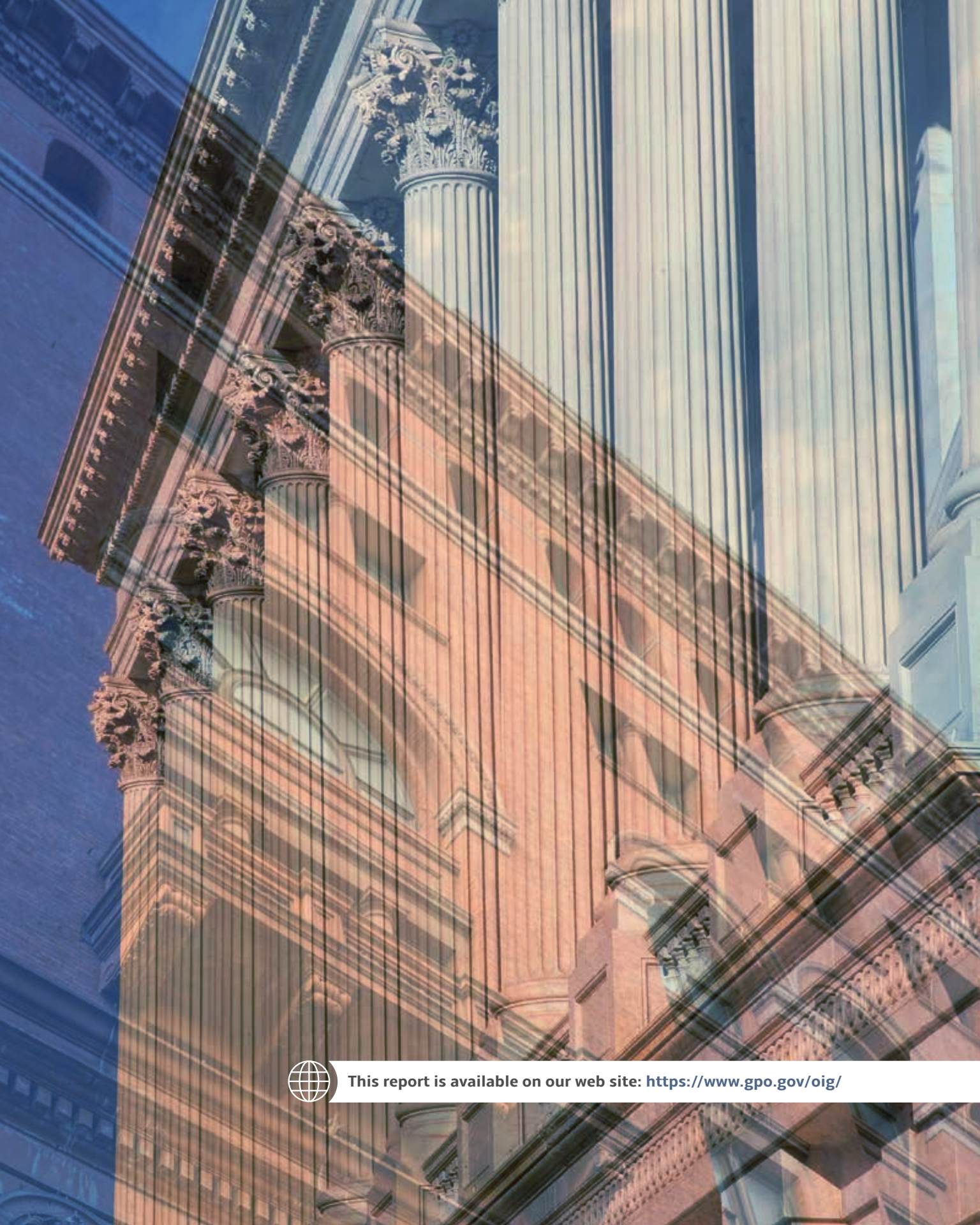**GPO** | **U.S. GOVERNMENT PUBLISHING OFFICE**
Office of Inspector General

SEMIANNUAL REPORT TO CONGRESS

October 1, 2018 – March 31, 2019

ABOUT THE GOVERNMENT PUBLISHING OFFICE

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 govinfo.gov and partnerships with 1,132 libraries nationwide participating in the Federal Depository Library Program (FDLP).[1] GPO employs approximately 1,740 personnel.[2]

ABOUT 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; and prevent and detect fraud, waste, and abuse.

