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

SEMIANNUAL REPORT TO CONGRESS

10.1.12 THROUGH 3.31.13

ABOUT THE GOVERNMENT PRINTING OFFICE

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 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/.

A MESSAGE FROM THE INSPECTOR GENERAL

I am pleased to submit this Semiannual Report to Congress, which highlights the most significant activities and accomplishments of the OIG for the 6-month period ending March 31, 2013. Our audits and investigations continue to assess the effectiveness, efficiency, economy, and integrity of GPO programs and operations.

During this reporting period, we issued 12 audit and other reports that, among other things, identified funds put to better use in the amount of $1.4 million and other monetary impact related to financial accounting totaling $24.4 million. Among our many significant accomplishments, we reported on the following Agency activities:

- Effectiveness of general and application Information Technology (IT) controls supporting financial processing environment and related IT infrastructure.
- Conformity of consolidated financial statements with generally accepted accounting principles.
- Effectiveness of internal controls over financial reporting.
- Process GPO followed when accepting risks associated with major legacy and minor applications.
- Follow-on work of Enterprise Architecture associated with Oracle licenses.
- Key aspects of Federal Employees' Compensation Act (FECA) operations related to returning claimants to work.
- Oversight of current and former employee indebtedness.
- Effectiveness of automation as it relates to continuous monitoring for the FDsys and whether GPO has an effective vulnerability scanning process for its networks and databases including a corrective action process for correcting known vulnerabilities.

Our investigative work led to $2,204 in restitution, six debarments, four referrals to management for potential administrative action, and one personnel action.

These accomplishments clearly demonstrate the exceptional work done by our professional and dedicated OIG staff. I want to express my appreciation for the hard work performed by our employees who strive to execute the OIG mission to improve the economy, effectiveness, and efficiency of GPO programs as well as prevent and detect fraud, waste, and abuse. I also thank the Acting Public Printer and other senior GPO officials for their support of our work and their receptiveness for improving Agency programs and operations.

Michael A. Raponi
Inspector General

CONTENTS

SELECTED STATISTICS

AUDITS AND INSPECTIONS

Audit and other reports issued . . . 12

Funds put to better use . . . $1.4 million

Other monetary impact (financial accounting) . . . $24.4 million

Number of recommendations made. . . . 41

INVESTIGATIONS

Investigative cost efficiencies, restitutions, fines and penalties . . . $2,204

Complaints opened . . . 20

Complaints closed . . . 8

Investigative cases referred for prosecution. . . . 2

Investigative cases referred for administrative/civil action . . . 2

Investigative cases closed . . . 3

Debarments . . . 6

MANAGEMENT CHALLENGES

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

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

CHANGES FROM PREVIOUS REPORTING PERIOD

In the previous reporting period, the consideration of internal controls over financial reporting resulted in a significant deficiency related to IT, which was reported in the Audit of GPO's Consolidated Financial Statement audit. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

During this period, we note progress in correcting a number of those internal control deficiencies. As a result, the significant deficiency was removed. Because of those improvements, we combined the challenge associated with improving the Enterprise Architecture and Infrastructure to support enterprise-wide and FDsys transformation with an earlier management challenge of securing IT systems and protecting related information assets.

We added a new challenge as a result of the high level of uncertainty to which the impact of sequestration and future budgetary caps on Federal agencies will result in reduced orders for printing and related information product services to GPO.

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

CHALLENGE 1: 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 continues its efforts to plan for and respond to future changes. GPO has enhanced its strategic planning efforts by requiring Business Units to revise their strategic plans to better align with the GPO strategic plan. GPO has also incorporated scenario planning into its strategic planning process.

GPO continues its efforts to develop an organizational model where the chief executive officer and managing directors focus their efforts on organizational policy and long-range planning and the second in command serves as chief operating officer focusing on the day-to-day operations of the business.

CHALLENGE 2: ADDRESSING EMERGING WORKFORCE SKILLS

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

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

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

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

GPO's Progress: GPO continues to further develop and update its workforce plan to better support transformation by adopting a more strategic view of human capital management and by having human resources officials work collaboratively with GPO managers. 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.

GPO has designated Human Capital with providing leadership and support to Business Units for identification of training needs and accomplishment of training plans that include training on new technology.

GPO is also developing and institutionalizing a human capital planning capacity based on a recent recommendation by the National Academy of Public Administration to effectively integrate and align the Agency's human resources policies, programs, and practices with its strategies for achieving mission success and desired programmatic results.

CHALLENGE 3: IMPROVING THE ENTERPRISE ARCHITECTURE, INFRASTRUCTURE, AND IT SECURITY TO SUPPORT ENTERPRISE-WIDE AND FDSYS TRANSFORMATION

Overview: GPO relies extensively on computerized information systems and technology to support its transformation. The Government classifies Enterprise Architecture as an IT function and defines the term not as the process of examining the enterprise but as the documented results of that examination. Specifically, Chapter 36, Title 44 of the United States Code defines enterprise architecture as a "strategic information base" that defines the mission of an agency and describes the technology and information needed to perform that mission, along with descriptions of how the architecture of the organization should be changed in order to respond to changes in the mission. GPO's FDsys provides free online access to official information for the three branches of the Federal Government. FDsys includes all known Government documents within the scope of GPO's FDLP.

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

Challenge: Existing Enterprise Architecture and IT infrastructure may not be able to support the changes and increasing demands that GPO anticipates, including more support for mobile applications addressing the expanding market of e-readers and smart phone users.

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

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.

GPO's Progress: Recent audit work revealed improvements within IT security and systems related to financial reporting. For Fiscal Year (FY) 2012, the significant deficiency was removed. In previous years, 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. While GPO has made progress in its security program and closing several OIG recommendations, a significant number of OIG recommendations remain open. Previous reports recommended corrective action related to identified weaknesses in compliance with configuration management, identity and access management, incident response and reporting, risk management, security training, remote access management, and contingency planning.

Efforts to develop a fully mature Enterprise Architecture have been underway since 2008. In September 2012, we compared GPO's progress with the Government Accountability Office (GAO) framework for determining maturity of GPO's Enterprise Architecture. In 2010, GPO performed a self-assessment using the GAO framework and 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. Based on both our audit and the GPO self-assessment conducted in 2010, GPO had not fully expanded and evolved the Enterprise Architecture and its use for transformation and optimization. We found similar results with the architecture maturity level of FDsys, which has not yet evolved to support transformation or optimization. GPO has developed and continues to implement an Enterprise Architecture policy, created the Enterprise Architecture Program Office, appointed a Chief Architect, uses an automated tool that contains reference models that assist in developing an Enterprise Architecture, and from 2008 to 2010 established an Architect Review Board.

