for almost all Government printing. Title 44 requires that any printing, binding, and blank-book work for Congress, the 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, must be accomplished at GPO. 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: Identifying violators of title 44 and working with Executive Branch agencies to prevent a loss of documents for the FDLP and preventing a potential higher printing cost due to inefficient printing by Executive Office agencies.



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.

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.

Controls over Information Security Management

The OIG contracted with KPMG, LLP, to audit the GPO financial statements. As part of this audit, KPMG identified a significant deficiency with IT security. The significant deficiency was not considered a material weakness. Audit results indicated deficiencies in the design and/or operations of GPO's IT general and application controls in the areas of security management, access controls, segregation of duties, configuration management, and contingency planning. Those conditions were generally the result of resource constraints and competing

priorities at GPO. (*Report on Business Information System (GBIS), Report No. 12-10, March 1, 2012 and Report on General Support System (GSS), Report No. 12-11, March 1, 2012*).

Security Management: GPO progressed toward formalizing its established information security objectives and high-level policy. KPMG noted however, that although GPO had completed a security assessment and authorization process for the GPO Business Information System (GBIS) and GPO General Support System (GSS), GBIS had been operating without an up-to-date security authorization since May 2010 when the Interim Authorization to Operate for GBIS expired. For both GSS and GBIS, KPMG also noted in the review that the System Security Plans and Risk Assessment Reports did not include IT security controls equivalent to the high impact control baseline from the National Institute of Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations."

Access Controls: Overall, access controls at GPO continue to require strengthening in order to provide a more secure environment. Management progressed in addressing access control deficiencies noted during previous reviews. However, KPMG noted user access was not consistently removed after users left GPO or changed job duties, periodic

reviews of user access were not consistently documented, and audit logs at the application level for GBIS were not reviewed.

Segregation of Duties: Effective segregation of duties starts with effective entity-wide policies and procedures that are implemented at the system and application levels. KPMG noted that although the Office of Finance and Administration segregation of duties procedures document conflicting activities within GBIS, the procedures were not sufficiently detailed to identify which roles within GBIS were considered conflicting. Not identifying conflicting roles within GBIS may lead to GBIS users having conflicting access to this key financial system, which could result in a user having end-to-end control over a transaction such that they could both initiate and approve an erroneous transaction.

Configuration Management: GPO did not centrally manage the security patching of desktop and laptop computers using Microsoft Windows. Desktop

and laptop computers without updated Windows security patches may not be properly safeguarded from security vulnerabilities. As a result, vulnerabilities may be exploited and data and resources may be subject to unauthorized use, loss or disclosure.

Contingency Planning: The contingency plan for GPO's GSS has not been finalized, approved or tested, and is still in draft form. Without a finalized and published contingency plan, GPO may not be able to successfully recover critical applications and systems to maintain business functions during the event of a service disruption.

Recommendation: KPMG recommended that the Chief Information Officer (CIO) continue strengthening its IT general and application controls over GBIS and GSS and ensure appropriate resources are available to provide effective oversight of the areas identified as significant deficiencies. Management agreed with the recommendations and stated that it is planning to implement these and other steps.





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 Statement Audit

GPO received an unqualified opinion on its annual consolidated financial statements. The OIG contracted with KPMG, LLP, to audit these statements. KPMG issued an unqualified opinion and concluded that GPO's financial statements were presented fairly. (*FY2011 Independent Auditors' Report on the U.S. Government Printing Office's FY 2011 Consolidated Financial Statements, Report No. 12-02, December 21, 2011*).

In considering the internal controls over financial reporting, KPMG identified a significant deficiency related to the control over processing and maintenance of human resource and payroll information. The significant deficiency was not considered a material weakness.

The auditors noted that 35 of 120 employees tested during the year were nominated and

approved for a goal sharing payment. Of those 35, auditors noted that 1 employee never received the goal sharing award of \$100 even though the employee was approved and included on the list of approved awardees.