The GPO Inspector General Act of 1988, Title 44, Chapter 39 of the United States Code, establishes the responsibilities and duties of the OIG. OIG is located in Washington, D.C. It is authorized 22 employees and is organized into 2 major functions—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 fully informed of any problems or deficiencies relating to administering and operating GPO. The IG reports directly to and serves at the pleasure of the Director as an independent function within GPO. OIG follows professional standards as required by the Act.

1 Superintendent of Documents email, dated April 2, 2019.
2 GPO Budget Justification for Fiscal Year 2019

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

INSPECTOR GENERAL MESSAGE

I am honored to have been selected to serve as the Acting Inspector General (IG) for GPO, and it is my pleasure to submit this Semiannual Report to Congress on the operations of GPO's Office of Inspector General (OIG). This report covers OIG activities for the period from October 1, 2018, through March 31, 2019.

OIG remains steadfastly committed to providing independent and objective oversight of GPO programs and operations by conducting timely and relevant audits, investigations, and other reviews. Throughout the reporting period, our oversight work identified inefficiencies; reduced fraud, waste and abuse; and improved performance. We also identified systemic vulnerabilities and recommended programmatic changes that will ultimately strengthen internal controls and mitigate risk.

Although I have only had the opportunity to serve as the Acting IG for a short period, I have been consistently impressed by the hard work and dedication of the exceptional auditors, investigators, counsel, and support staff who make up the OIG team. I want to thank these dedicated men and women who work so diligently each day to accomplish OIG's essential mission. I would also like to acknowledge the considerable effort expended by GPO management during this past reporting period to enhance the efficiency and effectiveness of GPO operations by addressing and resolving a large number of open recommendations reported by this office in previous Semiannual Reports.

Additionally, I would like to express my deepest appreciation and best wishes to former GPO IG Melinda Miguel, who moved on to a new position as Chief Inspector General of the Executive Office of the Governor of the State of Florida.

Finally, I would like to thank the U.S. Senate Committee on Rules and Administration, the U.S. House of Representatives Committee on House Administration, and the U.S. Congress Joint Committee on Printing, for their continued support of OIG initiatives.