GPO provided corrective action plans that address the recommendations in our audits and reported some corrective actions as complete. However, vulnerabilities continue to exist, and GPO needs to effectively address and eliminate IT security deficiencies where possible, continue providing mitigating controls for vulnerabilities, and implement remaining planned actions to correct system weaknesses.

CHALLENGE 4: MANAGING WORKERS' COMPENSATION PROGRAMS

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

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

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

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

GPO's Progress: GPO developed or plans to develop corrective action plans that address various aspects of 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) regular basis medical updates, and (5) 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 has also provided some training to Business Unit managers and supervisors to provide them with an understanding of their responsibilities under FECA and is planning on expanding the use of IT to administer the program. GPO reported that beginning April 30, 2013, employees will have the option to use the Department of Labor's Employees' Compensation Operations and Management Portal system to perform certain functions related to filing workers' compensation cases.

CHALLENGE 5: IMPROVING PRINT PROCUREMENT PROGRAMS

Overview: GPO is the principal agent for almost all Government printing. Title 44 requires that GPO accomplish any printing, binding, and blank-book work for Congress, executive branch offices, the Judiciary—other than the Supreme Court of the United States—and every Executive Office, independent office, and establishment of the Government. The only exceptions

include: (1) classes of work that the Joint Committee on Printing (JCP) considers urgent or necessary to be completed elsewhere, (2) printing in field printing plants operated by an Executive Office, independent office, or establishment, and (3) procurement of printing by an Executive Office, independent office, or establishment from allotments for contract field printing, if approved by the JCP.

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

GPO's Progress: GPO is continuing to work 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.

GPO continues to work with GAO in support of a request JCP made in April 2012 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 initiated an internal project to develop a blueprint it can use to identify instances of fugitive printing activity.

CHALLENGE 6: UNCERTAINTIES RELATED TO SEQUESTRATION AND FUTURE BUDGETARY CAPS

As part of the Budget Control Act of 2011, across-the-board cuts, also known as sequestration, were included for the purpose of compelling Congress to act on deficit reduction and reaching a budget compromise. Without a compromise, the cuts were initially set to begin on January 1, 2013, but that date was postponed by 2 months by the American Taxpayer Relief Act of 2012. On March 1, 2013, the President issued a sequestration order canceling $85 billion in budgetary resources across the Federal Government for FY 2013. Those across-the-board budget reductions remain in effect for FY 2013 and will also result in a lowering of discretionary caps and sequestration of mandatory spending in the years 2014 through 2021.

On March 1, 2013, OMB's Report to the Congress on sequestration for FY 2013 reported a 5-percent reduction to the level of appropriations provided to GPO under the continuing resolution for the first 6 months of FY 2013 (P.L. 112-175). Subsequently, Congress and the President enacted a continuing appropriations bill (P.L. 113-6) for the balance of FY 2013 that reduced GPO's funding by an additional 2.6% from a combination of funding reductions and sequester action. GPO reported a final net FY 2013 appropriation reduction totaling 7.4 percent from the beginning of FY 2013.

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

GPO Progress: GPO has increased scrutiny on discretionary bonuses, new hiring, training, conference and travel spending, and some capital investment. GPO has also initiated scenario-based strategic planning to help with the fiscal uncertainties. GPO is also closely monitoring Federal agencies spending on printing in its Print Procurement Program.

TRANSFORMING GPO INTO A DIGITAL PLATFORM

OIG STRATEGIC GOAL 1:

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

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

Controls Over Information Security Management

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

OIG contracted with KPMG, LLP, to audit the GPO financial statements. As part of this audit, weaknesses were noted with IT security related to its financial systems. Audit results indicated deficiencies in the design and/or operations of GPO's IT general and application controls in the areas of access controls, security patches, and contingency planning. Those conditions were generally the result of resource constraints and competing priorities at GPO.

Access Controls. In close concert with an organization's entity-wide information security program, access controls for General Support System (GSS) and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized modification, disclosure, loss, or impairment. Overall, access controls at GPO continue to require strengthening in order to provide a more secure environment. It was noted that: (1) GPO Business Information System (GBIS) segregation of duties does not identify conflicting roles, and (2) access control activities have not been performed consistent with Federal Information Processing Standards (FIPS) requirements and the National Institute of Standards and Technology (NIST) guidance.

Configuration Management. Configuration management involves identification and management of security features for hardware, software, and firmware components of an information system at a given point and systematically controls configuration changes throughout the system's life cycle. During the FY 2012 IT control testing, it was noted GPO did not centrally manage the security patching of Windows desktops and laptops for all of FY 2012. Centralized patch management was not fully implemented until August 2012.

Contingency Planning. Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. For that reason, an agency should have (1) procedures in place for protecting information resources and minimize the risk of unplanned interruptions and (2) a plan for recovering critical operations should interruptions occur. It was noted the GSS contingency plan has not yet been finalized, approved, and tested.

Recommendation: It was recommended that the Chief Information Officer (CIO) continue strengthening its IT general and application controls over GBIS and GSS. Management agreed with the recommendations and stated that it plans to implement these and other steps. *(GSS – Notification of Findings and Recommendations Related to the General and Application Controls Testing Fiscal Year 2012 Audit of GPO's Consolidated Financial Statements, Report No. 13-08, February 12, 2013, and GBIS – Notification of Findings and Recommendations Related to the General and Application Controls Testing Fiscal Year 2012 Audit of GPO's Consolidated Financial Statements, Report No. 13-07, February 12, 2013, and Management Advisory Comments From the Review of Information Technology Controls in Support of the Consolidated Financial Statement Audit for the Year Ended September 30, 2012, Report No. 13-11, March 29, 2013).*

OPERATIONAL AND FINANCIAL MANAGEMENT

OIG STRATEGIC GOAL 2:

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

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

Financial Statement Audit

GPO received an unqualified opinion on its annual consolidated financial statements. The OIG contracted with KPMG, LLP, to audit these statements. GPO received an unqualified opinion and it was concluded that GPO's financial statements were presented fairly.