Auditors also tested leave balances in the Web Time & Attendance (WebTA) system. The auditors noted that of the 120 balances reviewed, 24 did not agree with the annual leave balance recorded by the National Finance Center (NFC). NFC is GPO's service provider for payroll processing.

The auditors also noted that of the 72 employee files reviewed, the GPO payment plan reflected on the Standard Form (SF)-50, Notification of Personnel Action, 2 files did not agree with the GPO payment plan reflected on the SF-52, Request/or Personnel Action, maintained in the employee's personnel file.

Of the 120 WebTA sheets reviewed, 8 instances existed where the WebTA sheet was certified by a person not identified on the list of approved supervisors.

Recommendations: KPMG recommended that the Chief Financial Officer (CFO) strengthen its controls over the processing and maintenance of human resource and payroll information by performing a review of all information updated to the NFC to verify accuracy. They also recommended that the CFO accomplish the following tasks: (1) develop and implement procedures detailing how to

correctly enter leave adjustments in the WebTA system and the NFC mainframe, (2) develop and implement policies and procedures for payroll personnel to reconcile annual leave balances per WebTA to NFC, (3) establish improved communication with NFC to ensure that GPO payment plan information reflected on the SF-50's maintained in employee personnel files is accurate, and (4) develop and implement policies and procedures over the maintenance of authorized and approved WebTA certifiers.

Management concurred with these recommendations and has already worked to implement a corrective action plan.

Management Advisory Comments

In conjunction with the financial statement audit, KPMG issued a Management Letter to relay findings not included in the consolidated financial audit report but require management's attention toward ensuring a sound overall internal control structure and requiring management's attention. This report was intended to improve internal controls and other operational efficiencies. (*Management Advisory Comments Identified in the Engagement to Audit*

the Consolidated Financial Statements for the Year Ended September 30 2011, Report No.12-07, February 14, 2012).

The FY 2011 Management Letter identified eight findings with recommendations, some of which incorporated elements of prior years' findings related to GPO's operations and financial reporting controls.

- Improve controls over the Code of Conduct.
- Strengthen controls over maintenance of publications sales deposit account.
- Strengthen controls over paper inventory and recording inventory.
- Strengthen controls over the government accounts receivable reconciliation.
- Improve controls over account number 1214 reconciliation.
- Strengthen controls over the disposal of fixed assets.
- Improve controls over the non-GAAP thresholds for contingent liabilities.
- Strengthen controls over advanced billing.

The FY2012 financial statement audit will evaluate GPO's actions in response to the recommendations.





PRINT PROCUREMENT PROGRAMS

OIG STRATEGIC GOAL 3:

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

Vendor Invoice Processing: Printing

During this reporting period, OIG closed four investigations of vendors who falsified from 2006 until 2012 approximately 79 invoices and shipping documents totaling approximately \$405,691. As part of these investigations, OIG discovered that vulnerability existed with the verification of shipments which had allowed vendors to obtain payment without fulfilling contract terms.

Procedures require that vendors submit receipts or shipping documents, or both, that equal the quantity ordered and the quantity billed. Carriers must sign and indicate an actual pickup date on both Government bills of lading and commercial bills of lading. Straight bills of lading are not considered adequate shipping documentation. They must be commercial carrier airway or freight bills.

GPO has generally relied on the honesty and integrity of vendors and pays the vendors upon receipt of the required documentation during invoice processing. GPO does not perform any online verification of vendor invoices and/or shipping claims with the commercial carrier. The investigation uncovered the following flaws in the system.

(Vendor Invoice Processing: Printing, Management Implication Report No. 12-01, March 15, 2012)

- A vendor disclosed that it submitted 126 invoices from 2006 through April 2008 totaling \$416,022, along with shipping documentation, requesting rapid compensation in exchange for a discount. For at least 50 invoices and shipping documents, totaling \$368,093, the documents stated work was complete and shipped to the customer when in fact, shipment was not complete.

Outcome: In 2009, the vendor received a 3-year debarment from contracting with GPO.

