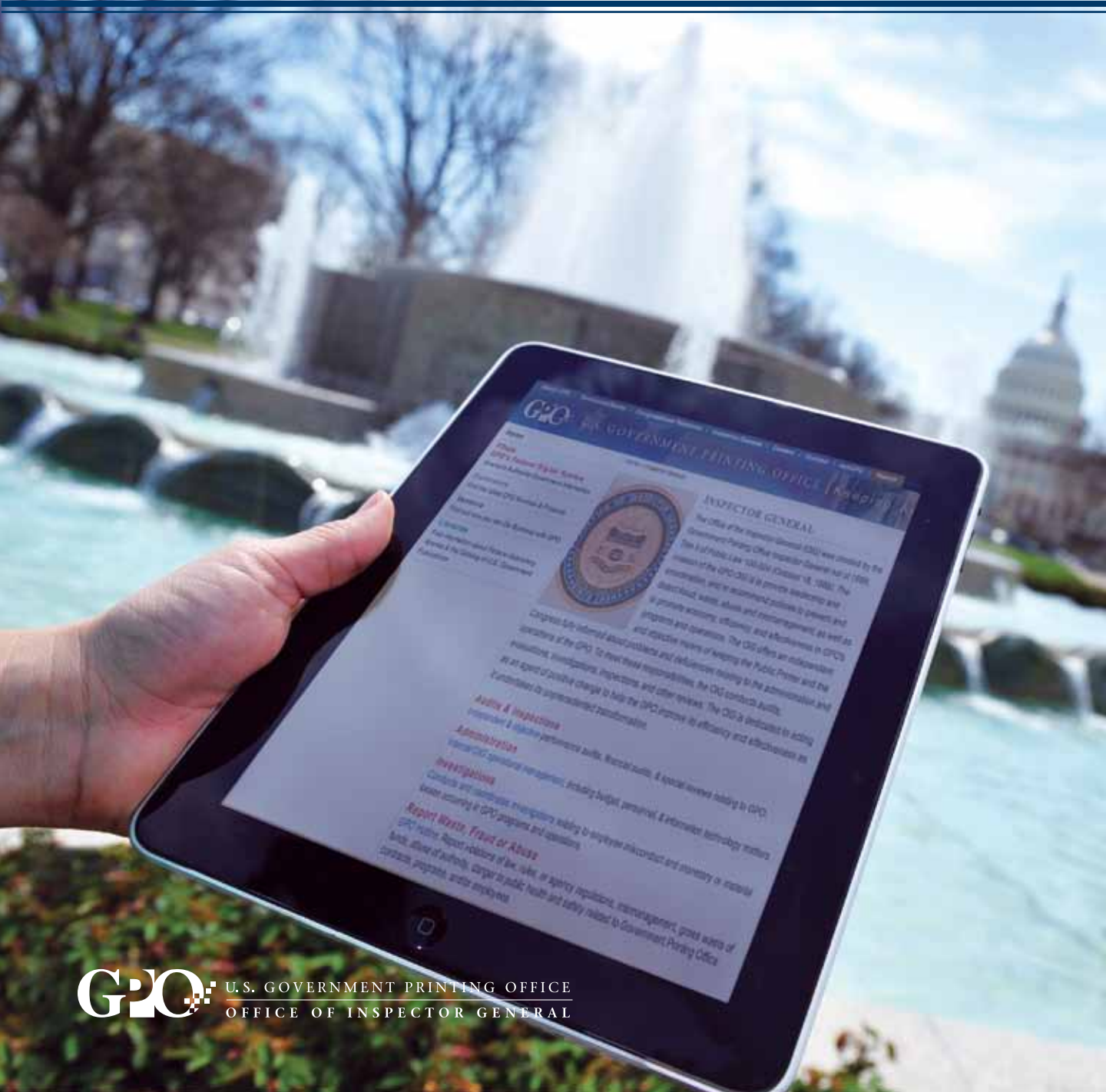


U. S. GOVERNMENT PRINTING OFFICE ■ OFFICE OF INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

OCTOBER 1, 2010 THROUGH MARCH 31, 2011



GPO U.S. GOVERNMENT PRINTING OFFICE | INSPECTOR GENERAL

MISSION
The Office of the Inspector General (OIG) was created by the Government Printing Office Inspector General Act of 1998, Title I of Public Law 105-261 (October 18, 1998). The mission of the OIG is to provide leadership and oversight, advise, advise and recommend policies to prevent and identify waste, fraud, and abuse and to improve the efficiency and effectiveness of the GPO's operations. The OIG offers an independent and objective review of the Public Printer and the operations of the GPO. To report these responsibilities, the OIG conducts audits, investigations, inspections, and other reviews. The OIG is dedicated to acting as an agent of positive change to help the GPO improve its efficiency and effectiveness and to provide the best possible service to the public.