In considering the internal controls over financial reporting, a material weakness was identified. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. Deficiencies were noted over financial reporting in all key process areas relating to preparation, review, and posting of journal entries and review and approval of account reconciliations. It was also noted that manager and supervisor reviews were not performed timely or at a precision level that would detect and correct a material misstatement. Collectively, those matters are considered to be a material weakness in internal controls over financial reporting.

The following items are examples of weaknesses noted during the audit:

- One accounts payable year-end entry for $12.2 million was recorded incorrectly and not identified during management's review, resulting in a $24.4 million misstatement of accounts payable. In addition, the same entry for $12.2 million was not supported by documentation but rather $9 million was the correct amount that should have been recorded. Management subsequently recorded entries to correct the errors as of September 30, 2012 (12-NFR-13).
- The year-end salary payable reconciliation was not properly prepared or reviewed as of September 30, 2012. Specifically, the original reconciliation

provided did not agree with the general ledger by $5.9 million. (12-NFR-12).

- The audit noted $862,319 in advanced billings recorded incorrectly. GPO management performed additional analysis of advanced billings and identified overstatements of $5.1 million related to 2012 transactions and $1.4 million related to prior fiscal years (12-NFR-16).
- The audit identified $200,000 discrepancies in the accruals, GPO management performed additional analysis of the accrued expenses and determined further adjustments netting to $2.3 million in overstatement were required (12-NFR-15).

In addition, one significant deficiency was identified in processing and maintenance of human resource and payroll information. Several matters were noted that highlighted the need for improved internal controls over processing and maintenance of human resource and payroll information.

Recommendation: The most significant recommendations made included: (1) develop and implement policies and procedures that would ensure transactions recorded in accounts are appropriate throughout the year, (2) provide training to personnel for increasing their understanding of the subsidiary ledgers and reports used in the reconciliation process, (3) require that reconciliation preparers ensure the completeness and accuracy of information before performing the reconciliations, (4) perform reviews of reconciliations in a timely manner and at a monetary precision level that would detect and correct material errors, (5) perform a review of all information uploaded to the National Finance Center (NFC) to verify that the upload was successful and accurate, (6) develop and implement policies and procedures for employees and supervisors to reconcile annual leave balances and timely inform payroll personnel of any corrections that need to be made to ensure accurate leave balances are maintained, (7) improve communication with NFC to ensure that the GPO payment plan information reflected on the appropriate form maintained in employee personnel files is accurate and employee pay plans provided to NFC agree with employee actions and their personnel file, and (8) develop and implement policies and

procedures over the maintenance of authorized and approved Web Time and Attendance certifiers.

OIG also recommended that the Chief Financial Officer prepare a comprehensive Corrective Action Plan (CAP) for addressing the material weakness identified in the consolidated financial statement audit. The CAP should include measurable indicators of compliance and resolution to assess and validate progress throughout the resolution cycle. GPO should closely monitor and update the CAP periodically.

Management concurred with these recommendations and has already worked to implement a CAP. *(FY 2012 Independent Auditors' Report on the U.S. Government Printing Office's FY 2012 Consolidated Financial Statements, Report No. 13-09, February 28, 2013).*

Management Advisory Comments

In conjunction with the financial statement audit, a Management Letter was issued to GPO relaying findings not included in the consolidated financial audit report requiring management's attention toward ensuring a sound overall internal control structure and requiring management's attention. The report was intended to improve internal controls and other operational efficiencies.

The FY 2012 Management Letter identified three findings with recommendations, some of which incorporated elements of previous findings related to GPO's operations and financial reporting controls.

- Improve controls over the Code of Conduct
- Strengthen controls over the disposal of fixed assets
- Strengthen controls over deposit account maintenance

Generally, it was recommended that: (1) GPO should update and approve their Code of Conduct and distribute to employees on a periodic basis, (2) GPO accountants should review invoices and purchase orders related to fixed asset additions to determine that all related costs are appropriately and timely recorded as of the in service date, and (3) GPO should continue to conduct periodic assessments of all inactive deposit accounts to determine the appropriate action for these accounts.

The FY 2013 financial statement audit will evaluate GPO's actions in response to the recommendations. *(Management Advisory Comments Identified in the Engagement to Audit the Consolidated Financial Statements for the Year Ended September 30, 2012, Report No. 13-10, March 20, 2013).*

PRINT PROCUREMENT PROGRAMS

OIG STRATEGIC GOAL 3:

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

Audit of Computer Security: GPO's Risk Acceptance Process for Major Legacy and Minor Applications

In September 2012, Information Technology & Security (IT&S) requested that the Acting Public Printer accept the security risk for 8 of its 16 major legacy applications. IT&S reported that none of 16 applications completed a Certification and Accreditation (C&A). IT&S reported many of the eight major applications recommended for potential risk acceptance have been in operation for more than 20 years without any known IT security incident or fraudulent usage incident.

The eight major legacy applications support both GPO's print procurement programs and print production operations. GPO's print procurement programs provide comprehensive print procurement services to the entire Federal Government. The print procurement process uses predominately manual processes with information organized in a now aging computer mainframe environment. GPO's print production operations are configured primarily to meet the basic needs of Congress. GPO produces the daily and permanent editions—in both online and print formats—of the Congressional Record, bills, resolutions, amendments, hearings, committee reports, committee prints, documents, stationery, and a wide variety of other products. GPO is in the process of increasing efficiencies within the print procurement process and Plant Operations and is planning to reduce its reliance on existing mainframe technology.

Our audit revealed that GPO could benefit by obtaining additional information to make a risk acceptance decision for its major legacy and minor applications. For the eight major legacy applications, our audit revealed: (1) applications were not categorized as low, moderate, or high risk based on the confidentiality, integrity, and availability of the information it stores, processes, or transmits; (2) risk assessments were not conducted assessing the sensitivity

of data, threats, vulnerabilities, and effectiveness of current and/or proposed safeguards or documenting the risk assessments; and (3) risk acceptance procedures or guidelines were not fully developed. We believe the condition to be true for all 16 legacy major applications. Without categorizing, conducting risk assessments, and providing a uniform approach to risk acceptance, GPO cannot be assured that management controls in place apply the appropriate level of controls for preventing unauthorized access, use, disclosure, disruption, modification, or destruction.

Also, GPO could not demonstrate minor applications and subsystems with varying impact levels had adequate protection established either by major applications or general support systems. That condition was the result of GPO's use of a streamlined security process.