- A vendor submitted a false claim in 2009 for payment. A comparison between the actual U.S. Postal Service shipping receipt and documentation submitted disclosed that the vendor altered the shipping receipt to reflect an additional \$1,271 of shipping costs over the actual costs.

Outcome: The vendor admitted to altering the shipping receipt and in February 2012 began a 3-year debarment from contracting with GPO.

- In 2012, a vendor invoiced \$90,585 for services. That amount was the full contract price. The vendor was required to produce, bind, and ship 23,600 handbooks to the Defense Automated Printing Service (DAPS). However, DAPS received only 15,600 handbooks (a shortage of 8,000) because the vendor submitted false shipping documents. The failure of that vendor cost GPO approximately \$30,681.

Outcome: In February 2012, the vendor began a 3-year debarment from contracting with GPO.

- From October 2008 through February 2011, a vendor submitted 130 invoices totaling \$24,100. For at least 27 invoices and Federal express (FedEx) receipts, totaling \$5,741, the vendor admitted pre-billing GPO by submitting false FedEx shipping documents before the required work was complete. The vendor denied pre-billing for the 22 items.

Outcome: Effective November 2011, the vendor began a 3-year debarment from contracting with GPO.

This Management Implication Report was for informational purposes and we recommended working with the commercial carrier to determine if an online verification process would reduce the vulnerability.



ANALYSIS

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.

Management Controls over Overtime Pay

Federal employees are expected to complete assigned duties during regular working hours. On occasion, however, employees may need to work overtime.

We conducted an audit to determine if opportunities existed at GPO that would enhance controls and provide assurance overtime was necessary.

The audit concluded that during FY 2011 and FY 2012, GPO significantly reduced overtime costs, citing that overtime costs dropped approximately 33 percent (\$4 million) in FY 2011 from 192,073 hours in FY 2010 to 129,298 hours in FY 2011. We commend GPO in its accomplishment.

We did, however, bring to the Agency's attention inherent risks that could jeopardize its ability to either maintain or achieve, or both, future overtime reductions.

For the first quarter of FY 2012, we estimated that of the 18,393 hours of paid overtime, 14,163 hours (77 percent) were not authorized before employees worked. Managers reported that such a situation was primarily the result of oversight and a long-standing

management practice of approving overtime while certifying payroll at the end of each pay period rather than before the work was performed. We noted in the report that GPO policies do not require that an employee's supervisor obtain approval before working overtime.

We estimated that GPO paid without prior approval \$741,794 for overtime during the first quarter of FY 2012. We believe that GPO may have paid at least \$2,967,176 in overtime pay in FY 2011 if the same conditions were applied to overtime paid during FY 2011. (*Maintaining Effective Control over Employee Overtime, Report No. 2-08, March 30, 2012*)

We recommended the Acting Public Printer consider (a) modifying GPO Directive 640.7D, "General Pay Administration," dated April 2008 requiring that supervisors obtain approval before asking employees to work overtime; (b) reiterating the requirement to approve overtime requests before employees work; and (c) establishing a process for monitoring compliance with the Directive.

Management generally agreed with the recommendations.

Time and Attendance and Payroll Administration

Management requested that OIG audit the various components of time and attendance and payroll administration. Management expressed concern that it may not always be complying with certain

statutes and directives related to payroll processing. As a result, managers were also concerned about excessive use of Leave Without Pay (LWOP) and employee Absent Without Leave (AWOL) throughout the Agency.

We believe that GPO should strengthen controls related to: requesting and approving LWOP, detecting instances of employees exceeding bi-weekly pay limitations, and advancing annual leave. The audit revealed 340 violations to pay limitations in 2009 and 2010. As a result of those violations, the Agency overpaid about \$372,717. (*Selected Aspects of GPO Time and Attendance and Payroll Administration, Report No. 12-01, November 16, 2011*)

Of the 11 recommendations we made, management agreed with 6. We asked for additional information to clarify those with which it disagreed. We will continue to provide updates on the status of the recommendations.