Respectfully,

James R. Ives
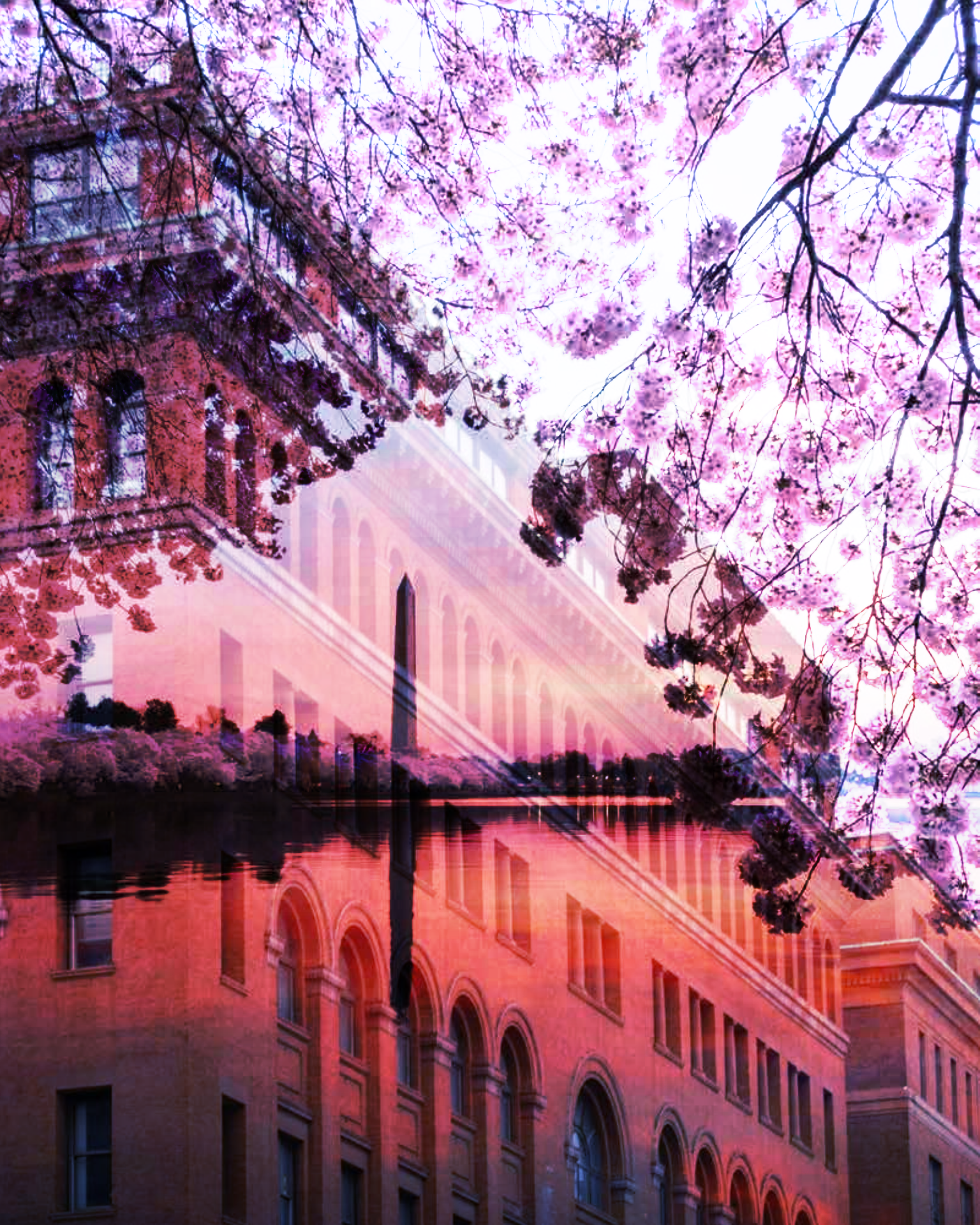*Acting Inspector General*

TABLE OF CONTENTS

SELECTED STATISTICS

Investigations

Audits and Inspections

MANAGEMENT CHALLENGES

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 also examine other GPO Annual Reports, Budget Justification Reports, and Strategic Plans for relevant information about key factors facing the Agency. The prior Semiannual Report showed the following as challenges GPO faces:

- Keeping focus on its mission of information dissemination
- Improving the Enterprise Architecture and Information Technology Infrastructure
- Securing Information Technology (IT) systems and protecting related information assets
- Improving Print Procurement Programs

For each challenge, OIG provides a statement about GPO's progress in addressing that challenge.

Changes from Previous Reporting Period

The following key criteria are considered for whether to remove a management challenge from a prior report: (1) demonstrated strong leadership commitment in addressing the issue; (2) ability to address the problem; (3) plan for how corrective measures will be implemented; (4) program for monitoring the corrective action; and (5) demonstrated progress in the implementation of the corrective measures. The following challenges were reported in the previous reporting period. Updates may be included in the next 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 impacted each 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 EA and IT Infrastructure

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, Title 44, Chapter 36 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 continues to anticipate.

GPO's Progress: Since our prior report, GPO has completed its transformation of FDsys to govinfo. OIG would like to commend GPO on its efforts and we have modified our challenge statement to reflect this accomplishment, recognizing the fact that GPO should continue to strive to improve its defined EA and IT infrastructure framework.

Challenge 3: Securing Information Technology Systems and Protecting Related Information Assets

Overview: GPO IT 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. OIG conducts penetration testing to assist in mitigating certain risks associated with this strategic challenge.

Challenge 4: Improving Print Procurement Programs

Overview: GPO is the principal agent for almost all Government printing. Title 44, Chapter 5, Section 501 of the United States Code requires that GPO perform all printing, binding, and blank-book work for Congress, the Executive Office, the Judiciary—other than the Supreme Court of the United States—and every executive department, 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 department, independent office, or establishment; and (3) procurement of printing by an executive department, independent office, or establishment from allotments for contract field printing, if approved by the JCP.

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

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

AUDITS AND INSPECTIONS

U.S. Government Publishing Office FY 2018 Independent Auditors' Report

OIG contracted with an independent audit firm to audit GPO's financial statements. In the opinion of the independent auditors, the consolidated financial statements presented fairly, in all material respects, the financial position of GPO as of September 30, 2018, and 2017, and the results of its operations and cash flows for the years then ended in accordance with U.S. generally accepted accounting principles.