If an incident were to occur, GPO could experience anywhere from minor delays to major service disruptions. For example, GPO's print procurement process relies on major legacy applications to generate random and rotating potential vendor lists for solicitations based upon order specifications, allow print procurement customers to place orders directly with a GPO contractor, format payment files to produce checks, provide order entry capability, order status, contractor performance history, quality records, exception reports, and order-tracking.

For GPO's print production operations, a senior manager stated that if the Production on Estimating and Planning System, a major legacy application, is offline, the impact would affect GPO's ability to provide congressional and executive agency publications.

Recommendation: We recommended that the CIO: (1) categorize applications as low, moderate, or high risk based on the confidentiality, integrity, and availability of the information it stores, process, or transmits; (2) conduct risk assessments that include, at a minimum, an assessment of the sensitivity of data, threats, vulnerabilities, and effectiveness of current/proposed safeguards, and document the risk assessments; (3) develop procedures or guidance that adequately provide detailed instructions for risk acceptance; (4) determine if each major application or general support system provides adequate protection to subordinate minor applications; and (5) inform Business Units about the exposure and potential impact on the business unit's operations if the security solution in regard to the identified risk or risks, or both, is not feasible or cannot be implemented.

Management stated that the recommendations were reasonable activities generally requiring long-term remediation actions and requiring a significant investment by GPO. Management either concurred or partially concurred with the recommendations. Partial concurrence was based on budgetary limitations. We consider management's planned actions responsive to the recommendations. *(Audit of Computer Security: GPO's Risk Acceptance Process for Major Legacy and Minor Applications, Report No. 13-05, February 13, 2013).*

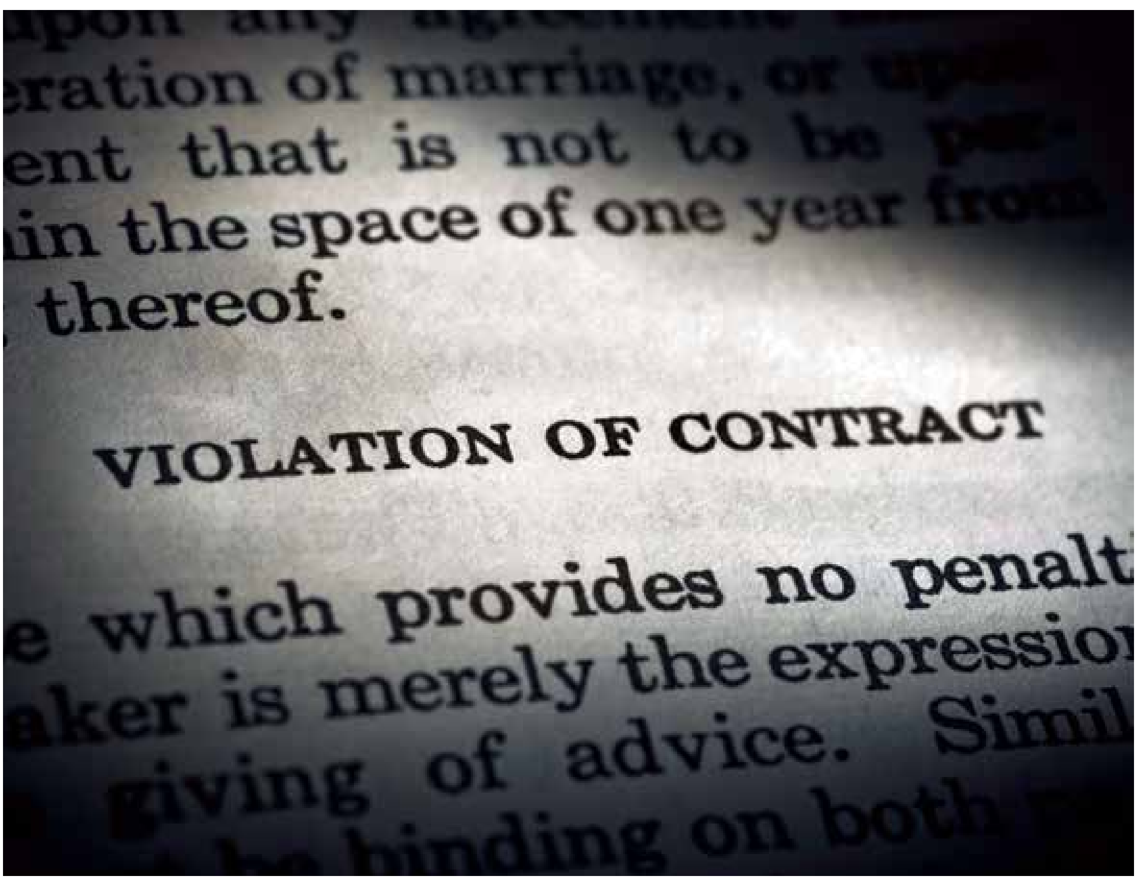
Fredericksburg, Virginia, Media Company and Owner Debarred

An OIG investigation revealed that Philip Leonhardt, owner of CSL Media, willfully submitted false claims and statements related to 159 invoices, totaling more than $235,000, by certifying CSL Media independently fulfilled the contracts awarded to the company under the GPO Simplified Purchase Agreement program when, in fact, Mr. Leonhardt subcontracted the work to another GPO vendor.

Outcome: On February 25, 2013, the GPO Debarring and Suspending Official debarred CSL Media, LLC and Mr. Leonhardt as GPO contractors, subcontractors, or contractor representatives. The debarments end on July 26, 2016. *(Report of Investigation No. 11-0010-I)*

Rock Falls, Illinois, Company and Owners Debarred

The OIG received information regarding allegations of prohibited brokering, forgery, and bid collusion on the part of business partners, Richard Keefe and Russell McSweeney of MBK Services. The complainants alleged that Keefe and McSweeney procured GPO contracts for companies for a commission in violation of GPO Publication 310–Contract Terms



(Rev. 6-01). It was also alleged that in an attempt to procure GPO contracts, Keefe forged the signature of company representatives on bid solicitations in violation of section 1001, title 18, United States Code, "Fraud and False Statements." The complainants believed Keefe and McSweeney submitted bids to GPO on the behalf of at least 10 companies possibly in violation of section 1, title 15, United States Code –"Trusts, etc.," in restraint of trade illegal. *(Case No. 10-0020-I)*

Outcome: On February 25, 2013, the GPO Debarring and Suspending Official debarred MBK Services, Inc., Richard Keefe, Russell McSweeney, and Marcel Keefe, owners of MBK Services, as GPO contractors, subcontractors, or contractor's representatives. The debarments end on July 26, 2016.

