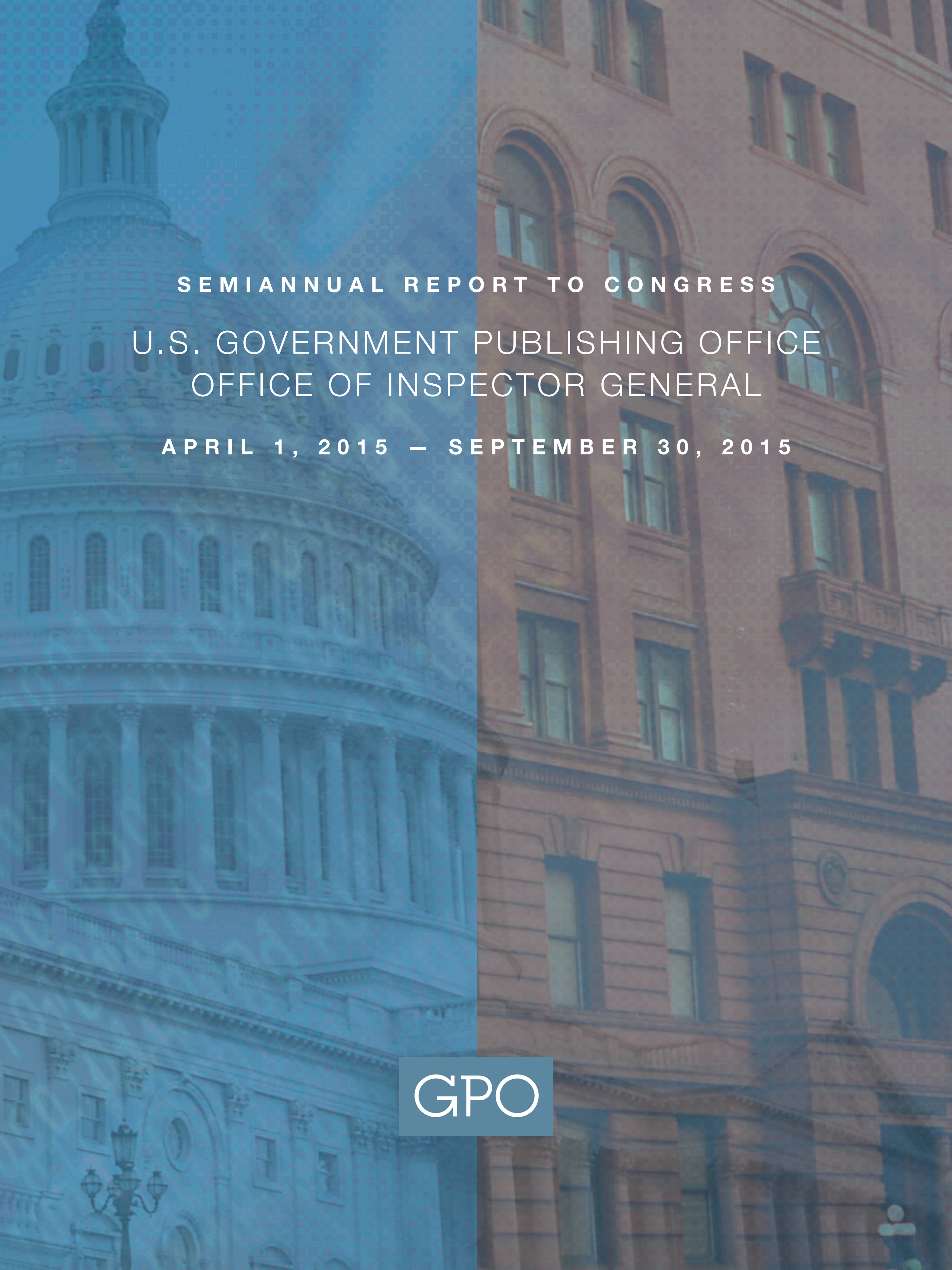

SEMIANNUAL REPORT TO CONGRESS

U.S. GOVERNMENT PUBLISHING OFFICE OFFICE OF INSPECTOR GENERAL

APRIL 1, 2015 — SEPTEMBER 30, 2015

GPO

GPO

U.S. GOVERNMENT PUBLISHING OFFICE
Keeping America Informed | OFFICIAL | DIGITAL | SECURE

ABOUT THE GOVERNMENT PUBLISHING OFFICE …

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

AND THE OFFICE OF INSPECTOR GENERAL …

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

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

ONLINE AVAILABILITY

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

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

A MESSAGE FROM THE INSPECTOR GENERAL

This Semiannual Report to Congress covers the 6-month period ending September 30, 2015, and summarizes the most significant accomplishments of the U.S. Government Publishing Office (GPO) Office of Inspector General (OIG).