Violations by Employees of Workers Compensation

GPO Employee Disclosure of Outside Employment Earnings

OIG received an allegation regarding an employee receiving benefits from the Office of Worker's Compensation Program (OWCP) while employed. Our investigation revealed that the employee stated he or she was not employed outside GPO, when, in fact, that employee was. As a result of those false statements, DOL assessed the employee an overpayment of \$374. The employee was subsequently terminated. (*Report of Investigation No. 10-00023-1*)

Former Employee Operates Janitorial Service While Receiving Disability Compensation

OIG investigated a former GPO employee who failed to disclose self-employment on 25 monthly reports—DOL Form CA-7, Claim for Compensation—filed



between 2008 and 2010. The former employee also omitted earnings from a self owned and operated business on the DOL Form CA-1032, Request for Information on Earnings, Dual Benefits, Dependents and Third Party Settlements Form, submitted in December 2011. Because of these omissions, the former employee's disability compensation was not offset to account for earnings received. The findings of this investigation were forwarded to DOL to recover the compensation paid in accordance with subsection 10.529, title 20, Code of Federal Regulations (20 CFR § 10.529), and for any other action as deemed appropriate. *(Report of Investigation No. 11-0006-1)*

Employee Misconduct

Employee Pleads Guilty to One Count of Attempted Deceptive Labeling

On September 7, 2011, the OIG received information that a GPO employee was using GPO computer systems to make illegal copies of movies on DVDs.

A search of the employee's work area found the employee sitting at a GPO computer, which had a Web site for movies on the monitor. We discovered DVDs with various titles of movies, movie cases, printed copies of movie labels with various titles, and a list of movies written on a piece of card board. A search of a bag located on the table, to which the employee admitted belonged to him, revealed several more DVDs with various titles.

Several of these movies appeared to be pornographic. The employee admitted making illegal copies of movies using GPO computer systems. The employee denied selling the movies and stated that he only gave the movies away. On November 14, 2011, the employee appeared in Superior Court of the District of Columbia (DC Court) and plead guilty to one count of Attempted Deceptive Labeling. He received a 60-day suspended sentence, 9 months unsupervised probation, and a \$50 fine.

On March 1, 2012, the employee resigned from his position in lieu of termination/disciplinary action. *(Report of Investigation No. 11-0017-1)*

Employee Engages in Prohibited Activities on GPO Grounds

OIG received a complaint alleging that an employee sold cigarettes on GPO property to other employees. The confidential source alleged that an employee sold Virginia taxed cigarettes to numerous GPO employees for approximately \$6 a pack. The source also alleged that the employee loaned money to other GPO employees, all while on GPO property. The source further alleged that the employee charged \$25 in interest for every \$100 borrowed and charged an additional \$75 every pay-period until the borrower repaid the loan.

We substantiated the allegations that the employee sold cigarettes and made usurious loans to GPO employees on GPO property in violation of GPO Directives 825.38A

Rules and Regulations Governing Buildings and Grounds, dated August 2010 and 655.3A, Standards of Conduct for Government Printing Office, Officers and Employees, dated June 1988. The employee received a letter of warning. *(Report of Investigation No. 10-0018-1)*



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.

System Development of FDsys

OIG contracted with American Systems of Chantilly, Virginia to conduct an Independent Verification & Validation (IV&V) in accordance with methodology established by the Institute of Electrical and Electronic Engineers (IEEE) Standard 1012-2004, the IEEE Standard for Software Verification and Validation. The OIG issued four reports on the development of FDsys.

The Fifteenth (15th) IV&V Quarterly Report covers development work performed from March 11, 2011, through July 6, 2011

The fifteenth assessment provided a high-level overview of key technical, schedule, and cost risks during the period. American Systems made 11 recommendations designed to strengthen FDsys program management, particularly for future FDsys releases. During this reporting period, the FDsys Program Management Office completed the deployment of four (4) Release 2 production builds and prepared/updated FDsys technical documentation.