Services
The OIG provides a variety of services, including:

- **Audit & Inspection**
Financial and compliance audits, financial audits, and special reviews relating to GPO.
- **Investigations**
Conducts and oversees investigations relating to employee misconduct and integrity in special cases, including GPO programs and operations.
- **Report Waste, Fraud or Abuse**
GPO waste, Report violations of law, rules, or agency regulations, mismanagement, gross waste of funds, abuse of authority, danger to public health and safety related to Government Printing Office contracts, programs, and/or employees.

THE U.S. GOVERNMENT PRINTING OFFICE

For well over a century, the U.S. Government Printing Office (GPO) has fulfilled the needs of the Federal Government for information products and distributing those products to the public. GPO is the Federal Government's primary resource for gathering, cataloging, producing, providing, authenticating, and preserving published U.S. Government information in all its forms. GPO also produces and distributes information products and services for each of the three branches of Government.

Under the Federal Depository Library Program, GPO distributes a wide range of Government publications in print and online to more than 1,250 public, academic, law, and other libraries across the country. In addition to distributing publications through that library system, GPO provides access to official Federal

Government information through public sales and other programs, and—most prominently—by posting more than a quarter of a million titles online through GPO Access (www.gpoaccess.gov).

Today approximately 97% of all Federal Government documents begin as digital products and are published directly to the Internet. Such an evolution of creating and disseminating information challenges GPO, but it has met those challenges by transforming itself from primarily a print format entity to an agency ready, willing, and able to deliver from a digital platform a high volume of information to a multitude of customers.

Although a transition to digital technology changes the way products and services are created and offered, GPO strives to continually satisfy the requirements of Government and accomplish its mission of *Keeping America Informed*.

THE OFFICE OF INSPECTOR GENERAL

The Office of Inspector General (OIG) was created by the GPO Inspector General Act of 1988—title II of Public Law 100-504 (October 18, 1988) (GPO IG Act). The OIG at GPO is dedicated to acting as an agent of positive change—changes that will help GPO improve its efficiency and effectiveness as the Agency undertakes an era of unprecedented transformation. Through evaluation of GPO's system of internal controls, the OIG recommends policies, processes, and procedures that help prevent and detect fraud, waste, abuse, and mismanagement.

The OIG also recommends policies that promote economy, efficiency, and effectiveness in GPO programs and operations.

The OIG informs the Public Printer and Congress about problems and deficiencies as well as any positive developments relating to GPO's administration and operation. To accomplish those responsibilities, the OIG conducts audits, assessments, investigations, inspections, and other reviews.

TABLE OF CONTENTS

MESSAGE FROM THE INSPECTOR GENERAL	3
HIGHLIGHTS OF THIS SEMIANNUAL REPORT	5
OIG MANAGEMENT INITIATIVES	6
PERSONNEL UPDATE	7
COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY	7
REVIEW OF LEGISLATION AND REGULATIONS	8
GPO MANAGEMENT CHALLENGES	9
OFFICE OF AUDITS AND INSPECTIONS	21
A. Summary of Audit and Inspection Activity	21
B. Financial Statement Audit	21
C. Audit and Inspection Reports	22
D. Ongoing Work	25
E. Status of Open Recommendations	26
OFFICE OF INVESTIGATIONS	31
A. Summary of Investigative Activity	31
B. Types of Cases	32
C. Summary of Investigative Accomplishment	33
D. Management Implication Reports	35
APPENDICES	
A. Glossary and Acronyms	37
B. Inspector General Act Reporting Requirements	40
C. Statistical Tables	41
Table C-1: Audit Reports with Questioned and Unsupported Costs	42
Table C-2: Audit Reports with Recommendations for Funds That Can Be Put to Better Use. .	43
Table C-3: List of Audit and Inspection Reports Issued During Reporting Period	44
Table C-4: Investigations Case Summary	45
Table C-5: Investigations Productivity Summary	46
D. Peer Review Results	47

MESSAGE FROM THE INSPECTOR GENERAL

“

NOW IS THE TIME TO EMBRACE TECHNOLOGY, anticipate customer and stakeholder needs, and provide real-time access to information in a usable, searchable, and sustainable electronic format. ”



“The rules have changed. In a single generation, revolutions in technology have transformed the way we live, work and do business. Steel mills that once needed 1,000 workers can now do the same work with 100.”