Recommendations: The report did not contain any recommendations. (*U.S. Government Publishing Office FY 2018 Independent Auditors' Report, Report No. 19-01*)

FDsys Headquarters Application Attempted Defacement Incident

OIG conducted an audit of GPO's FDsys Headquarters Application controls prior to a cyberattack in March 2017 and reviewed the steps GPO took for enhancing cybersecurity subsequent to the attack. GPO's FDsys provided free online access to official publications from the three branches of the Federal Government.

The audit found that FDsys had various controls in place as part of its IT platform for preventing security breaches. Despite the controls, however, an attacker overwrote more than 24,000 files with Hypertext Markup Language code in a defacement attempt. The attacker also created a file on one of the four FDsys servers, and subsequently uploaded Perl scripts and content to the four servers, which eventually rendered one of four servers nonoperational.

Following the cyberattack, GPO OIG requested forensic and investigative support from the U.S. Postal Service OIG's Computer Crimes Unit (CCU). CCU noted that GPO's computer forensic capabilities associated with FDsys did not have provisions sufficient enough to allow for a more robust forensic review. Additionally, GPO OIG found that GPO:

- Did not take advantage of a real-time vulnerability detection alerting tool that could have provided an early warning of the attacker's intrusions.

- Made incorrect risk assumptions during its vulnerability evaluation that could have mitigated the attacker's exploitation.

- Should be more proactive in implementing all applicable cybersecurity measures available.

GPO subsequently installed new log and storage devices and fully migrated log/packet sources at GPO's datacenter sites. GPO also implemented a real-time data stream to the Virtual Security Operations Center (V-SOC) monitoring system with signature detection capabilities. Additionally, GPO created layered security controls for augmenting the V-SOC monitoring system and established a Web Application Firewall.

Recommendations: OIG made two recommendations that included updating GPO's security policy and migration to a Web Application Firewall. Management implemented or has plans to implement the necessary corrective actions. (*Information Security: GPO Should Strengthen Network Controls to Avoid Future Cyber Attacks, Report No. 19-02*)

Management Letter—FY 2018 Financial Statements

In conjunction with the FY 2018 financial statement audit, a management letter was issued to GPO reporting operational matters involving internal controls not included in the consolidated financial audit report. The following five areas with recommendations were reported. The monetary impact related to those areas totaled $2.3 million.

- Processing of Personnel Actions

- Commercial Printing Contract Review Board Actions

- Review and Approval Controls within Acquisition Services

- Review of Invoices Related to Certain Expenses

- Recording of Inventory Receipts

Recommendations: OIG made five recommendations for improving internal controls over financial reporting and other operating efficiencies. (*Management Letter—FY 2018 Financial Statements, Report No. 19-03*)

Information Technology—FY 2018 Financial Statements

In connection with the audit of the GPO FY 2018 financial statements, an assessment of IT controls was performed. Audit results indicated deficiencies in the areas of access controls, segregation of duties, and contingency planning. Those conditions were generally the result of GPO's resource constraints and competing priorities.

Access Controls. Controls could be strengthened in the GPO Business Information System (GBIS) separated user process and the new user process.

Segregation of Duties. The GBIS segregation of duties policy could be strengthened.

Contingency Planning. The General Support System contingency plan was not finalized, approved, and tested.

Recommendations: OIG made three recommendations for improving internal controls associated with financial accounting computer systems. (*Information Technology—FY 2018 Financial Statements, Report No. 19-04*)

Evaluation of Cybersecurity Controls of GPO's govinfo

OIG conducted penetration testing of GPO's govinfo. The testing assessed the Agency's cybersecurity efforts and identified vulnerabilities that could be exploited. Govinfo is a website that provides free public access to official publications from the three branches of the Federal Government. In addition, govinfo includes a content management system and a standards-compliant preservation repository. We found three vulnerabilities requiring cybersecurity countermeasures.