Vendor Misrepresents Invoice Quantity

The Chicago-Regional Printing Procurement Office reported that a print procurement vendor received payment from GPO for a product that was never delivered. The vendor entered into a contract agreement with the GPO on April 18, 2008, thereby agreeing to produce and deliver 60 tents to the U.S. Navy Recruiting Command. Our investigation disclosed the vendor delivered only 10 viable tents. It also showed the vendor submitted an invoice on June 23, 2008, for $176,640, and a second invoice on January 5, 2009, for $20,689 to GPO for payment. GPO paid $174,873.60 on July 8, 2008, based on the invoice and shipping documentation he submitted on June 23, 2008. *(Report of Investigation No. 10-0027-I)*

Outcome: As a result of the vendor's non-compliance and lack of communication, GPO was forced to re-procure the entire U.S. Navy Recruiting Command contract in February 2009 for $183,410.89. In October 2012, the OIG referred the vendor to GPO for suspension and/or debarment after an on-going investigation revealed the vendor willfully violated Print Procurement contract terms, causing GPO to incur a loss of more than $180,000.

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.

Opportunities Exists to Reduce Costs Associated with Oracle Software Licensing

The audit was a follow-on audit related to work on GPO's Enterprise Architecture in 2012 in which OIG reported that 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. 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. The purpose of the audit was to identify any major instances of potential duplication and overlap of Oracle modules and licenses present and if so, which controls could be strengthened to mitigate the condition.

For FY 2013, GPO reported it will spend approximately $3.2 million on Oracle licenses. Today, in addition to an expanded role in Finance and Administration, GPO uses Oracle to support Business Units such as Plant Operations, Library Services and Content Management, Security and Intelligent Documents, and Customer Services. GPO has executed four key contracts with Mythics, an Oracle resale partner that represents the entire Oracle product line of software, support, hardware, engineered systems, and appliances.

The audit disclosed that GPO has worked toward modernizing information systems in which Oracle products play a key role. However, given that GPO will spend approximately $3.2 million on Oracle licenses in FY 2013, further analysis is necessary to ensure all current Oracle licenses and products are needed. For example, we identified 14 instances where GPO pays for both an application user license and processor license for the same Oracle products costing $301,547. We noted GPO uses Oracle on Demand hosting for its e-Passport production to maintain standby databases, a master repository, and the NetApp Snap Mirror costing GPO $583,693 when a less expensive alternative may be available. We also identified excess user licenses and processor licenses, which may result in cost savings. We attribute those instances to the lack of policies and procedures for software license management and an incomplete inventory of Oracle products that crosswalks to GPO applications. As a result, GPO may be paying for excess and duplicate Oracle licenses and products.

Recommendation: The OIG recommended that the CIO mitigate risks of potentially investing in duplicative licenses by (1) developing and implementing processes, policies, and procedures to address goals and objectives of software license management program, (2) conducting an assessment of the current Oracle software licenses and Oracle products versus GPO requirements to determine the correct license and product mix and make the necessary adjustments, and (3) revising the current inventory listing to include a crosswalk from major Oracle commercial-off-the-shelf (COTS) software products to GPO applications.

Management concurred with the recommendations. Management reported they will document and assign license management duties for each of its component divisions and a single lead will be established to monitor and coordinate license management activities while validating planned renewals or purchase. Management will conduct a license audit for all Oracle products. In addition, management will develop a crosswalk to illustrate how each licensed feature of the Oracle product line maps to usage by the COTS and custom developed applications to ensure that GPO is not paying for unnecessary features. *(Opportunities Exists to Reduce Costs Associated with Oracle Software Licensing, Report No. 13-06, March 29, 2013)*

Management Oversight: Federal Employees' Compensation Act Operations

GPO has financial and management responsibilities for its own FECA cases. The costs of FECA benefits are initially paid by the Department of Labor through the Employee Compensation Fund, which the Office of Workers' Compensation Programs (OWCP) administers. At the end of each fiscal year, GPO reimburses the FECA program for their employees' FECA expenses through a process known as chargeback. Within GPO, the Workers' Compensation Services administers the FECA program. Between July 2011 and March 2012, GPO paid $4.4 million on 201 cases under DOL's FECA program. The figure does not include payments made for the first 45 days when a claimant is in a Continuation of Pay status.

We conducted the audit to assess GPO's monitoring of key aspects of its FECA operations related to returning claimants to work. We also reviewed training of GPO personnel, such as ensuring that supervisors understand their responsibilities under FECA and the reliance of IT to administer the program.

We identified opportunities where additional action could strengthen monitoring FECA operations. At a minimum, monitoring FECA should include: (1) updating the current marital status of claimants, (2) evaluation of the continued eligibility of the claimants dependents, (3) seeking opportunities to bring claimants back on a modified, limited, or light duty assignment, (4) receiving medical updates on a regular basis, (5) obtaining second medical opinions where the record indicates the claimant has some potential of eventually returning to work, (6) responding to requests for vocational training, and (7) requesting employees are included in OWCP's Assisted Reemployment program. While it may perform many of these duties on an ad hoc basis, GPO could not demonstrate that it monitors FECA on a program-wide basis. GPO could also strengthen Business Unit supervisor understanding of their responsibilities under FECA and expand the use of IT to administer the program.

We attributed this to current practices and procedures not fully addressing monitoring, supervisory FECA training and IT used to administer FECA program. Taking the actions may provide opportunities to better assess the overall risk of improperly paying compensation and medical costs and may reduce the amount paid or result in the removal of claimants from the periodic roll and to re-employment. For example, although not reviewing claim files, we did observe four instances where GPO missed opportunities to return claimants to work, resulting in $267,161 worth of FECA compensation paid while each claimant could have returned to work.

Recommendation: The OIG recommended that the Chief Human Capital Officer further strengthen FECA operations by developing procedures and a standardized program-wide monitoring process for routinely monitoring adherence to FECA requirements; strengthen Business Unit supervisor understanding of responsibilities under FECA by developing and implementing a formal training program; and, expand use of IT to administer the program such as the use of Department of Labor's Employees' Compensation Operations and Management Portal electronic software.