Because of the sharp increase in data breaches reported by Federal agencies, our audit efforts focused on information technology (IT) and cybersecurity. Our investigative efforts yielded $21.8 million in funds put to better use and savings and referral of 16 businesses/individuals to GPO for suspension and/or debarment consideration.

Our audits and investigations continue to assess the effectiveness, efficiency, economy, and integrity of GPO's programs and operations. Our activities are described according to our strategic goals, as outlined in the OIG Strategic Plan for Fiscal Years (FYs) 2012 through 2016.

The accomplishments are the result of the dedicated work of OIG's professional staff and their commitment to ensuring the efficiency and effectiveness of GPO programs and operations. Our success is due, in large part, to not only the continued support received from GPO's Director and senior managers but also interested Committees and Members of the Congress.

MICHAEL A. RAPONI
Inspector General

CONTENTS

SELECTED STATISTICS

Investigations

Investigative cost-efficiencies, restitutions, fines, penalties, and funds put to better use	$21.8 million
Complaints opened	31
Complaints closed	33
Investigative cases opened	7
Investigative cases referred for prosecution	5
Investigative cases referred for administrative/civil action	3
Investigative cases closed	9
Suspension and/or debarment referrals	16
Suspensions	14
Debarments	11
Subpoenas issued	16
Referrals to GPO management	7

Audits and Inspections

Audits and other reports issued	9
Number of recommendations made	53

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 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. We believe GPO faces the following major challenges:

- **Keeping focus on its mission of information dissemination**
- **Addressing emerging workforce skills**
- **Improving the enterprise architecture and infrastructure to support enterprise-wide as well as GPO's Federal Digital System (FDsys) transformation**
- **Securing information technology (IT) systems and protecting related information assets**
- **Improving print procurement programs**
- **Managing workers' compensation programs**

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

Changes from Previous Reporting Period

When GPO attains significant progress toward resolving an issue identified as a management challenge, OIG removes the challenge. The following key criteria are considered in whether to remove a management challenge: (1) demonstrated strong leadership commitment to addressing the issue, (2) ability to address the problem, (3) plan for how corrective measures will be implemented, (4) program to monitor the corrective action, and (5) demonstrated progress in the implementation of the corrective measures.

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

Challenge 1: Keeping Focus on Its Mission of Information Dissemination

Overview: The transformation of GPO has been underway for several years. The trend of producing Government documents through electronic publishing technology and providing the public with Government documents through the Internet has affected all of the programs at GPO and reduced production, procurement, and sales of printed products. Those areas have historically provided GPO with a vital source of revenue.

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

GPO's Progress: Senior management continues its focus on advancing GPO's transformation. GPO continues to identify and develop technological innovations to support its transformation.

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 ePassports for the Department of State. As the next generation ePassport is developed, GPO facilities will need modification and upgrades put into place that will support installation of new ePassports 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 ePassports into the most secure identification credential.

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

GPO is exploring new ways for users to interact with FDsys content by providing mobile-optimized access to FDsys and enabling direct interfacing with it 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 is continuing its efforts to identify workforce skill gaps and core competencies.

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

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

Challenge: Existing EA and IT infrastructures need to be able to support the changes and increasing demands that GPO anticipates.

GPO's Progress: GPO is coordinating and collaborating across the organization as it continues to address elements of its enterprise architecture.

Challenge 4: Securing IT Systems and Protecting Related Information Assets

Overview: GPO systems contain vital information central to the GPO mission and 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 and IT developments—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.

During this reporting period, OIG completed several audits of GPO identifying vulnerabilities in IT infrastructure.

Challenge: 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 theft or other fraudulent use of information.

GPO Progress: GPO continues its efforts to strengthen incident response capabilities and threat detection. GPO is also continuing to involve the entire organization as it addresses security of information assets.