Recommendations: OIG made three recommendations for strengthening cybersecurity controls. Management implemented the necessary corrective actions for addressing the vulnerabilities. (*Information Security: Penetration Testing on govinfo, Report No.19-05*)

Evaluation of Cybersecurity Controls of GPO's FDLP eXchange

OIG conducted penetration testing of GPO's FDLP eXchange. FDLP is a Government program created to make U.S. Federal Government publications available to the public at no cost. There are 1,132 depository libraries in the United States and its territories. GPO, through FDLP, distributes certain classes of Government documents to designated libraries throughout the United States and its territories.

The FDLP eXchange replaces and expands upon the former National Needs and Offers. The National Needs and Offers is the old FDLP eXchange that processed FDLP customer requirements. The goal was to build an application that libraries in FDLP could use as a "one stop shop" for the entire Needs and Offers process. FDLP eXchange automates disposition processing by allowing libraries to enter information on materials they want to discard and to have the process managed by an automated workflow. No significant weakness in the configuration of this host or web applications were noted.

Recommendations: The report did not contain any recommendations. (*Information Security Penetration Testing of GPO's FDLP eXchange, Report No. 19-06*)

Evaluation of Cybersecurity Controls of GPO's Productivity Reporting for Operations, Budgeting, and Expenditures (PROBE) System

OIG conducted penetration testing of GPO's Productivity Reporting for Operations, Budgeting, and Expenditures (PROBE) system. PROBE is a labor-tracking system that operates 24 hours a day, 7 days a week. It captures time and attendance data for employees located at GPO's Central facility. PROBE is an internal GPO system that provides employees with the ability to charge their labor to different operations and classes. We discovered 14 vulnerabilities requiring corrective actions.

Recommendations: OIG made 14 recommendations for strengthening cybersecurity controls. Management implemented or has plans to implement the necessary corrective actions for addressing the vulnerabilities. (*Information Security: Penetration Testing of GPO's Productivity Reporting for Operations, Budgeting, and Expenditures (PROBE) System, Report No. 19-07*)

GPO's Management of Simplified Purchase Agreements

OIG examined Simplified Purchase Agreements (SPA) to determine whether GPO effectively trained and supervised SPA participants and ensured they complied with SPA requirements.

GPO established SPA with qualified vendors as an easy method for filling anticipated non-repetitive needs for printing, binding, related supplies, and related services with qualified sources. Using SPA, authorized Federal customers can place orders directly with individual vendors for products or services up to $10,000. GPO certifies vendors for SPA and notifies both customer agencies and contractors of new participants. GPO pays the vendor and then bills the customer. GPO operates 14 SPAs in its central and regional offices, including DC SPA 960. We reviewed SPAs operated by DC SPA 960.

The audit found that although GPO generally trained and supervised SPA participants, additional actions should have been taken for full compliance. Specifically, the audit revealed that GPO did not have sufficient documentation related to key components of SPA, which included Memorandums of Agreement (MOAs) (1 of 6 not located), training completion (8 of

53 personnel not supported), and procurement authority (2 of 43 missing). Additionally, GPO did not properly execute one of its MOAs and 3 of 43 customer agency personnel reviewed with authorizations were not on the authorized user list.

GPO uses the SPA authorized user list to track customer agency officials approved to use SPA vendors and determine if a user is authorized to submit the order. SPA vendors use the list to confirm that SPA users soliciting bids from their company are authorized as well as ascertain the purchasing limit for the user.

Personnel from selected Federal customers that received services under DC SPA 960 rated GPO's administration of SPA as excellent or good.

Recommendations: OIG made three recommendations with regard to improving controls and oversight of SPAs. (*GPO's Management of Simplified Purchase Agreements, Report No. 19-08*)

Evaluation of Cybersecurity Controls of GPO's Procurement Information Control System

OIG conducted penetration testing of GPO's Procurement Information Control System (PICS). The PICS application comprises two sub-system applications (hosted on the GPO mainframe and datacenter). PICS captures receipt of the Standard Form 1 (SF-1) order data from GPO Federal customers for the print procurement business function. Overall, the single host comprising this system did not have any significant weaknesses.

Recommendations: The report did not contain any recommendations. (*Information Security: Penetration Test of GPO's Procurement Information Control System (PICS), Report No. 19-09*)

Evaluation of Cybersecurity Controls of GPO's Secure Credentials and Personalization System

Penetration testing of GPO's Secure Credentials and Personalization System (SECAPS) was conducted to determine if GPO had appropriate security controls in place for reducing the risk of a cyberattack. The SECAPS application is used to securely ingest card production orders from authorized GPO card program customers and to securely produce the cards and provide secure order fulfillment for the cards in response to customer orders. Overall, no significant weaknesses were found in SECAPS.

