SEMIANNUAL REPORT TO
CONGRESS

April 1, 2017 – September 30, 2017

GPO

U.S. GOVERNMENT PUBLISHING OFFICE

Office of Inspector General

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

The GPO Inspector General Act of 1988, title II of Public Law 100-504 (October 18, 1988) establishes the responsibilities and duties. OIG, located in Washington, D.C., has 22 employees and is organized into 3 line elements—the Office of Investigations, the Office of Information Technology Audits 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 any problems or deficiencies relating to administering and operating GPO.

Online Availability

This report is available on our Web site: https://www.gpo.gov/oig/

Message from the INSPECTOR GENERAL
U.S. GOVERNMENT PRINTING OFFICE

In this Semiannual Report to Congress for the period ending September 30, 2017, OIG issued 21 reports. We made 59 program improvement recommendations and referred 11 businesses and individuals for suspension and/or debarment to GPO for consideration. OIG audits, reviews, investigations, and other reviews identified more than $1.7 million in funds put to better use and other monetary impact.

OIG continues to place emphasis on Information Technology (IT) and cybersecurity. For this period, 16 of our reports relate to technology issues.

I look forward to working with all stakeholders as we address the challenges ahead. With the support of GPO management and Congress, OIG will continue to play a key oversight role in maintaining the integrity and accountability.

Michael A. Raponi
Inspector General

TABLE OF CONTENTS

SELECTED STATISTICS

Investigations

Investigative cost efficiencies, restitutions, fines, penalties,
and funds put to better use $942,247

Complaints opened 13

Complaints closed...13

Investigative cases opened 10

Investigative cases referred for prosecution.. 3

Investigative cases referred for administrative/civil action 2

Investigative cases closed 7

Suspension and/or debarment referrals..11
.
Subpoenas issued.. 2

Referrals to GPO management...1

Audits, Inspections and Information Technology

Audits and other reports issued 18

Questioned costs, funds put to better use, and other monetary impact $760,081

Number of recommendations made 59

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 challenges:

- Keeping focus on its mission of information dissemination

- Improving the Enterprise Architecture (EA) and infrastructure to support enterprise-wide as well as GPO's FDsys transformation

- Securing Information Technology (IT) systems and protecting related information assets

- Improving Print Procurement Programs

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

We believe GPO has met the criteria for removing the management challenge associated with developing effective strategies for addressing emerging issues related to potential labor and skills shortages as GPO continues its transformation to a digital-based platform. OIG will monitor GPO's actions and progress toward addressing the challenge.

MANAGEMENT CHALLENGES (Continued)

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.

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 by identifying and developing technological innovations that support its mission.

Challenge 2: 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 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, chapter 36, title 44 of the United States Code defines EA 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.

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

GPO's Progress: GPO continues to address its defined EA and IT infrastructure framework.

Challenge 3: Securing Information Technology 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.

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 to identify and address risks to cyber assets, information, and efforts for resolving identified deficiencies.

Challenge 4: 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 FDLP as well as preventing potential higher printing cost as a result of inefficient printing by Executive Office agencies.

GPO's Progress: GPO continues to address contract specifications and publishing needs.

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 Cybersecurity Controls of Web Application Hosted Service

Penetration testing of select web application hosted services was conducted to find vulnerabilities that an attacker could exploit. Testing disclosed opportunities for strengthening controls for the following 11 web applications:

- Web-hosted service—www.usgovernmentmanual.gov
- Web-hosted service—publications.usa.gov
- Web-hosted service—www.memberguide.gpo.gov
- Web-hosted service—cah.gpo.gov
- Web-hosted service—www.fedreg.gov
- Web-hosted service—www.federalregister.gov
- Web-hosted service—www.uscc.gov
- Web-hosted service—www.riddick.gpo.gov
- Web-hosted service—conferencereport.gpo.gov
- Web-hosted service—www.ofr.gov
- Web-hosted service—www.ecfr.gov