—President Barack Obama

In his 2011 State of the Union Address, President Obama made a clarion call to the people of the United States. His message also resonates on the realities of GPO operations. As the digital revolution advances, the need for printed product is quickly being replaced by demand for documents on the Internet and digital devices such e-readers and iPads. But, as the President noted,

“[T]his shouldn’t discourage us. It should challenge us . . . The first step in winning the future is encouraging American innovation. . . . Thirty years ago, we couldn’t know that something called the Internet would lead to an economic revolution. What we can do—what America does better than anyone else—is spark the creativity and imagination of our people.”

With that challenge, GPO stands at a cross roads. The need to innovate has never been more critical. Indeed, thirty years ago, we had no idea that the Internet, Blackberries, social networking, and the like would reshape our day-to-day lives.

Consider that three years ago, we could not conceive of the iPad. Yet these innovations and technological advances have reshaped how we access and use information. And the momentum for ongoing digital innovation remains unabated. While the print industry often invokes the words of Benjamin Franklin, to remain viable, the industry must embrace the revolutions created by the likes of Steve Jobs, Mark Zuckerberg, and Jeff Bezos—to name only a few.

This is an important backdrop to other realities facing the GPO during these challenging fiscal times. Trudy Givens, a worker for the Federal Bureau of Prisons, won the President’s 2010 SAVE AWARD for suggesting that GPO cease printing and mailing thousands of copies of the *Federal Register*, the federal government’s official daily publication of executive branch rules, notices, orders and other presidential documents. Savings are estimated at approximately \$4 million per year. In addition, after have been several bills have been introduced in Congress to limit printing by GPO. Federal agencies, in efforts to reduce costs, are also curtailing printing.

Yet, a decline in printing does not translate as a decline in the need or desire for information. In fact, the opposite appears true. Congress and the American people want information – they just want it faster, quicker, and in a searchable and usable format. While we may enjoy big books on the desk, there is no search function on the paper version of the budget or congressional bills.

The demand for change is real and again evidenced by the Public Online Information Act recently introduced in both the House and Senate. Congress notes specifically that “[a]s the public moves online, the Government must do so as well. *It should do so in ways that take advantage of modern technology, that anticipate the public’s needs, and that provide access to the greatest number of people.*”

Charged with Keeping America Informed, GPO should be on the forefront of these digital transformation efforts. GPO has taken the first steps with the Federal Digital System (FDsys) and its recent agreement to offer GPO publications through the Google ebookstore, but it should do more to spark the creativity and imagination of the GPO workforce. Now is the time to innovate, educate, and build an Agency that can meet the demands of today and the future. Now is the time to embrace technology, anticipate customer and stakeholder needs, and provide real-time access to information in a usable, searchable, and sustainable electronic format. By so doing, GPO can heed the President’s clarion call, and in the process can become more efficient and economical – a model for innovation.

Indeed, technology has also transformed the way the GPO OIG does business. Our oversight efforts continue to focus on the innovations and technology developments at GPO, while also addressing the potential for fraud during an economically fragile time. And within the OIG, we continue to utilize technology to help address customer and stakeholder needs, as well as provide access to our reports and information.

During this reporting period, the Office of Audits and Inspections (OAI) continued to examine the vulnerabilities and risks associated with implementation of the FDsys and we are pleased that several recommendations have been closed during this period. OAI also identified serious issues related to

the inventory control and management of laptop computers within the Agency. While Agency management accepted our recommendations, we will continue to monitor this matter as the Agency has yet to account for its full inventory of laptop computers. OAI also made several recommendations to help improve the ethics program and culture at GPO.

Our Office of Investigations (OI) continued its focus on contract and procurement fraud, which resulted in one conviction, seven debarments, and the issuance of numerous subpoenas in several ongoing investigations. OI also issued two management implication reports that have alerted Agency management to a variety of issues of employee misconduct on night shifts and vulnerabilities in surplus property management – underscoring the need for greater controls in property management at GPO.