Management agreed with the recommendations and will develop a database to improve monitoring claimant's status. Major updates will be performed on a quarterly basis in coordination with the receipt of the Chargeback report. Management will also conduct quarterly briefings and/or Q&A sessions for all managers. Management initiated a Memorandum of Understanding with the Department of Labor and received a briefing in January on the Employees' Compensation Operations and Management Portal electronic software. *(Management Oversight: Federal Employees' Compensation Act Operations, Report No. 13-01, January 15, 2013)*

GPO Faces Challenges with Current and Former Employee Indebtedness

We conducted the audit to determine if opportunities existed to enhance controls over the prevention, establishment, and collection of debts owed GPO by current and former employees.

The audit disclosed that generally GPO has worked toward developing policies that meet the objectives of the Debt Collection Improvement Act of 1996. However, several key areas existed where improvements would enhance controls over prevention, establishment, and collection of debts owed GPO by current and former employees. Specifically, management could not demonstrate that it followed proper procedures for 95 percent of the sample population. The audit identified deficiencies related to administrative oversight, un-recouped advanced leave, un-recouped health benefits paid by GPO during leave without pay (LWOP), and un-recouped pay advances. We noted that 40 percent of the employees listed were delinquent more than 180 days and were either not transferred to the Department of the Treasury for servicing or serviced by GPO using similar collection techniques.

We found that improvement was needed in regard to certain controls, specifically (1) coordination between the Offices of Finance and Administration and the Chief Human Capital Officer was not always present, (2) clearance procedures were not always followed in determining if employees had outstanding debts when terminated, transferred, or separated, (3)

GPO did not maintain adequate records and reports of debts owed by employees, (4) collection procedures, including the withholding of an employee's final paycheck, were not always followed to ensure prompt and aggressive follow-up collection action on accounts, and (5) standard operating procedures for referring delinquent debt more than 180 days to the Department of the Treasury or conduct debt servicing with similar collection techniques were not developed.

Recommendation: The OIG recommended that the Chief Human Capital Officer Revise GPO Directive 610.16, "Procedures for Employees Separating From the GPO," to inform employees that the failure to complete and submit the Separation Clearance and Property Return Checklist (GPO Form 2938) may result in the withholding of any final payments due the separating employee.

We also recommended that the Chief Financial Officer: (1) periodically monitor NFC collection activities associated with employee indebtedness to ensure that all collection activities are achieving the intended results and incorporate the requirements of transferring employee debt greater than 180 days to the Department of the Treasury for debt servicing (or develop a process that will provide similar serving activities), maintaining sufficient supporting documentation for all debts, and withholding the final paycheck of all separating employees who are in debt to the Agency, into all pertinent standard operating procedures and/or Directives.

Management agreed with the recommendation and will revise Directive 610.16 to strengthen the debt collection efforts. Management has begun to implement a number of actions. The Office of Finance and Administration is currently working with the Office of the Chief Human Capital Officer and NFC to review, research, and collect debts recorded in both GPO's and NFC records. The Agency is also revising its Debt Collection Directive. In addition, it will incorporate the requirements of transferring employee debt greater than 180 days to the Department of the Treasury for debt servicing (or develop a process that will provide similar serving activities), maintaining sufficient supporting documentation for all debts, and withholding the final paycheck of all separating employees who are in debt to the Agency, into all pertinent standard operating procedures and/or Directives. *(GPO Faces Challenges with Current and Former Employee Indebtedness, Report No. 13-02, March 27, 2013)*

Employee Misconduct: GPO Parking Program and Transit Subsidy Program Violations Result in a Last Chance Agreement and Restitution

In November 2012, a GPO employee returned to duty after signing a Last Chance Agreement following an OIG investigation that revealed the employee knowingly violated the terms of the GPO Parking and Transit Subsidy programs for personal gain. *(Report of Investigation No. 12-0003-I)*

Outcome: The Last Chance Agreement included, among several conditions, a 1-year ban from participating in both programs and a restitution order to repay GPO the balance of the monies lost as a result of the employee's fraud. The employee previously repaid GPO a partial amount of the identified loss as a result of a deferred prosecution agreement issued prior to the Last Chance Agreement.

Employee Misconduct: Prohibited Political Activity by GPO Employees

On September 24, 2012, OIG received an anonymous complaint complaining of an invitation to a partisan political event that was sent via email by a co-worker. The email was sent in the GPO employee's official capacity to numerous other GPO email accounts. Further, although the invitation referred to a free event, the email included boilerplate language at the bottom that encouraged the recipient to contribute time and money to "help . . . make this campaign a success."

The investigation revealed the employees used their official GPO e-mail accounts to facilitate partisan political activity that violate the Hatch Act.

The Hatch Act and GPO's "Standards of Conduct for Government Printing Office Officers and Employees" prohibits employees from knowingly soliciting a political contribution from any person except in certain instances not applicable in this case. Employees are further prohibited from engaging in political activity while on duty and employees are prohibited from engaging in political activity in a government building. *(Report of Investigation No. 13-0001-I)*

Outcome: In March 2013, the OIG referred the investigative matter regarding alleged Hatch Act violations by three employees to GPO for administrative action consideration.

OIG coordination with the Department of Justice resulted in the investigative findings being declined for criminal prosecution in lieu of the respective Assistant U.S. Attorney's desire to defer the matter to GPO and, possibly, GPO's referral to the Office of Special Counsel for adjudication.

Employee Misconduct: Gambling on Government Property and Refusing to Cooperate

OIG received information from the Uniform Police Branch that a complaint was made alleging an employee engaged in questionable transactions on GPO property. In November 2012, the employee voluntarily agreed to answer questions after acknowledging receipt and understanding of a Garrity warning, which is equivalent to a non-custodial Miranda warning. During this joint interview with Uniform Police Branch, the employee admitted to engaging in sports betting (gambling) on GPO property with an estimated 15 to 20 GPO employees. He provided other employees with a pre-printed document consisting of point spreads for various professional and college football games for the purpose of betting. A spread is a range of outcomes and the bet is whether the outcome will be above or below the spread. He said he received 10 percent of the total weekly amount bet. Employees bet $5 to $10 to each, resulting in an average total collection of $300 per week.