Recommendations: OIG made 31 recommendations for strengthening cybersecurity controls with the 11 web applications. Management implemented or has plans for the necessary corrective actions for addressing the vulnerabilities. *(Information Security: Penetration Testing of GPO's Web-Hosted Service—www.usgovernmentmanual. gov, Report No. 17-14, August 18, 2017), (Information Security: Penetration Testing of GPO's Web Hosted Service—publications.usa.gov, Report No. 17-15, August 18, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—www. memberguide.gpo.gov, Report No. 17-16, August 18, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—cah.gpo.gov, Report No. 17-17, August 18, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—www.fedreg.gov, Report No. 17-18, September 7, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—www.federalregister.gov,*

Transforming GPO Into A Digital Platform (Continued)

Report No. 17-19, September 7, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—www.uscc.gov, Report No. 17-20, August 30, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—www.riddick.gpo.gov, Report No. 17-21, August 30, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—conferencereport.gpo.gov, Report No. 17-22, September 7, 2017; Information Security: Penetration Testing of GPO's Web-Hosted Service—www.ofr.gov, Report No. 17-23, September 7, 2017; and Information Security: Penetration Testing of GPO's Web-Hosted Service—www.ecfr.gov, Report No. 17-24, August 30, 2017.

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. GPO's PKI is cross-certified with the Federal Bridge Certificate Authority. This requires that GPO PKI undergo an annual independent compliance assessment. The assessment determined that GPO's Principal CA 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.

Recommendations: The reports did not contain any recommendations. (Federal PKI Compliance Report, Report No. 17-27, September 15, 2017, and WebTrust for Certification Authority, Report No. 17-28, September 15, 2017).

OPERATIONAL AND FINANCIAL MANAGEMENT

OIG Strategic Goal 2:

Promote economy, efficiency, and effectiveness in GPO operations by helping 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.

Unscheduled and Unpaid Absenteeism: Security and Intelligent Documents

OIG conducted a review to identify irregular patterns of unscheduled and unpaid absenteeism within GPO's Security and Intelligent Documents (SID) business unit. Our work revealed that nearly 19 percent (33 of 175) of SID employees incurred an unpaid absence such as leave without pay (LWOP), absent without leave (AWOL), or both. The audit revealed that GPO did not always maintain effective controls over the absence due to a lack of documentation supporting leave requests, missing medical and Family and Medical Leave Act forms, and not following procedures for validating and certifying employee timesheets. Also, disciplinary actions were not taken for some employees for which AWOL was recorded in the GPO payroll system. Additionally, in several instances monetary on the spot awards were given to employees who had been identified as AWOL during the previous 12 month period. The total compensation paid to the employees in question for 2016 was $760,081 including $123,922 over their base salary.

Recommendations: We recommended that GPO: (1) reiterate to approving officials within SID the requirements for approving leave without pay, disciplining instances of AWOL, providing incentive awards, and approving time and attendance, (2) review the 2016 time and attendance records for employees identified in the report and correct any errors associated with the approval of LWOP, and (3) monitor time and attendance records to ensure LWOP is adequately supported and employees with recorded AWOL are disciplined in accordance with GPO policy, and the actions taken documented. *(Unscheduled and Unpaid Absenteeism: Security and Intelligent Documents, Report Number 17-13, August 18, 2017).*

PRINT PROCUREMENT PROGRAMS

OIG Strategic Goal 3:

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

Suspension/Debarment Referral–California-Based Print Procurement Contractor Violated Buy American Act

A California-based contractor violated the Buy American Act and GPO Contract Terms when it provided foreign-manufactured goods in fulfillment of GPO contracts. Shipping documents, for our period of review, provided in the contractor's invoice submissions disclosed 23 contracts (or jackets) referenced China, Hong Kong, as the place of origin and in one instance, Canada.