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. 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. Other exceptions to printing are the categories of work included in the note to Title 44 and work GPO is not able or equipped to do.

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

GPO's Progress: GPO continues its outreach efforts to Executive Office agencies in an effort to inform them of available publication services as well as offer economical printing prices. GPO also continues efforts to maintain the integrity of the FDLP.

Challenge 6: Managing Workers' Compensation Programs

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

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

Challenge: 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.

GPO's Progress: GPO reported it has achieved a lower accident rate than the related industry accident rate as it continues to work toward strengthening safety programs and its FECA Program case management practices.

TRANSFORMING GPO INTO A DIGITAL PLATFORM

OIG Strategic Goal 1:

GPO is increasingly dependent on IT to efficiently and effectively deliver its programs and provide meaningful and reliable financial reporting. As a result, OIG will 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.

Evaluation of Selected Information Technology and Cybersecurity Areas

At the request of the U.S. House of Representatives, Committee on House Administration, OIG conducted an assessment on the state of GPO's cybersecurity posture based on security measures identified by the U.S. House of Representatives, Committee on House Administration. OIG evaluated GPO's documented IT cybersecurity policies, procedures, and practices. We evaluated GPO's major systems and applications for compliance with GPO's key policies such as certification and accreditation, risk assessments, current and target security postures, and contingency planning and testing.

We found that while GPO has taken or planned to take steps for protecting data processed and maintained by the complex set of systems and interconnections that support its mission, GPO needs more comprehensive data collection and analysis to better assess its overall security posture. Without that, describing the target state for cybersecurity that is necessary to identify and prioritize opportunities for improvement and assess progress will be challenging.

Recommendations: OIG made two recommendations for improving GPO's overall cybersecurity posture by incorporating the use of cybersecurity intelligence data into its security program and ensuring that personnel complied with IT security policies. Management agreed with our recommendations and has planned necessary corrective actions. (*Information Security: Evaluation of Selected Information Technology and Cybersecurity Areas, Report No. 15-17, August 7, 2015*)

Information Security: Penetration Testing of GPO's Citrix Remote Access System

Security testing to mimic a real-world attack was performed in an attempt to identify ways of circumventing the security features of GPO's Citrix Remote Access System. The audit disclosed GPO continuously monitors Citrix Remote Access application, proactively upgrades, and tests the system. The audit also disclosed opportunities for strengthening select access and configuration management controls.

Recommendations: OIG made eight recommendations. Management agreed and has implemented or planned necessary corrective actions. (*Information Security: Penetration Testing of GPO's Citrix Remote Access System, Report No. 15-13, August 10, 2015*)

Federal Public Key Infrastructure Compliance Report and WebTrust for Certification Authority

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

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

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

E&Y's opinion for the period July 1, 2014, through June 30, 2015, was that the GPO Principal Certification Authority Certificate Practices Statement conformed in all material respects to GPO-CA and the Federal PKI common policies, and GPO fairly stated management's assertion in all material respects based on the American Institute of Certified Public Accountants/ Canadian Institute of Chartered Accountants Trust Services Criteria for Certification Authorities.

Recommendations: The reports did not contain any recommendations. (*Federal PKI Compliance Report, Report No. 15-20, September 24, 2015, and WebTrust for Certification Authority, Report No. 15-21, September 24, 2015*)

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.

Budget Formulation for Select Congressional Products

At the request of the U.S. House of Representatives, Committee on House Administration, OIG examined GPO's budget practices for Bills, Resolutions, Amendments; Miscellaneous Publications; and Miscellaneous Publishing and Services.

We found that GPO established a framework for estimating costs for publishing congressional products. GPO estimates the volume, size, and mix of legislative materials. GPO also uses actual costs from prior years, and other trend information plus an estimate of near-term congressional publishing requirements.