The employee refused to identify the other GPO

employees involved or any other facts. GPO employees are required to cooperate fully with any OIG investigation, as Directive 655.38, "Standards of Conduct for Government Printing Office Officers and Employees," dated September 24, 2012, prescribes and that states public service is a public trust, requiring employees to place loyalty to the Constitution, the laws, and ethical principles above private gain. *(Case No. 13-0007-C)*

Outcome: In March 2013, OIG referred the investigative matter regarding alleged employee misconduct to GPO for administrative action consideration. OIG coordination with the Department of Justice resulted in the investigative findings being declined for criminal prosecution in lieu of the respective Assistant U.S. Attorney's desire to defer the matter to GPO for adjudication.

Employee Misconduct: Unreported Allegations of Illegal Drug Possession

OIG completed an inquiry into allegations that an employee was arrested and charged with possession of a controlled dangerous substance. In 1986, the

President signed Executive Order 12664, which establishes the goal of a drug-free Federal workplace. The order requires that Federal employees refrain from using illegal drugs both on and off duty. Policy states the use of illegal drugs by a GPO employee presents critical safety and health risks to the employee and others because of the agency's industrial environment. Therefore, to establish a drug-free GPO workplace program, the policies of the GPO are as follows: (1) GPO is a drug-free workplace, (2) employees must refrain from the use of illegal drugs, and (3) Individuals who use illegal drugs are not suitable for employment in the GPO and, if employed, may be dismissed. The policy requires that managers, supervisors, and employees report any suspected sale, use, or possession of illegal drugs.

Our inquiry revealed that the employee was arrested and charged on two separate occasions and cited on one occasion from November 2011 through April 2012 in three different jurisdictions—each of the three incidents involved drugs and/or alcohol and occurred while off-duty. Our inquiry revealed no evidence that the employee reported any of the instances to management or Security Services, as required. *(Case No. 13-0002-C)*

Outcome: In March 2013, OIG referred the matter to management for administrative action. The referral indicated that the employee was arrested and charged by local law enforcement on more than one occasion for alcohol and/or drug related violations. Some of the charges are still being adjudicated by the respective court systems.

Select Other Investigative Matters

Several complaints resulted in referrals to GPO management for disposition.

- OIG received an anonymous complaint alleging an employee did not work an 8-hour day on a specific day as certified on his time and attendance sheet. *(Case No. 12-0040-C)*
- We reported previously that OIG received allegations several managers suspected that they had been retaliated against for whistleblowing. We referred the allegations to the Office of General Counsel for further assessment. Subsequently, the Office of General Counsel reported that the Director of Equal Employment Opportunity (EEO) informed him that the employees are pursuing EEO complaints and that they will be investigated fully by an independent contractor. Accordingly, since allegations receive a comprehensive review in the EEO process, the Director did not consider it necessary that his office pursue a parallel inquiry. After the conclusion of the EEO process, OIG will evaluate the results and determine if further action—either on the part of GPO or OIG—is warranted. *(Case No. 12-0009-I)*

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.

Report on FDsys Compliance with FISMA as it Relates to Continuous Monitoring

OIG initiated an audit to determine whether GPO was effectively using automation as it relates to continuous monitoring for FDsys and whether GPO has an effective vulnerability scanning process for its networks and databases including a corrective action process for correcting know vulnerabilities, and 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.

The audit determined that during the past year, GPO's Office of Information Technology and Systems and Programs Strategy and Technology division made marked efforts to continuously monitor FDsys, including proactively testing various components of this multi-platform system. As part of its ongoing monitoring program, GPO periodically performed network scanning, targeted FDsys scans and annually re-certified and re-accredited this application, consistent with NIST guidance.

Although vulnerability tests are periodically performed, additional work is still needed to ensure controls are in place and operating effectively. The FDsys application remains vulnerable to outsider/insider attacks primarily as a result of old security patches and fixes that were not applied at the date of this evaluation; certain security parameters were not set to optimize security of these servers and audit logging was not adequately configured or consistently monitored. *(Report on FDsys Compliance with FISMA as it Relates to Continuous Monitoring, Report No.13 -03, January 7, 2013)*

Recommendation: We recommended that the CIO identify, document, and implement patch management procedures for ensuring that vulnerabilities are patched timely, (2) review anti-virus configurations and ensure updates are occurring timely, (3) configure the minimum password length to match the enterprise standard for password length, (4) develop and implement a procedure to ensure log files are reviewed, (5) configure audit settings to equally log failed access attempts, (6) configure the logon process to contain the end user acceptance of acceptable use policy prior to granting access to the computer system; and (7) implement procedures to periodically assess baseline configurations to ensure security control compliance with agency standards.

Management agreed with the recommendations. Management described and outlined its plans to address the audit recommendations, implemented mitigating controls, and provided target dates for when the final actions would be completed.

ABBREVIATIONS AND ACRONYMS

AICPA	American Institute of Certified Public Accountants
CFR	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
COTS	Commercial-Off-The-Shelf
CP&B	Congressional Printing and Binding
EEO	Equal Employment Opportunity
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
GBIS	GPO Business Information System
GPO	Government Printing Office
GSS	General Support System
IG	Inspector General
IT	Information Technology
JCP	Joint Committee on Printing
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

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 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 5(a)(10)	Summary of Each Audit Report over Six Months Old for Which No Management Decision Has Been Made	33
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	38