Our investigation revealed that 13 of the 23 foreign sourced contracts were within the 12-percent margin established by the Buy American Act and GPO Contract Terms. Therefore, considered unreasonable. The Buy American Act and GPO Contract Terms state that if the domestic offer is from a small business, the domestic price is considered unreasonable if it exceeds the foreign offer by more than 12 percent. For the 13 contracts, the contractor was paid $310,852.

We also noted the contractor failed to disclose the country of origin for the products during the bidding process nor was it issued a waiver to the Buy American Act, as required by GPO Contract Terms. Between January 1, 2011, and March 14, 2017, GPO awarded the contractor 213 contracts and paid the contractor more than $2.6 million. OIG referred three parties to the GPO Suspending and Debarring Official for disposition (Case Number 16-0019-I).

PRINT PROCUREMENT PROGRAMS (Continued)

Suspension/Debarment Referral–New York-Based Print Procurement Contractor Violated Buy American Act

Three New York-based companies operating as affiliates violated the Buy American Act for seven contracts. The contractor was paid $631,395. The three companies shared key personnel and operated as one entity. The Buy American Act, with several exceptions, generally requires that Federal agencies give preference in procurements to domestically produced end products over foreign end products. aGPO incorporates these requirements into its contracts. Our investigation identified seven contracts that were foreign sourced and their respective bids were within the 12-percent margin established by the Buy American Act and GPO Contract Terms. The Contractors also failed to disclose the country of origin for the products during the bidding process nor were they issued waivers to the Buy American Act, as required by GPO Contract Terms. OIG referred eight parties to the GPO Suspending and Debarring Official for disposition *(Case Number 14-0020-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.

Secure Credentials: Accountability Over Select Card Stock

OIG received information regarding missing blank card stock used to produce Department of State identification documents it issues to foreign government personnel. OIG conducted a review to determine the steps GPO took to safeguard against the loss and/or unauthorized use of select card stock.

OIG reported that key business processes were not always followed for ensuring accountability of card stock. For example: 1) GPO did not always have written procedures in place to account for and monitor the receipt, progress, and delivery of card stock inventory between SID and Central Receiving in Plant Operations and the Quality Control and Inventory Management Branches, and 2) when Standard Operating Procedures had been developed and approved, the procedures were not always followed.

We reported that the lack of effective accountability may leave GPO at an increased risk that individuals who intend to cause harm can possibly personalize the blank card stock and exploit it for the purpose of identity fraud. In some cases, when the select stock card stock reviewed is personalized, the bearer of the identification card is entitled to full criminal immunity and may not be arrested or detained by law enforcement.

Recommendation: We recommended that GPO: (1) review existing procedures and requirements, specifying if necessary products requiring chain of custody documentation to track and control a transfer, analysis, and disposition of physical or electronic security and intelligent documents, and (2) strengthen monitoring of procedures that will ensure chain of custody protocols are followed. (Secure Credentials: *Accountability over Select Card Stock, Report Number 17-12, July 24, 2017)*.

PROGRAM AND OPERATIONAL INTEGRITY (Continued)

GPO Employee Placed Two Issues of a Magazine the Islamic State of Iraq and the Levant (ISIL) Uses for Propaganda and Recruitment on GPO Premises

OIG identified 679 items on a GPO employee's work computer pertaining to a wide range of topics from terrorism, Middle East politics, Russian politics, and events related to North Korea. Of the 679 items, OIG identified 15 issues and/or volumes of the Rumiyah and/or Dabiq magazines. Rumiyah is known as an online magazine ISIL uses for propaganda and recruitment; Rumiyah is the successor to Dabiq, which ceased publication when the Syrian town of the same name was captured by prowestern forces. The employee downloaded and printed material sympathetic to the Islamic State on his GPO computer and placed two issues of Rumiyah in a common area frequented by other employees.

The employee's actions were violations of GPO's internet and email policy, which specifically prohibits employees from accessing and downloading information related to terrorist activities and engaging in conduct that creates a hostile working environment. In part, the matter was referred to GPO management for disposition (Case number 17-0013-I).