While a framework exists, OIG noted some areas where the framework (a manual process) could be strengthened to reduce the risk of making budget estimate errors. In addition, we identified a variance in page counts reported through GPO Business Information System (GBIS) compared to page counts reported in the Budget Justification for Bills, Resolutions, and Amendments. For FY 2013, the difference was 63,770 (33 percent), and for FY 2014 the difference was 5,396 (6 percent). Officials stated the variation in counts could be attributed to a greater number of published blank page counts in hard copy form (reported through GBIS) than blank pages in documents posted on FDsys. Officials also stated that from FY 2009 through FY 2013 GPO incorrectly included page counts in rider documents as original page counts with Bills, Resolutions, and Amendments. We further noted that GPO transfers funds based on accumulated actual costs and not by way of a page-billing rate for Bills, Resolutions, and Amendments. We did not identify any instance where GPO transferred funds other than incurred costs from the Congressional Publishing Appropriation for Bills, Resolutions, and Amendments.

Recommendations: OIG recommended that the Chief Financial Officer review and if necessary revise applicable Standard Operation Procedures and the Budget Justification process to better reflect current activities performed, including the clarification of references to page rates, page counts, the calculation of actual costs, and if feasible automate the manual process used for page counts. Management agreed with the recommendation and has planned the necessary corrective actions. (*Budget Formulation for Select Congressional Products, Report No. 15-19, September 25, 2015*)

PRINT PROCUREMENT PROGRAMS

OIG Strategic Goal 3:

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

Information Security: Penetration Testing of GPO's Contractor Connection Web Application

Cybersecurity testing of GPO's Contractor Connection Web Application disclosed risks. While OIG found no exploitable instances, the application was vulnerable to outsider and insider attacks. We reported GPO could strengthen access and configuration management controls.

Recommendations: OIG made 18 recommendations to strengthen vulnerabilities of GPO's Contractor Connection Web Application. Management agreed with our recommendations and has either implemented or planned the necessary corrective actions. (*Information Security: Penetration Testing of GPO's Contractor Connection Web Application, Report No. 15-12, August 4, 2015*)

Medicare & You 2015 Handbook Contract Requirements Were Not Always Clear

OIG found contract requirements to produce the Medicare & You 2015 handbook on behalf of the U.S. Department of Health and Human Services were not always clear. Our investigation revealed that while contracting documents stated that all paper furnished must be in accordance with Congressional JCP paper specifications, the same contract documents named three of four text paper stock products on the Qualified Products List that did not meet all JCP specifications. Deviations included noncompliance with coating, caliper, gloss, and smoothness specifications. Our investigation also disclosed contractors opted to use paper stock products named on the Qualified Products List.

Applying acceptance criteria referenced in contract documents resulted in a determination that the products were critically defective and subject to outright rejection.

OIG reported that ensuring paper specifications are clearly defined could have a favorable effect on GPO's ability to recover costs and/or take appropriate disciplinary action where vendors did not comply with contract requirements. As a result, approximately $21.1 million worth of funds could have been put to better use. Also, based on investigative results, GPO assessed contract discounts totaling approximately $350,000. (*Case No. 14-0022-I*)

California Company Committed Bankruptcy Fraud

An OIG investigation revealed the company violated GPO Contract Terms and the GPO Printing Procurement Regulation when it failed to notify GPO of its Chapter 13 bankruptcy. Our investigation also revealed the company's owners/operators made false statements to the U.S. Bankruptcy Court by omitting company assets and income during its bankruptcy proceedings. Furthermore, the investigation disclosed the company submitted an inaccurate officer/owner name on its initial registration application to GPO.

OIG recommended GPO suspend and/or debar the company, its owners/ operators, and an affiliated company. (*Case No. 14-0008-I*)

Two Illinois Companies Engaged in Collusive Behavior

OIG recommended suspension and/or debarment of two Illinois companies and its officers after an OIG investigation disclosed that the companies were collocated, the presidents of the two companies were married, and that appropriate safeguards were not established to demonstrate bid prices were arrived at independently.

OIG determined the companies bid on the same GPO contract opportunities 19 times since October 2012, of which 3 were for the same amount. In addition, the investigation found that: (1) one of the companies knowingly submitted misleading information when it withheld its affiliation with the second company on its initial application to do business with GPO, (2) one of the companies masked its association with the other by submitting bids using the company president's first name only and dropping the use of the shared surname, and (3) one company double billed GPO for work, causing GPO to mistakenly overpay the company $11,017. As of the date of our investigation, the company has failed to repay $2,303 of its debt to GPO, despite several attempts from the Agency to recoup the monies owed. (*Case No. 14-0025-I*)

Personally Identifiable Information Not Safeguarded

An OIG investigation disclosed a company violated contract requirements when it altered documents to conceal unauthorized employees engaged in the production of sensitive documents containing Government beneficiary personally identifiable information (PII). The company also violated contract requirements when it did not adequately protect PII from loss, theft, and/or inadvertent disclosure. The failure of the company and its representatives to adhere to the contract requirements affected two GPO contracts valued at more than $3 million.