The key recommendations included the following tasks:

- update the GPO FDsys Master Test Plan to convey a complete and comprehensive strategy that will delineate, define, and describe the testing approach to be implemented for all levels/phases of testing that will be conducted on the FDsys,
- update the FDsys Program Management Plan and initiate the use of earned value analysis,
- conduct more frequent internal Program Management Reviews,
- develop and implement a Quality Assurance Program,
- develop and implement a Quality Assurance Surveillance Plan to oversee contracted work,
- develop and implement an organizational change management program,
- ensure that all required testing is performed on the FDsys COOP Instance,
- verify functional requirements using the Demonstration and/or Test verification methods,
- develop a solution and/or workaround so that the FDsys Production Instance and the FDsys COOP Instance can meet the 20,000 concurrent-user requirements,
- form a requirements Integrated Product Team or equivalent that consists of members of the system and software engineering teams, and members of the test team.

(FDsys IV&V Fifteenth Quarter Report, Report No.12-03, January 18, 2012).

Management generally agreed with the recommendations.

The Sixteenth (16th) IV&V Quarterly Report covers development work performed from July 7, 2011, through September 30, 2011

The sixteenth assessment provided a high-level overview of the key technical, schedule, and cost risks identified during the period. American Systems made 10 recommendations designed to strengthen FDsys program management, particularly for future FDsys releases. During this reporting period, the FDsys PMO deployed two Release 2 production builds, and prepared/updated FDsys technical documentation.

The key recommendations included the following tasks:

- update the FDsys Requirements Management Plan to reflect use of Microsoft (MS) Excel as the requirements management tool. The Plan should also redefine the processes needed to maintain the requirements' records, and the responsibilities associated with the MS Excel requirements database,



- ensure that the RTVM is consistent, as of its issue date, with the information contained in the FDsys Master Requirements List,
- draft a Program Directive indicating that the requirements derivation process will not be implemented for remaining high-level requirements unless a new feature is introduced that impacts those existing requirements,
- create a single report that aligns the system requirements, derived requirements, software components, and Test Cases,
- reestablish an active risk management program,
- develop a strategy for FDsys moving forward; i.e., will the design and development of FDsys to the original requirements set continue, or will further efforts on the Program be restricted to responding to other government agency requests,
- form a requirements working group, which includes members of the design, development, and testing teams, to decompose high-level requirements into derived requirements,
- develop a project management resources plan.

(FDsys IV&V Sixteenth Quarter Report, Report No.12-04, February 24, 2012).

Management generally agreed with the recommendations.

The Seventeenth (17th) IV&V Quarterly Report covers development work performed from October 1, 2011, through December 31, 2011

The seventeenth assessment noted that the FDsys Program did not maintain the Master Schedule on a consistent basis. There are activities and tasks in the Master Schedule (December 9, 2011 version) with dates that were overdue. The date did not change, and were not 100 percent complete. They were not deemed to have an effect on the overall scheduled completion of the Group D activities. Technical risks, schedule risks, and cost risks inherent with the technical issues were identified during the October to December 2011 timeframe. (FDsys IV&V Seventeenth Quarter Report, Report No.12-05, February 27, 2012).



During the period, no new recommendations were made because the issues were encompassed by open recommendations reported in previous reports.

FDsys IV&V Training Material and User Documentation Analysis Report

The assessment noted that since the original plan was reviewed and evaluated in March 2009, the FDsys Documentation and Training Plan (D&TP) has been brought up to date. The assessment also noted, however, that the document was not updated for Release 2. In addition, training was not delivered in accordance with the schedules in the training plan. That condition was probably because the FDsys Program had to respond to requests from other Government agencies for development of additional Collections or other applications, and sufficient time was unavailable to permit the review and update of the training material in a timely manner.

Key recommendations focused on improving the User Manual, improving training sessions and material, and making improvements to the D&TP.

Recommendations to improve the User Manual by revising it to include all of the features specified in Section 4 of the D&TP and update user manuals to reflect changes to the system resulting from correction of system problems and updates to system functionality in Release 2. It was recommended to improve training sessions and material by adding user exercises specific to each user role to the training sessions, updating training material to reflect changes to the system resulting from correction of system problems, and having the trainer check with the trainees periodically to make sure none of them are stuck or lost. It was also recommended to improve the D&TP by having the PMO update the D&TP for Release 2, capturing software and process changes related to each specific user category. (*FDsys Release 2 Training Material, User Documentation, and Training Implementation Task Report, Report 12-06, February 24, 2012*).