Information Security: Penetration Testing of GPO's PROBE System

Penetration testing was conducted on GPO's PROBE System. The PROBE system is the core labor tracking system that operates 24 hours a day, 7 days a week, and captures time and attendance data for the majority of employees located at the Central facility.

Recommendation: We made 18 recommendations for strengthening vulnerabilities of the PROBE System. (Information Security: *Penetration Testing of GPO's PROBE System, Report No. 17-11, July 24, 2017).*

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.

Information Security: Penetration Testing of GPO's Next Generation Federal Digital System

Penetration testing was conducted of GPO's Next Generation FDsys to simulate an attack on the computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.

Recommendations: We made three recommendations for strengthening identified vulnerabilities of GPO's Next Generation Federal Digital System. *(Information Security: Penetration Testing of GPO's Next Generation Federal Digital System, Report No. 17-25, September 7, 2017)*

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

Penetration testing of the GPO's Ben's Guide Web Application to identify vulnerabilities that an attacker could exploit. Testing disclosed opportunities existed for strengthening technical controls.

Recommendations: OIG made two recommendations for strengthening cybersecurity controls with the systems. Management has implemented or planned necessary corrective actions for addressing strengthening the controls. (Information Security: Penetration Testing of GPO's Ben's Guide Web Application, Report No. 17-10, July 24, 2017)

ABBREVIATIONS AND ACRONYMS

AWOL   Absent Without Leave

CA   Certification Authority

EA   Enterprise Architecture

FDLP   Federal Depository Library Program

FDsys   Federal Digital System

GPO   Government Publishing Office

IG   Inspector General

ISIL   Islamic State of Iraq and the Levant

IT   Information Technology

JCP   Joint Committee on Printing

LWOP   Leave Without Pay

OIG   Office of Inspector General

PKI   Public Key Infrastructure

SID   Security and Intelligent Documents

GLOSSARY OF TERMS

Criminal Complaint

A formal charging document that sets out the facts and cause of action (establishing probable cause) that the Government alleges are sufficient to support a claim against the charged party (the defendant).

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 Inspector General (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.

Indictment

The written formal charge of a crime by the grand jury, returned when 12 or more grand jurors vote in favor of it.

Information

The written formal charge of crime by the United States Attorney, file against an accused who, if charged with a serious crime, must have knowingly waived the requirements that the evidence first be presented to a grand jury.

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.

GLOSSARY OF TERMS (Continued)

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	21
Section 5(a)(4)	Matters Referred to Prosecutive Authorities	25
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	5-12
Section 5(a)(7)	Summary of Significant Reports	All
Section 5(a)(8)	Statistical Tables on Management Decisions on Questioned Costs	22
Section 5(a)(9)	Statistical Tables on Management Decisions on Recommendations That Funds Be Put to Better Use	22

APPENDIX A (Continued)

REPORTING	REQUIREMENT	PAGE
Section 5(a)(10)	Summary of Each Audit Report over 6 Months Old for Which No Management Decision Has Been Made	20
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 5(a)(17)	Statistical Tables on Investigative Reports Issued; Persons Referred to Department of Justice, State, and Local Prosecuting Authorities for Criminal Prosecution; and Indictments and Criminal Informations	23
Section 5(a)(18)	A Description of Metrics Used for Developing the Data for the Statistical Tables under Paragraph (17)	23
Section 5(a)(19)	Investigations Involving Senior Government Employees Where Allegations of Misconduct Were Substantiated	24
Section 5(a)(20)	Description of Any Instance of Whistleblower Retaliation	24
Section 5(a)(21)	Description of Any Attempt by the Agency to Interfere With the Independence of the OIG	24
Section 5(a)(22)	Inspections, Evaluations, and Audits, and Investigations Involving Senior Government Employees That Were Not Disclosed	24
Section 3(d)	Peer Review	27