I am also very proud to report that both the OAI and OI underwent and passed peer reviews this period. These reviews provide third-party assurance that the GPO OIG is in compliance with federal standards and has in place internal safeguards and management procedures to ensure such compliance. I commend my senior management team on their continued efforts to review and improve our operations and efficiencies, while also creating a positive and enriching work environment.

And on a final personal note, this will be my last semi-annual report as Inspector General of the GPO. It has been an honor and privilege to serve the dedicated members of the OIG, the GPO, its customers and stakeholders, and the American public in this capacity. I am very proud of the women and men of the OIG and the commitment they demonstrate every day to their profession. I leave with a sense of accomplishment knowing that the OIG is on course to meet its mission and statutory obligations to be an independent and objective force to promote economy, efficiency, and effectiveness and ferret out fraud, waste, and abuse in the programs and operations of GPO.



J. Anthony Ogden
Inspector General
U.S. Government Printing Office

HIGHLIGHTS OF THIS SEMI ANNUAL REPORT



The Office of Audits and Inspections (OAI) issued six reports during this reporting period. Those six reports included an audit of the agency's ethics program as well as an audit of the control and accountability of laptop computers. An audit was also completed of the information technology (IT) security controls over GPO's Secure Card Personalization System (SECAPS). OAI also continued to oversee the Independent Verification and Validation (IV&V) efforts related to implementation of the Federal Digital System (FDsys) and the annual audit of GPO's financial statement.

OAI's significant accomplishments during this reporting period include the following:

- An audit of the agency's ethics program showed that GPO does not have an established ethics program consistent with Federal Government best practices. A majority of Agency employees who completed a survey on GPO's ethical climate and the effectiveness of the ethics program did not believe or were unsure whether GPO's culture and atmosphere promote ethical behavior and conduct. The audit report recommended that the Agency require employees to undergo regular ethics training and update Agency ethics policies to reflect Federal Government best practices.
- An audit of control and accountability of laptop computers showed that GPO could not account for between 150 and 213 laptops issued to personnel

between 2005 and 2009. The audit further showed that GPO could not account for the laptops in part because management did not establish standard operating procedures to implement written policies on property control and accountability for laptops. The audit report recommended that management develop standard operating procedures for laptop acquisition, management, and cradle-to-grave inventory tracking.

- An audit of IT controls over GPO's Secure Card Personalization System (SECAPS) identified opportunities to strengthen IT security controls and further reduce the potential risk of system compromise.
- Continued to oversee the efforts of American Systems as it conducted IV&V for the public release of FDsys. We issued two quarterly reports during this reporting period that provided observations and concerns on the program's technical, schedule, and cost risks as well as requirements traceability of those risks and the effectiveness of the program management processes in controlling risk avoidance.
- Completed our oversight responsibilities with respect to GPO's annual financial statement audit for which the Agency received an unqualified opinion from the Independent Public Accounting (IPA) firm of KPMG, LLP (KPMG).

The Office of Investigations (OI) opened 7 investigations and 33 complaints for preliminary

investigation, while closing 9 investigations and 46 complaints. At the end of this reporting period, OI had 31 ongoing investigations and 3 complaints. Seven investigations and 14 complaints were referred to GPO management for information or appropriate action.

More than 70 percent of the ongoing investigations involve allegations of procurement fraud. That number reflects continuing OI efforts to identify and investigate contract and financial fraud within GPO. This past reporting period, as a result of referrals from OI, GPO debarred seven entities from doing business with the Agency. OI also referred to the GPO Office of General Counsel for consideration of suspension/debarment the findings of two investigations involving allegations against an additional five entities.

The Department of Justice (DOJ), including its Antitrust Division, continues to work with OI on ongoing investigations into allegations of false statements, false claims, and collusive bidding. In furtherance of those investigations and others, the IG issued 28 subpoenas for documents this reporting period.

OI's significant accomplishments during this reporting period include:

- As a result of OI referrals, five employees were suspended for violating GPO directives.
- One subject in an ongoing criminal investigation pled guilty to one count of making false statements.
- OI issued two Management Implication Reports concerning management of night shift employees within Plant Operations and management of GPO surplus property.

The Office of Administration/Legal Counsel (OALC) provides legal advice and counsel on issues arising during audits, inspections, and investigations, including opinions regarding legal accuracy and sufficiency of OIG reports. OALC manages administrative and management issues as well as congressional and media relations and requests for information. OALC reviews and edits audit, inspection, and investigative reports before IG approval.