OIG recommended GPO suspend and/or debar a Pennsylvania company and several of its representatives. (*Case No. 15-0007-I*)

Georgia Company Violated GPO Contract

An OIG investigation revealed a company violated contract requirements when it altered and submitted a false shipping document and subcontracted the predominant production function on two contracts without proper authorization. Additionally, the owner/operator never advised GPO that the company was experiencing major financial difficulties leading it to liquidate its production equipment, thereby making it solely dependent upon subcontracting the predominant production function to complete future GPO contracts. The company had been doing business with GPO since October 2014, completed 14 GPO-awarded contracts totaling more than $80,000, and routinely delivered late.

OIG recommended GPO suspend and/or debar a Georgia company, its owner/operator, and an affiliated company. (*Case No. 15-0015-I*)

PROGRAM AND OPERATIONAL INTEGRITY

Strategic Goal 4:

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

Employee Misappropriated GPO Property for Personal Use

OIG referred investigative findings to GPO for possible corrective action specifying that an employee misappropriated GPO property (scrap metal and other supplies) and removed it from GPO premises for personal use. The employee acknowledged the misappropriation and returned the property to GPO during the OIG investigation. The investigation also revealed that colleagues of the employee, as well as the employee's supervisor, were aware of the misappropriation, but failed to stop or report it. Finally, the findings detailed that the supervisor lacked candor with OIG during the investigation by repeatedly denying knowledge of the misappropriation despite evidence to the contrary. (*Case No. 15-0013-I*)

Threatened Workplace Violence

OIG referred investigative findings to GPO for possible corrective action detailing a threat to harm another employee as a result of a workplace-related issue. The case is pending trial. (*Case No. 15-0019-I*)

Other Investigative Matters

- In June 2015, following a March 2015 Plea Agreement, a U.S. District Judge in the Eastern District of North Carolina found a former GPO employee guilty on one count of violating section 1920, title 18, of the United States Code, *False Statements to Obtain Federal Employees' Compensation*, and sentenced him to 2 years of probation and pay restitution to the Department of Labor in the amount of $139,458.12. In addition, the Department of Labor terminated the former employee's workers' compensation coverage—an estimated cost savings of $381,377. The outcomes resulted from a joint GPO OIG and Department of Labor OIG investigation that disclosed the former employee fraudulently claimed travel expenses associated with his workers' compensation benefits for doctor visits not made. (*Case No. 11-0014-I*)

STEWARDSHIP OVER OFFICIAL PUBLICATIONS

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.

Information Security: Penetration Testing of GPO's Ben's Guide Web Application

Security testing of GPO's Ben's Guide Web Application identified vulnerabilities to outsider and insider attacks. We reported that GPO could strengthen access and configuration management controls. We also reported security controls and web server configuration management controls could be strengthened.

Recommendations: OIG made nine recommendations to strengthen vulnerabilities. Management agreed with our recommendations and has either implemented or planned the necessary corrective actions. (*Information Security: Penetration Testing of GPO's Ben's Guide Web Application, Report No. 15-14, July 29, 2015*)

Information Security: Penetration Testing of GPO's Federal Depository Library Program (FDLP.Gov) Web Application

Security testing revealed risks were not always mitigated to minimize the success of an outsider and insider attack of GPO's Federal Depository Library Program (FDLP.Gov) Web Application. We reported deficiencies in the area of access and configuration management controls.

Recommendations: OIG made nine recommendations to strengthen vulnerabilities of GPO's FDLP.Gov Web Application. Management agreed with our recommendations and has either implemented or planned the necessary corrective actions. (*Information Security: Penetration Testing of GPO's FDLP.Gov Web Application, Report No. 15-15, July 29, 2015*)

Information Security: Penetration Testing of GPO's Online Bookstore

The audit identified instances where the application was vulnerable to outsider and insider attacks.