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				
Final Report FY 2012 Management Advisory Comments - Information Technology, Report No. 13-11, March 28, 2013	6	0	0	0
Operational and Financial Management				
FY 2012 Independent's Auditor's Report on the US Government Printing Office's FY 2012 Consolidated Financial Statements, Report No. 13-09, February 28, 2013	11	0	0	$24,400,000 (financial accounting)
Management Advisory Comments Identified in an Audit of the Consoli-dated Financial Statement Audit for the Year Ended September 30, 2012 Report No. 13-10, March 20, 2013	3	0	0	$19,694 (financial accounting)
Print Procurement				
Audit of Computer Security: GPO's Risk Acceptance Process for Major and Legacy and Minor Applications, Report No. 13-05, January 14, 2013	5	0	0	0
Program and Operational Integrity				
GPO Faces Challenges With Current and Former Employee Indebtedness, Report No. 13-02 March 28, 2013	3	0	$245,104	0
Opportunities Exist to Reduce Costs Associated with Oracle Software Licensing, Report No. 13-06, March 15, 2013	3	0	$885,240	0
Management Oversight: Federal Employees' Compensation Act Operations, Report No. 13-01, January 15, 2013	3	0	$267,162	0
Stewardship over Official Publications				
Report on FDsys Compliance with FISMA as it Relates to Continuous Monitoring, Report No. 13-03, January 7, 2013	7	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 ($)
Nov. 16, 2011	Audit of Selected Aspects of GPO Time and Attendance and Payroll Administration	12-01	6	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 ($)
Jan. 11, 2010	GPO FISMA	10-03	9	0
Nov. 16, 2011	Audit of Selected Aspects of GPO Time and Attendance and Payroll Administration	12-01	6	$372,717
Dec. 16, 2011	Independent Auditor's Report – US GPO FY 2011	12-02	5	0
Feb 14, 2012	Final Report FY 2011 Management Advisory Comments	12-07	5	0
Mar. 1, 2012	Consolidated Financial Statement Audit GPO Business Information System (GBIS)	12-10	4	0
Mar. 1, 2012	Consolidated Financial Statement Audit General Support System (GSS)	12-11	4	0
Mar. 30, 2012	Maintaining Effective Control Over Employee Overtime	12-08	1	0

APPENDIX E

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

DESCRIPTION	NUMBER OF REPORTS	FUNDS PUT TO BETTER USE 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 - GPO Faces Challenges With Current and Former Employee Indebtedness, Report No. 13-02, March 27, 2013		$245,105
Audit Report – Management Oversight: Federal Employees' Compensation Act Operations, Report No. 13-01, January 15, 2013		$267,162
Audit Report – Opportunities Exist to Reduce Costs Associated with Oracle Software Licensing, Report No. 13-06, March 15, 2013		$885,240
		$24,400,000
Audit Report – FY 2012 Independent's Auditor's Report on the US Government Printing Office's FY 2012 Consolidated Financial Statements, Report No. 13-09, February 28, 2013		$19,694
Management Advisory Comments Identified in an Audit of the Consolidated Financial Statement Audit for the Year Ended September 30, 2012 Report No. 13-10, March 20, 2013		
Subtotals	5	$25,817,201
Reports for which 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		$25,817,201
Reports for which management decisions was made by end of reporting period	0	0
Report for which no management decision was made within 6 months of issuance	0	0

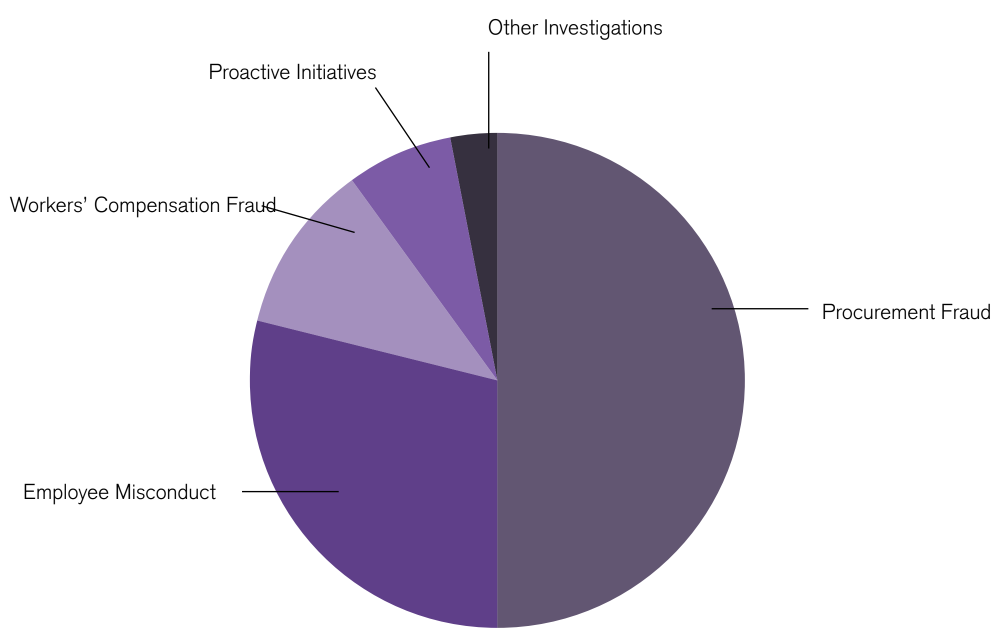
APPENDIX F

Investigations Case Summary

ITEM	QUANTITY
Total New Hotline/Other Allegations Received during Reporting Period	20
Preliminary Investigations (Complaints) Closed to the File	2
Complaint Referrals to Other Agencies	2
Complaint Referrals to OAI	0
Investigations Opened by OI during Reporting Period	1
Investigations Open at Beginning of Reporting Period	30
Investigations Closed during Reporting Period	3
Investigations Open at End of Reporting Period	28
Referrals to GPO Management (Complaints and Investigations)	4

CURRENT OPEN INVESTIGATIONS BY ALLEGATION	NUMBER	PERCENT
Procurement Fraud	14	50
Employee Misconduct	8	29
Workers Compensation Fraud (OWCP)	3	11
Proactive Initiatives	2	7
Other Investigations	1	3
Total	28	100

CURRENT OPEN INVESTIGATIONS BY ALLEGATION



APPENDIX G

Investigations Productivity Summary

ITEM	QUANTITY
Arrests	0
Total Presentations to Prosecuting Authorities	2
Criminal Acceptances	0
Criminal Declinations	2
Indictments	0
Convictions	0
Guilty Pleas/Deferred Prosecution Agreements	0
Probation (months)	0
Jail Time (days)	0
Civil Restitutions	0
Civil Acceptances	0
Civil Agreements	0
Civil Declinations	0
Amounts Recovered Through Investigative Efforts	$2,204
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	4
Contractor Debarments	6
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions	2
Proposed Employee Suspensions	0
Employee Terminations	0
Subpoenas	0

APPENDIX H

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 "non-compliant."

Peer Review of GPO-OIG Audit Function

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

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

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

Peer Review of GPO-OIG Investigative Function

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

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

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

Peer Reviews of other OIGs

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

P.O. Box 1790 Washington, DC 20013-1790

Email: gpoighotline@gpo.gov

Fax: 1.202.512.1030 | Hotline: 1.800.743.7574

OFFICIAL DIGITAL SECURE