During this reporting period, OALC accomplished the following:

- Reviewed, edited, and approved 28 IG subpoenas; reviewed and edited 5 audit reports and 7 reports of investigation.

- Updated and issued an information security policy for the OIG.
- Coordinated and led an informal internal review of OIG operations against the Quality Standards for Federal OIGs.
- Coordinated and led a review of the GPO OIG Web site and proposed changes designed to enhance communications with our stakeholders and the public.
- Supported the IG in his role as the Chair of the Legislation Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE) in reviewing and analyzing proposed legislation affecting the IG community, soliciting comments, and drafting letters and informal comments for members of Congress.
- Acted on a variety of matters as the OIG liaison to the GPO General Counsel and the GPO Office of the Chief of Staff, including support with GPO litigation and personnel action matters.

OIG MANAGEMENT INITIATIVES

During this reporting period, the OIG underwent peer reviews of its audit and investigation functions. We are pleased to report, as noted in Appendix D, that both functions passed their peer reviews, meaning that both OAI and OI are performing their duties in compliance with applicable professional standards. Assistant Inspector General for Audits and Inspections, Kevin Carson, and Assistant Inspector General for Investigations, Matthew Elliott, are to be commended for their efforts to continuously improve their operations to reflect the high standards of the IG community.

After the peer reviews were conducted, the IG encouraged OIG management to undergo an informal, internal review of the OIG against the standards set out in the Quality Standards for Federal OIGs, known as the Silver Book. The quality standards for management, operation, and conduct of Federal OIGs were developed by the President's Council/Executive Council on Integrity and Efficiency, now renamed the Council of the Inspectors General on Integrity and Efficiency. Although these reviews are not mandatory, our informal review identified various issues that would result in improved and more

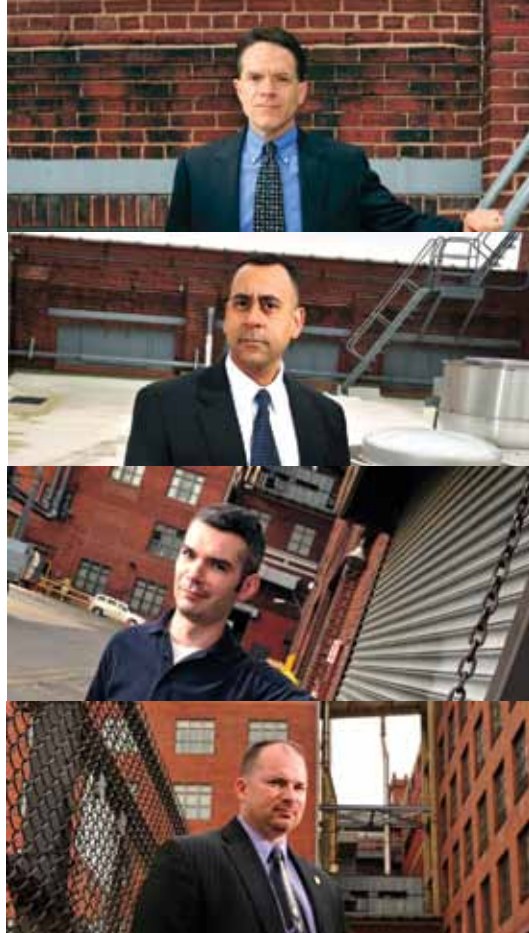
efficient and effective operations. We plan to address the issues during the upcoming reporting period.

Finally, during this reporting period, we reviewed the GPO OIG's Web site to determine the changes necessary to better explain the role of the IG and its functions, enable better external communications with our stakeholders and the public, and encourage more secure communications with potential complainants. As a result, we made recommendations to the Agency's Webmaster and expect to have a revised Web site during the upcoming reporting period.

PERSONNEL UPDATE

During this reporting period, Douglas Bonaro and LeRoy (Lee) Barnhill Jr. joined OI as Supervisory Special Agents. Both recently retired as officers from the Air Force Office of Special Investigations and bring more than 30 years of combined law enforcement experience to the OIG. Before joining OI, Douglas was a Special Agent with the OIG at the Department of Commerce. Douglas has a master's degree in the forensic sciences from The George Washington University and received a Bronze Star for his investigative efforts in Operation Iraqi Freedom. LeRoy has a master's degree in Business and Organizational Security Management from Webster University and before retiring from the Air Force Office of Special Investigations he commanded the Department of Defense's Criminal Investigative Task Force, Iraq.