Recommendations: The report did not contain any recommendations. (*Information Security: Penetration Test of GPO's Secure Credentials and Personalization System (SECAPS), Report No. 19-10*)

Table A: Audit Reports Issued In Reporting Period

Including Questioned Costs, Funds Put to Better Use and Other Monetary Impact				
Report Name	Number of	Questioned	Funds Put to Better Use	Other Monetary Impact
U.S. Government Publishing Office FY 2018 Independent Auditors' Report (Report No. 19-01)	0			
Information Security: GPO Should Strengthen Network Controls to Avoid Future Cyber Attacks (Report No. 19-02)	2			
Management Letter—FY 2018 Financial Statements (Report No. 19-03)	5			$2,350,000
Information Technology—FY 2018 Financial Statements (Report No. 19-04)	3			
Information Security: Penetration Testing on govinfo (Report No. 19-05)	3			
Information Security Penetration Testing of GPO's FDLP eXchange (Report No. 19-06)	0			
Information Security: Penetration Testing of GPO's Productivity Reporting for Operations, Budgeting, and Expenditures (PROBE) System (Report No. 19-07)	14			
GPO's Management of Simplified Purchase Agreements (Report No. 19-08)	3			
Information Security: Penetration Test of GPO's Procurement Information Control System (PICS) Report No. 19-09	0			
Information Security: Penetration Test of GPO's Secure Credentials and Personalization System (SECAPS) (Report No. 19-10)	0			

INVESTIGATIONS

December 28, 2018, Suspension Referral; Contractor Non-Compliance with Internal Bid Submission Practices (18-0006-I):

OIG developed evidence suggesting a potential bidder for GPO's Census 2020 contract failed to follow its own internal quality review processes when constructing its bid for the prior iteration of this contract. OIG provided an interim report to the GPO Suspending and Debarring Official (SDO) while bids were being evaluated so as to ensure GPO possessed potentially pertinent information prior to making a decision.

Agency Response: The contract for Census 2020 was awarded to a different vendor in January 2019, although no indication exists that the action was taken as a result of this interim report.

March 11, 2019, Suspension and Debarment Referral; GPO Contractor – Lack of Business Integrity (18-0006-I):

A Stamford, Connecticut company and its agent were investigated for submitting defective documents to GPO. The investigation revealed that the company, through its agent, submitted documents to GPO that contained serious errors. According to the agent, he bypassed company policy by not having the documents reviewed prior to providing them to GPO. After discovering the errors, the agent waited more than 2 weeks to report the claimed error to GPO, which contributed to a significant loss of time and effort for GPO contracting personnel.

Agency Response: The GPO SDO is considering this matter.

March 15, 2019, Suspension and Debarment Referral; Submission of False Invoice Documents (18-0015-I):

An investigation of a Simi Valley, California company disclosed that 17 invoice packets were submitted before the actual items were shipped by the company. In order to meet GPO's requirement for proof of shipment in the invoices submitted, the company included shipping documents from unrelated shipments. Furthermore, the company also submitted false shipping documents for 10 additional contracts. In those 10 contracts, the shipping documents contained in the invoices the company submitted did not match the city or state of the locations to which the items were actually delivered. The total value of the contracts for which the company submitted false documents was $50,979.

Agency Response: The GPO SDO is considering this matter.

Table B: Investigations Statistics for Reporting Period[3]

Item	Quanity
Complaints Opened	26
Complaints Closed	21
Complaints Referrals to Other Agencies	2
Complaints Referrals to Office of Audits and Inspections	0
Investigations Opened by Office of Investigations during Reporting Peiord	2
Investigations Open at End of Reporting Period	58
Investigations Closed	5
Total Number of Investigative Reports Issues in Reporting Period	3
Referrals to GPO Management (Complaints and Investigations for either Corrective Action or Informational Purposes)	7

Current Open Investigations	Number	Percentage
Procurement/Contract Fraud	27	47
Employee Misconduct	17	29
Workers' Compenstaion Fraud	0	0
IT/Computer Crimes	2	3
Proactive Intiatives	9	16
Other Investigations	3	5
TOTAL	**58**	**100**