Recommendations: OIG made six recommendations to strengthen identified vulnerabilities of GPO's Online Bookstore. Management agreed with our recommendations and has either implemented or planned the necessary corrective actions. (*Information Security: Penetration Testing of GPO's Online Bookstore, Report No. 15-16, July 29, 2015*)

ABBREVIATIONS AND ACRONYMS

CA	Certification Authority
EA	Enterprise Architecture
E&Y	Ernst & Young LLP
FBCA	Federal Bridge Certificate Authority
FDLP	Federal Depository Library Program
FDsys	Federal Digital System
FISMA	Federal Information Security Management Act
GBIS	GPO Business Information System
GPO	Government Publishing Office
IG	Inspector General
IT	Information Technology
JCP	Joint Committee on Printing
OIG	Office of Inspector General
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PPPS	Passport Printing and Production System

GLOSSARY OF TERMS

Finding
Statement of problem identified during an audit or inspection typically having a condition, cause, and effect.

Follow-Up
The process that ensures prompt and responsive action once resolution is reached on an IG recommendation.

Funds Put To Better Use
An IG recommendation that funds could be used more efficiently if management took actions to implement and complete the audit or inspection recommendation.

Management Decision
An agreement between the IG and management on the actions taken or to be taken to resolve a recommendation. The agreement may include an agreed-upon dollar amount affecting the recommendation and an estimated completion date, unless all corrective action is completed by the time agreement is reached.

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

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

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

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

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

Unsupported Costs
Questioned costs not supported by adequate documentation.

APPENDIX A

Index of Reporting Requirements under the IG Act of 1978

Reporting	Requirement	Page
Section 4(a)(2)	Review of Legislation and Regulation	None
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	All
Section 5(a)(2)	Recommendations with Respect to Significant Problems, Abuses, and Deficiencies	All
Section 5(a)(3)	Prior Significant Recommendations on Which Corrective Action Has Not Been Completed	20
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	23
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	7-14
Section 5(a)(7)	Summary of Significant Reports	All
Section 5(a)(8)	Statistical Tables on Management Decisions on Questioned Costs	21
Section 5(a)(9)	Statistical Tables on Management Decisions on Recommendations That Funds Be Put to Better Use	21
Section 5(a)(10)	Summary of Each Audit Report over Six Months Old for Which No Management Decision Has Been Made	19
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
Section 3(d)	Peer Review	24

APPENDIX B

Final Reports Issued and Grouped by OIG Strategic Goal

Report Name	Number of Recommendations	Questioned Costs ($)	Funds Put To Better Use ($)	Other Monetary Impact ($)
Transforming GPO into a Digital Platform				
Information Security: Penetration Testing of GPO's Citrix Remote Access System	8			
Evaluation of Selected Information Technology and Cybersecurity Areas	2			
Federal PKI Compliance Report	0			
WebTrust for Certification Authority	0			
Operational and Financial Management				
Budget Formulation for Select Congressional Products	1			
Print Procurement				
Information Security: Penetration Testing of GPO's Contractor Connection Web Application	18			
Program and Operational Integrity				
Stewardship over Official Publications				
Information Security: Penetration Testing of GPO's Ben's Guide Web Application	9			
Information Security: Penetration Testing of GPO's FDLP Government Web Application.	9			
Information Security: Penetration Testing of GPO's Online Bookstore	6			

APPENDIX C

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

Date Issued	Name of Audit	Report Number	Number of Recommendations	Costs ($)
None				

APPENDIX D

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

Date Issued	Name of Audit	Report Number	Number of Recommendations	Monetary Impact ($)
Nov. 16, 2011	Final Report on Audit of Selected Aspects of GPO Time and Attendance and Payroll Administration	12-01	1	$ 372,717
Sep. 21, 2012	Independent Audit of Harris Corporation	12-24	1	$ 1,178,814
Sep. 28, 2012	Audit of Controls over GPO's Fleet Credit Card Program	12-18	1	$ 4,751
Mar. 29, 2013	Opportunities Exist to Reduce Costs Associated with Oracle Software Licensing	13-06	1	$ 885,240
Sep. 18, 2013	PPPS Compliance With FISMA as it Relates to Continuous Monitoring	13-17	1	
Nov. 29, 2013	Commercial Printing and Dissemination of Government Information at the National Institutes of Health	14-02	1	$ 1,077,000
Mar. 24, 2014	Changes Can Provide GPO Better Information on Establishing Billing Rates for Congressional Hearings (Product Code 83)	14-07	2	$ 4,030,600
Mar. 25, 2014	Information Technology Professional Services—Oracle Software	14-08	1	$ 2,760,000
Mar. 27, 2014	Information Technology Microsoft Software Licenses	14-10	2	$ 250,000
Aug. 1, 2014	Acquisition of US Passport Covers	14-14	2	$15,700,000
Sep. 23, 2014	Prompt Payment of Invoices on Hold	14-21	1	$ 45,572
Sep. 26, 2014	IT Professional Services ILS	14-16	2	$ 1,100,000
Sep. 29, 2014	Accountability of Blank Passports	14-18	2	