Management agreed with the recommendations.



ABBREVIATIONS and ACRONYMS

AWOL	Absent Without Leave	IPA	Independent Public Accountant
CFO	Chief Financial Officer	IT	Information Technology
CIGIE	Council of the Inspectors General on Integrity and Efficiency	IT&S	Information Technology and Systems
CIO	Chief Information Officer	IV&V	Independent Verification and Validation
COOP	Continuity of Operations	JCP	Joint Committee on Printing
D&TP	Document and Training Plan	LWOP	Leave Without Pay
DAPS	Defense Automated Printing Service	NFC	National Finance Center
DHS	Department of Homeland Security	NIST	National Institute of Standards and Technology
FDsys	Federal Digital System	OAI	Office of Audits and Inspections
FECA	Federal Employees' Compensation Act	OI	Office of Investigations
FISMA	Federal Information Security Management Act	OIG	Office of Inspector General
FY	Fiscal Year	OWCP	Office of Worker's Compensation Programs
GAAP	Generally Accepted Accounting Principles	PMO	Project Management Office
GBIS	GPO Business Information System	SAR	Semiannual Report to Congress
GPO	U.S. Government Printing Office	SF	Standard Form
GSS	General Support System	SFAS	Statement of Financial Accounting Standards
HSPD	Homeland Security Presidential Directive	SFFAS	Statements of Federal Financial Accounting Standards
IEEE	Institute of Electrical and Electronics Engineers	WebTA	Web Time & Attendance
IG	Inspector General		



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	28
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	32
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	7–19
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	None
Section 5(a)(9)	Statistical Tables on Management Decisions on Recommendations That Funds Be Put to Better Use	29
Section 5(a)(10)	Summary of Each Audit Report over Six Months Old for Which No Management Decision Has Been Made	28
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	33

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				
Report on Business Information System (GBIS), Report No. 12-10, March 1, 2012	8	0	0	0
Report on General Support System (GSS), Report No. 12-11, March 1, 2012	4	0	0	0
Operational and Financial Management				
FY 2011 Independent Auditors' Report on the U.S. Government Printing Office's FY 2011 Consolidated Financial Statements, Report No. 12-02, December 21, 2011	5	0	0	0
Management Advisory Comments Identified in the Engagement to Audit the Consolidated Financial Statements for the Year Ended September 30 2012, Report No.12-07, February 14, 2012	8	0	0	0
Print Procurement Programs				
Vendor Invoice Processing: Printing, Management Implication Report No. 12-01, March 15, 2012	0	0	0	405,691
Program and Operational Integrity				
Maintaining Effective Control over Employee Overtime, Report No.12-08, March 30, 2012	2	0	2,967,176	0
Selected Aspects of GPO Time and Attendance and Payroll Administration, Report No. 12-01, November 16, 2011	11	0	372,717	0
Stewardship over Official Publications				
FDsys IV&V Fifteenth Quarter Report, Report No.12-03, January 18, 2012	11	0	0	0
FDsys IV&V Sixteenth Quarter Report, Report No.12-04, February 24, 2012	10	0	0	0
FDsys IV&V Seventeenth Quarter Report, Report No.12-05, February 27, 2012	0	0	0	0
FDsys IV&V Training Material and User Documentation Analysis Report	6	0	0	0

APPENDIX C

Unresolved Audit Recommendations More Than 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	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
9/28/07	Perimeter Security Assessment of a GPO Building	07-10	2	0
3/28/08	FDsys Independent Verification and Validation (IV&V) - First Quarter Observations and Recommendations	08-04	2	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	9	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	10	0
12/16/10	OIG Final Report on Audit of GPO's Ethics Program	11-01	6	0
12/6/10	Final Report on Audit of Control and Accountability of Laptop Computers	11-02	6	0