APPENDIX B

Final Reports Issued and Grouped by OIG Strategic Goal

REPORT NAME	NUMBER OF RECOMMENDATIONS	QUESTIONED COSTS	FUNDS PUT TO BETTER USES ($)	OTHER MONETARY IMPACT ($)
Transforming GPO into a Digital Platform				
Information Security: Penetration Testing of GPO's Web-Hosted Service—www.usgovernmentmanual.gov (Report No. 17-14)	2			
Information Security: Penetration Testing of GPO's Web-Hosted Service—publications.usa.gov (Report No. 17-15)	5			
Information Security: Penetration Testing of GPO's Web-Hosted Service—www.memberguide.gpo.gov (Report No. 17-16)	2			
Information Security: Penetration Testing of GPO's Web-Hosted Service—cah.gpo.gov (Report No. 17-17)	5			
Information Security: Penetration Testing of GPO's Web-Hosted Service—www.fedreg.gov (Report No. 17-18)	4			
Information Security: Penetration Testing of GPO's Web-Hosted Service—www.federalregister.gov (Report No. 17-19)	2			

APPENDIX B (Continued)

REPORT NAME	NUMBER OF RECOMMENDATIONS	QUESTIONED COSTS	FUNDS PUT TO BETTER USES ($)	OTHER MONETARY IMPACT ($)
Information Security: Penetration Testing of GPO's Web-Hosted Service—www.uscc.gov (Report No. 17-20)	2			
Information Security: Penetration Testing of GPO's Web-Hosted Service—www.riddick.gpo.gov (Report No. 17-21)	1			
Information Security: Penetration Testing of GPO's Web-Hosted Service—conferencereport.gpo.gov (Report No. 17-22)	4			
Information Security: Penetration Testing of GPO's Web-Hosted Service—www.ofr.gov (Report No. 17-23)	2			
Information Security: Penetration Testing of GPO's Web-Hosted Service–www.ecfr.gov (Report No. 17-24)	2			
Federal PKI Compliance Report (Report No. 17-27)				
WebTrust for Certification Authority (Report No. 17-28)				
Operational and Financial Management				
Unscheduled and Unpaid Absenteeism: Security and Intelligent Documents (Report No. 17-13)	3		$760,081	

REPORT NAME	NUMBER OF RECOMMENDATIONS	QUESTIONED COSTS	FUNDS PUT TO BETTER USES ($)	OTHER MONETARY IMPACT ($)
Program and Operational Integrity				
Secure Credentials: Accountability Over Select Card Stock (Report No. 17-12)	2			
Information Security: Penetration Testing of GPO's PROBE System (Report No. 17-11)	18			
Stewardship over Official Publications				
Information Security: Penetration Testing of GPO's Ben's Guide Web Application (Report No. 17-10)	2			
Information Security: Penetration Testing of GPO's Next Generation Federal Digital System (Report No. 17-25)	3			

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
Mar. 24, 2014	*Changes Can Provide GPO Better Information on Establishing Billing Rates for Congressional Hearings* (Product Code 83)	14-07	1	
Mar. 25, 2014	*Information Technology Professional Services—Oracle Software*	14-08	1	$2,760,000
Aug. 1, 2014	*Acquisition of U.S. Passport Covers*	14-14	2	$15,700,000
Mar. 20, 2015	*Development of a Secure Credential Production System*	15-02	1	
Mar. 30, 2016	*Independent Verification and Validation of GPO's Composition System Replacement*	16-11	4	$742,952

APPENDIX D (Continued)

DATE ISSUED	NAME OF AUDIT	REPORT NUMBER	NUMBER OF RECOMMENDATIONS	MONETARY IMPACT ($)
Sept. 29, 2016	Information Security: *Information Technology: Oracle Maintenance and Support Licenses*	16-19	3	$7,076.179
Sept. 29, 2016	*Organizational Transformation: Composition System Replacement*	16-21	2	$4,600.000
Sept. 30, 2016	*Cloud Computing: Transition of GPO's Integrated Library System*	16-22	1	
		Total	**16**	**$31,251,848**