APPENDIX E

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

Description	Number of Reports	Funds Put to Better Use, Questioned Costs, and Other Monetary Impact ($)
Reports for which no management decisions were made by beginning of reporting period	0	0
Reports issued during reporting period: none	0	0
Subtotals	0	0
Reports for which a management decision was made during reporting period	0	0
1. Dollar value of recommendations not agreed to by management		
2. Dollar value of recommendations agreed to by management		
Reports for which no management decision was made by end of reporting period	0	0
Reports for which no management decision was made within 6 months of issuance	0	0

APPENDIX F

Investigations Case Summary

Item	Quantity
Total New Hotline/Other Allegations Received during Reporting Period	31
Preliminary Investigations (Complaints) Closed	33
Complaint Referrals to Other Agencies	3
Complaint Referrals to Office of Audits and Inspections	1
Investigations Opened by Office of Investigations during Reporting Period	7
Investigations Open at Beginning of Reporting Period	46
Investigations Closed during Reporting Period	9
Investigations Open at End of Reporting Period	44
Referrals to GPO Management (Complaints and Investigations for corrective action or information purposes)	7

Current Open Investigations	Number	Percent
Procurement/Contract Fraud	24	54.5
Employee Misconduct	9	20.5
Workers' Compensation Fraud	1	2.3
Information Technology/Computer Crimes	3	6.8
Proactive Initiatives	6	13.6
Other Investigations	1	2.3
Total	**44**	**100.0**

APPENDIX G

Investigations Productivity Summary

Item	Quantity
Investigative cost-efficiencies, restitutions, recoveries, fines, and penalties, Funds Put to Better Use	$21.8 million
Arrests	1
Presentations to Prosecuting Authorities	5
Criminal Acceptances	2
Criminal Declinations	1
Indictments/Information/Complaints	1
Convictions	1
Guilty Pleas/Deferred Prosecution Agreements	0
Probation (months)	24
Jail Time (days)	0
Criminal Fines, Fees, Recovery, and/or Restitution	$ 0
Presentations for Civil Action	0
Civil Acceptances	0
Civil Declinations	0
Civil Settlements	0
Civil Fines, Fees, Recovery, and/or Restitution	$ 0
Referrals to GPO Management for Possible Corrective Action and/or Information Purposes	4
Employee Corrective Action	1
Agency/Process Corrective Action	1
Business/Individual Referrals to GPO Suspending and Debarring Official (SDO) for Suspension and/or Debarment	16
Suspensions	14
Debarment	11
Other SDO Response/Action	13

APPENDIX H

Peer Review Reporting

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

Peer Review of GPO-OIG Audit Function

The Nuclear Regulatory Commission OIG reviewed the system of quality control for the audit organization of the GPO OIG, in effect for the year ended September 30, 2013, and issued a final report on May 2, 2014. GPO OIG received a peer review rating of pass with deficiencies.

After addressing the deficiencies, GPO OIG entered into a memorandum of understanding with the Library of Congress OIG to conduct a review of the system of quality control for the audit organization of the GPO OIG.

In September 2015, the Library of Congress OIG provided a draft letter stating nothing came to their attention that would indicate that GPO OIG would not receive a rating of pass in its upcoming peer review. We are awaiting the final report to be finalized in FY 2016.

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 OIG received a rating of compliant.

A copy of both peer review reports can be viewed
at **www.gpo.gov/oig/au-intro.htm**

Report Fraud, Waste, and Abuse

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

GPO

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

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

gpoighotline@gpo.gov

fx: **1.202. 512.1030** | Hotline: **1. 800.743.7574**