APPENDIX E

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

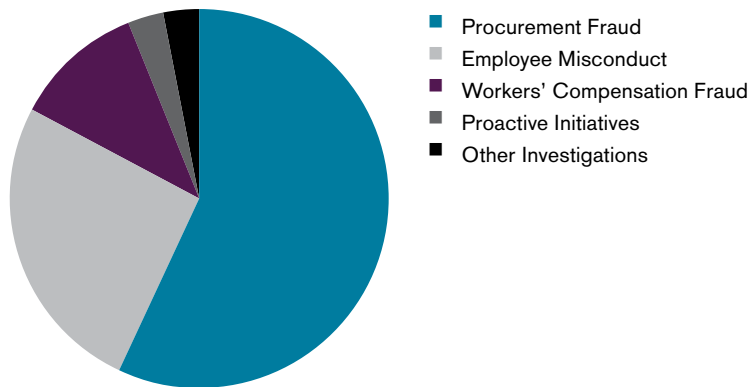
DESCRIPTION	NUMBER OF REPORTS	FUNDS PUT TO BETTER USE AND OTHER MONETARY IMPACT (\$)
Reports for which no management decisions were made by beginning of reporting period	0	0
Reports issued during reporting period	3	
Selected Aspects of GPO Time and Attendance and Payroll Administration, Report No. 12-01 November 16, 2011		372,717
Maintaining Effective Control over Employee Overtime Report No.2-08, March 30, 2012		2,967,176
Vendor Invoice Processing: Printing, Management Implication Report No. 12-01 March 15, 2012		405,691
Subtotals	3	3,745,584
Reports for which a management decision was made during reporting period		
1. Dollar value of recommendations not agreed to by management		3,372,867
2. Dollar value of recommendations agreed to by management		372,717
Reports for which no management decision was made by end of reporting period	0	0
Reports for which no management decision was made within six months of issuance	0	0

APPENDIX F

Investigations Case Summary

ITEM	QUANTITY
Total New Hotline/Other Allegations Received during Reporting Period	19
Preliminary Investigations (Complaints) Closed to the File	15
Complaint Referrals to Other Agencies	3
Complaint Referrals to OAI	0
Investigations Opened by OI during Reporting Period	4
Investigations Open at Beginning of Reporting Period	40
Investigations Closed during Reporting Period	13
Investigations Open at End of Reporting Period	36
Referrals to GPO Management (Complaints and Investigations)	17

CURRENT OPEN INVESTIGATIONS BY ALLEGATION	NUMBER	PERCENT
Procurement Fraud	20	57%
Employee Misconduct	9	26%
Workers' Compensation Fraud	4	11%
Proactive Initiatives	1	3%
Other Investigations	1	3%
Total	35	100%



APPENDIX G

Investigations Productivity Summary

ITEM	QUANTITY
Arrests	1
Total Presentations to Prosecuting Authorities	23
Criminal Acceptances	2
Criminal Declinations	11
Indictments	0
Convictions	1
Guilty Pleas	1
Probation (months)	9 Months
Jail Time (days)	60 Days*
Civil Restitutions	\$50
Civil Acceptances	4
Civil Agreements	0
Civil Declinations	4
Amounts Recovered Through Investigative Efforts	\$5,437
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	17
Contractor Debarments	13
Contractor Suspensions	0
Contractor Other Actions	1**
Employee Suspensions	1
Proposed Employee Suspensions	0
Employee Terminations	4
Subpoenas	2

*Suspended Sentence

**Proposed Debarment

APPENDIX H

Peer Review Reporting

The following meets the requirement under Section 989C of the Dodd-Frank Wall Street Reform and Consumer Protection Act (P.L. 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 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 provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards. The peer review gave GPO-OIG a pass rating.

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.