3. Metrics for developing data for reported statistics were obtained from OIG's Case Management Tracking System.

Table C: Investigations Productivity Statistics for Reporting Period[4]

Item	No. or Amt.
Arrests, including Summons in Lieu of Arrest	0
Persons Referred to Federal Prosecutors	4
Persons Accepted for Federal Prosecution	0
Persons Declined for Federal Prosecution	4
Persons Referred to State/Local Prosecutors	0
Persons Accepted for State/Local Prosecution	0
Persons Declined for State/Local Prosecution	0
Indictments/Information/Complaints	0
Convictions	0
Guilty Pleas/Deferred Prosecution Agreements	0
Probation (in Months)	0
Jail Time (in Days)	0
Criminal Fines, Fees, Recovery, and/or Restitution	$0
GPO Fines, Fees, and Restitution	$0
Persons Referred for Civil Action	2
Persons Accepted for Civil Action	0
Persons Declined for Civil Action	3
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	7
Employee Corrective Action	1
Agency/Process Corrective Action	0
Business/Individual Referrals to GPO Suspending and Debarring Official for Suspension and/or Debarment	4
Suspensions	13
Debarments	7
Other Response/Action	0
Employee Suspension/Termination/Other Action	1
Subpoenas Issued	0
Investigations Open at the Beginning of the Period	61
Investigations Open at the End of the Period	58
Complaints Open at the Beginning of the Period	31
Complaints Open at the End of the Period	36
Total: Fines, Questioned Costs, Overcharges, Restitution	**$50,979[5]**

4 Metrics for developing data for reported statistics were obtained from OIG's Case Management Tracking System.

5 This amount does not include any questioned costs or information on financial impact relating to the 2020 Census printing and mailing contract reported previously because the total impact is not yet known.

OTHER INFORMATION

Significant Revised Management Decisions

There were no significantly revised management decisions this reporting period.

Significant Management Decision with which the IG Disagreed

There were no significant management decisions with which the Acting IG disagreed during the reporting period.

Inspections, Evaluations, and Audits, and Investigations Involving Senior Government Employees that were Not Disclosed to the Public or Where Allegations of Misconduct Were Substantiated

There were no instances during the reporting period whereby OIG completed an inspection, evaluation, or audit without disclosing the results to the public. All such, product titles are listed on https://www.gpo.gov/oig/. Where possible, the report was also posted. Beginning October 2018, report titles and when possible, the audit and inspection reports, were posted at www.oversight.gov.

Whistleblower Retaliation Investigations

None.

Instances of GPO Refusing to Provide Information or Assistance or Interfering with the OIG's Independence

There were no instances whereby GPO refused to provide information or assistance or interfered with the OIG's independence during this reporting period.

PEER REVIEW RESULTS

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 and issued its report on June 2, 2017. GPO OIG received a peer review rating of pass with deficiencies. OIG addressed the deficiencies identified during the review.

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. GPO OIG received a rating of compliant with the quality standards the Council of Inspectors General on Integrity and Efficiency established and applicable Attorney General guidelines.

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

APPENDIX A

Summary of Each Audit Report over 6 Months Old for Which No Management Decision Has Been Made[6]

Date Issued	Name	Report Number	Numcer of Recommednations	Costs ($)
None				

---

6 Section 5(a)(10), IG Act of 1978.

APPENDIX B

Prior Audit Recommendations on Which Corrective Action Has Not Been Completed in More Than 1 Year[7]