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	18	$760,081
Subtotal	**18**	$760,081
Unscheduled and Unpaid Absenteeism: Security and Intelligent Documents Report Number 17-13, July 13, 2017	1	$760,081

APPENDIX F

Investigations Productivity Summary

ITEM	QUANTITY
Total New Hotline/Other Allegations Received during Reporting Period	22
Preliminary Investigations (Complaints) Closed	13
Complaint Referrals to Other Agencies	0
Complaint Referrals to Office of Audits and Inspections	1
Investigations Opened by Office of Investigations during Reporting Period	10
Investigations Open at Beginning of Reporting Period	53
Investigations Closed during Reporting Period	7
Investigations Open at End of Reporting Period	56
Referrals to GPO Management (Complaints and Investigations for Corrective Action or Information Purposes)	1

Current Open Investigations	Number	Percent
Procurement/Contract Fraud	24	43
Employee Misconduct	17	30
Workers' Compensation Fraud	1	2
Information Technology/Computer Crimes	5	9
Proactive Initiatives	6	11
Other Investigations	3	5
Total	**56**	**100**

APPENDIX F (Continued)

Senior Government Employees Where Allegations of Misconduct Were Substantiated Investigations

There were no investigations.

Whistleblower Retaliation Investigations

OIG has two whistleblower retaliation investigations open. One pertains to similar allegations pending a hearing with the Equal Employment Opportunity Commission. The second pertains to similar allegations associated with ongoing litigation.

Attempt by the Agency to Interfere With the Independence of the OIG

There were no investigations.

Inspections, Evaluations, and Audits, and Investigations Involving Senior Government Employees That Were Not Disclosed

There were no investigations.

APPENDIX G

Investigations Productivity Summary

ITEM	QUANTITY
Investigative cost efficiencies, restitutions, recoveries, fines, and penalties, Funds Put to Better Use	$942,247
Arrests, including summons in lieu of arrest	0
Persons referred to Federal prosecutors	21
Persons accepted for Federal prosecution	8
Persons declined for Federal prosecution	13
Persons referred to state/local prosecutors	0
Persons accepted for state/local prosecution	0
Persons accepted for state/local prosecution	0
Indictments/Information/Complaints	0
Convictions	0
Guilty Pleas/Deferred Prosecution Agreements	0
Probation (months)	0
Jail Time (days)	0
Criminal Fines, Fees, Recovery, and/or Restitution	$0

APPENDIX G (Continued)

Persons referred for civil action	24
Persons accepted for civil action	13
Persons declined for civil action	11
Civil Settlements	0
Civil Fines, Fees, Recovery, and/or Restitution	$0
Total Number of Investigative Reports Issued	3
Referrals to GPO Management for Possible Corrective Action and/or Information Purposes	0
Employee Corrective Action	1
Agency/Process Corrective Action	0
Business/Individual Referrals to GPO Suspending and Debarring Official for Suspending and /or Debarment	11
Suspensions	10
Debarment	10
Other Suspending and Debarring Official Response/Action	1
Employee Suspension/Termination	1

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 Export-Import Bank OIG reviewed the system of quality control for the audit organization of the GPO OIG. GPO OIG received a peer review rating of pass with deficiencies.

Peer Review of GPO OIG Investigative Function
The U.S. Pension Benefit Guaranty Corporation OIG conducted the most recent peer review of the investigative function at GPO in May 2016. OIG received a rating of compliant with the Council of Inspectors General on Integrity and Efficiency (CIGIE) quality standards established and the applicable Attorney General guidelines.

A copy of both peer review reports can be viewed at http://www.gpo.gov/oig/

REPORT FRAUD, WASTE, AND ABUSE

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

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

GPO

U.S. GOVERNMENT PUBLISHING OFFICE