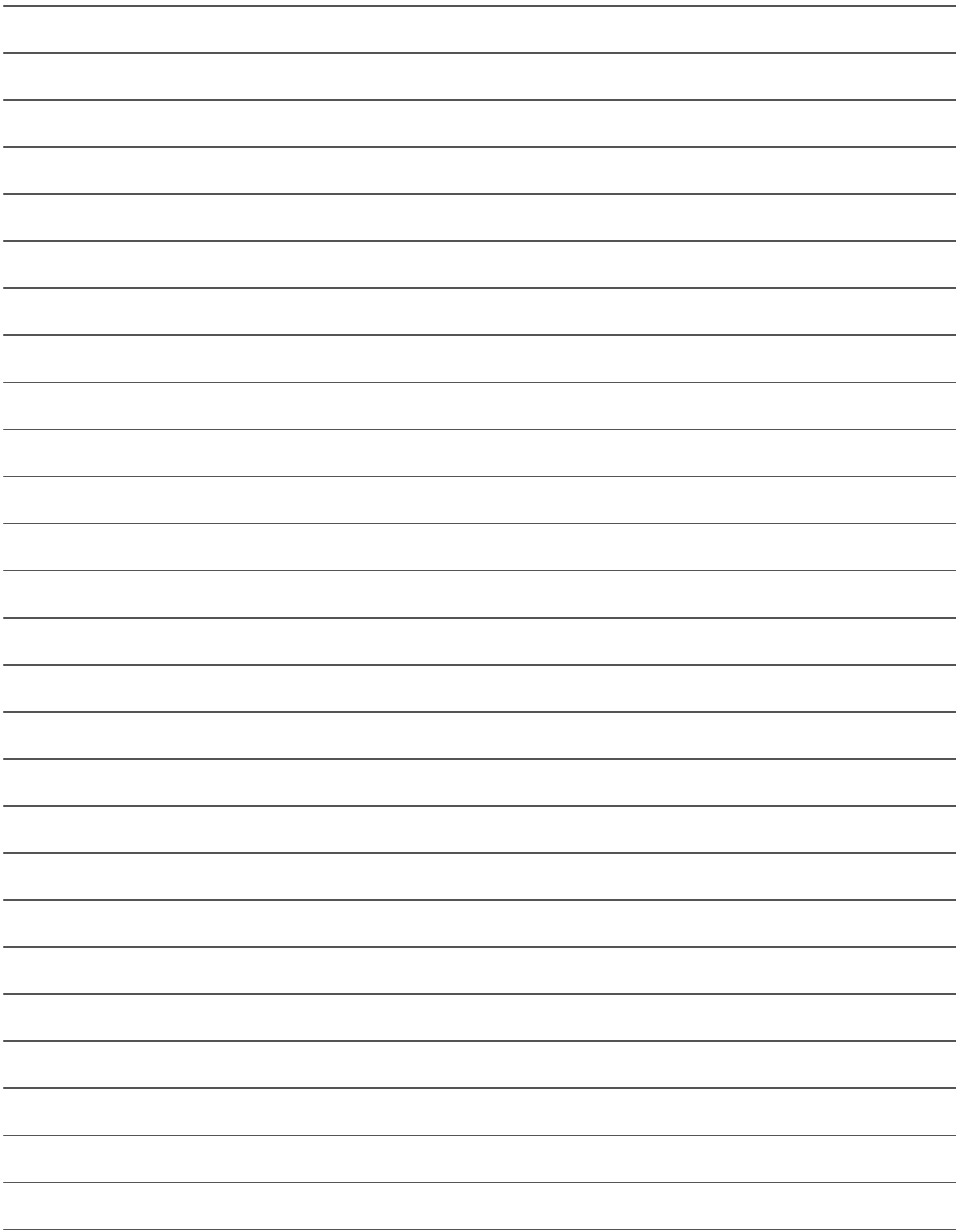
The National Science Foundation OIG reported that the system of internal safeguards and management procedures for the investigative function for the year ended 2010 complies with the quality standards established by the President’s Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency, the 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.





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

732 North Capitol Street, N.W. Washington, DC 20401

202-512-0039 | WWW.GPO.GOV/OIG

OIG HOTLINE 1-800-743-7574 | GPOOIGHOTLINE@GPO.GOV