Date Issued	Name of Audit	Report Number	Number of Recommendations	Monetary Impact ($)
Mar. 24, 2014	Changes Can Provide GPO Better Information on Establishing Billing Rates for Congressional Hearings (Product Code 83)	14-07	1	
Mar. 30, 2016	Independent Verification and Validation of GPO's Composition System Replacement	16-11	1	$742,952
Feb. 1, 2017	Information Security: Penetration Testing of GPO's Automated PDF Signing (APS)	17-02	2	
Mar. 28, 2017	Financial Management: Unbilled Congressional Publication Jackets	17-08	2	
Jul. 24, 2017	Information Security: Penetration Testing of GPO's PROBE system	17-11	6	
Aug. 18, 2017	Information Security: Penetration Testing of GPO's Web Hosted Service www.publications.usa.gov	17-15	1	
Aug. 18, 2017	Information Security: Penetration Testing of GPO's Web Hosted Service www.memberguide.gpo.gov	17-16	1	
Sep. 7, 2017	Information Security: Penetration Testing of GPO's Web Hosted Service www.cah.gpo.gov	17-17	4	
Sep. 7, 2017	Information Security: Penetration Testing of GPO's Web Hosted Service www.fedreg.gov	17-18	4	
Sep. 7, 2017	Information Security: Penetration Testing of GPO's Web Hosted Service www.ofr.gov	17-23	1	
Mar. 1, 2018	Information Security: Penetration Testing of GPO's WebTA version 4.2	18-05	2	
Mar. 27 2018	Information Security: Penetration Testing of GPO's Data Center in a Crate -2 System	18-11	5	
Total			**30**	**$742,952**

---

7 Section 5(a)(3), IG Act of 1978

APPENDIX C

Reporting Requirements under the IG Act of 1978

Reporting	Requirement	Pages
Section 4(a)(2)	Review of Legislation and Regulations (none for this period)	None
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	All
Section 5(a)(2)	Recommendations for Corrective Actions to Address Significant Problems, Abuses, and Deficiencies Identified	5-8
Section 5(a)(3)	Significant Outstanding Recommendations on which Corrective Action has Not Been Completed	15
Section 5(a)(4)	Matters Referred for Prosecutorial Authorities	11
Section 5(a)(5); 6(b)(2)	Information or Assistance Unreasonably Refused or Not Provided	12
Section 5(a)(6)	List of Completed Audit, Inspection, or Evaluation Reports	5-8
Section 5(a)(7)	Summary of Significant Reports	5-9
Section 5(a)(8)	Statistical Tables Related to Total Value of Questioned or Unsupported Costs	8
Section 5(a)(9)	Statistical Tables Related to Funds Recommended To Be Put to Better Use	8
Section 5(a)(10)	Summary of Each Audit Report over 6 Months Old for Which No Management Decision Has Been Made	14
Section 5(a)(11)	Description and Explanation of Any Significant Revised Management Decision	12
Section 5(a)(12)	Information on Any Significant Management Decision with which the IG Disagrees	12
Section 5(a)(13)	Information described under section 804(b) of the Federal Financial Management Improvement Act of 1996 – not applicable to GPO	N/A
Section 5(a)(14) Through (16)	Peer Review Results	13
Section 5(a)(17)	Statistical Tables Related to Investigations	10-11
Section 5(a)(18)	Description of Metrics Used for Developing the Data for the Statistical Tables under Section 5(a)(17)	10-11
Section 5(a)(19)	Investigations Involving Senior Government Employees Where Allegations of Misconduct Were Substantiated	12
Section 5(a)(20)	Description of Any Instance(s) of Whistleblower Retaliation	12
Section 5(a)(21)	Description of Any Attempt(s) by the Agency to Interfere with the Independence of the OIG	12
Section 5(a)(22)	Inspections, Evaluations, Audits, and Investigations Involving Senior Government Employees That Were Closed and Not Disclosed to the Public	12

APPENDIX D

Abbreviations and Acronyms

CCU	Computer Crimes Unit
EA	Enterprise Architecture
FDLP	Federal Depository Library Program
FDsys	Federal Digital System
FY	Fiscal Year
GBIS	GPO Business Information System
GPO	Government Publishing Office
IG	Inspector General
IT	Information Technology
JCP	Joint Committee on Printing
MOA	Memorandum of Agreement
OIG	Office of Inspector General
PICS	Procurement Information Control System
PROBE	Productivity Reporting for Operations, Budgeting, and Expenditures
SECAPS	Secure Credentials and Personalization System
SPA	Simplified Purchase Agreement
V-SOC	Virtual Security Operations Center

APPENDIX E

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 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 U.S. Attorney, filed 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.

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
Action 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 Cost
Questioned cost not supported by adequate documentation.

REPORT FRAUD, WASTE OR ABUSE

U.S. Government Publishing Office

Office of Inspector General

P.O. Box 1790

Washington, DC 20013-1790

Email: gpoighotline@gpo.gov
Fax: 202.512.1352
Main Number: 202.512.0039
Hotline: 1.800.743.7574