Michael Cravens and Erik Duncan also joined OI this reporting period as Special Agents. Michael retired from the Air Force Office of Special Investigations as a senior enlisted Special Agent and brings more than 20 years of law enforcement experience to OI. Just prior to joining the OIG, Michael was a Special Agent detailed to the U.S. Army Criminal Investigation Division and assigned to the Criminal Investigation Task Force. Erik served for 4 years as an active duty Special Agent with the U.S. Army Criminal Investigation Division before joining OI. Michael has a master's degree in Security Management from Bellevue University, and both Michael and Erik are combat veterans who served honorably in Iraq and other locations overseas.



Douglas Bonaro, LeRoy (Lee) Barnhill, Jr., Erik Duncan and Michael Cravens.

COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

On October 14, 2008, the IG Reform Act of 2008, Public Law 110-409, established the CIGIE. The CIGIE addresses integrity, economy, and effectiveness issues that transcend individual Government agencies and helps increase professionalism and the effectiveness of personnel by developing policies, standards, and approaches aiding in establishing a well-trained and highly skilled workforce in OIGs. The GPO OIG—along with other legislative branch OIGs—is a member of CIGIE.

The role of the CIGIE includes identifying, reviewing, and discussing areas of weakness and vulnerability in Federal programs and operations for fraud, waste, and abuse, and developing plans for coordinated Government-wide activities that address those problems and promote economy and efficiency in Federal programs and operations.

In May 2009, the IG at GPO was elected to serve

a 2-year term as Chairman of the CIGIE Legislation Committee. The Legislation Committee provides the IG community with helpful and timely information about congressional initiatives. The Committee also solicits the IG community's views and concerns in response to congressional initiatives and requests, and presents views and recommendations to congressional entities and the Office of Management and Budget (OMB).

On behalf of the CIGIE Legislation Committee, the IG kept CIGIE members informed about legislation affecting the IG community through monthly newsletters and communicated with several congressional committees on various legislative matters affecting the IG community, in particular regarding proposed amendments to the Paperwork Reduction Act and the Computer Matching Act. Those proposed amendments would exempt IGs from burdensome review and approval processes by third parties and would facilitate easier collection of information from non-Federal persons and the identification of fraud in Federal assistance payment and other programs.

In addition to participating in CIGIE meetings and events, legislative branch IGs meet regularly to promote communication, cooperation, and coordination with one another on an informal basis. During this reporting period, the IGs of the Architect of the Capitol and House of Representatives hosted meetings in which the following issues were discussed and are undergoing consideration.

- Shared training opportunities for legislative branch OIG personnel.
- Cross-cutting legislative branch audits and inspections.
- Model performance criteria and standards.
- Information technology issues and solutions.
- Legislative issues affecting the legislative branch OIG offices.

REVIEW OF LEGISLATION AND REGULATIONS

The OIG, in fulfilling its obligations under the IG Act, reviews existing and proposed legislation and regulations relating to programs and operations at GPO. It then reports in each semiannual report the impact

of legislation or regulations on the economy and efficiency of programs and operations administered or financed by GPO.

During this reporting period, four legislative proposals relating to GPO programs and operations were introduced in Congress, particularly to defund the Agency or curtail or eliminate the printing of bills or the *Congressional Record*. On January 26, 2011, Senator Rand Paul of Kentucky introduced Senate Bill 162 (S. 162), the Cut Federal Spending Act of 2011, which would defund GPO. S. 162 is currently on the Senate Calendar. On January 12, 2011, former Representative Christopher Lee of New York introduced House of Representatives Bill 292 (H.R. 292), the Stop the Overprinting (STOP) Act. H.R. 292 would eliminate mandatory printing of congressional bills and resolutions for members of Congress and require that they be available "only in an electronic format which is accessible through the Internet." The House of Representatives passed H.R. 292 by a vote of 399-0, and it was referred to the Senate. On January 26, 2011, Senator Thomas Coburn of Oklahoma introduced a companion bill, Senate Bill 210, which was referred to the Committee on Rules and Administration.

On March 30, 2011, Senator Coburn introduced Senate Bill 674 (S. 674), the *Congressional Record* Printing Savings Act of 2011. S. 674 would limit the printing of the Congressional Record to those copies required for "archival purposes" and require that the Congressional Record be available to the public on the GPO Web site in a format that enables downloading and printing.

These legislative proposals would require GPO to rely less on traditional printing of congressional documents, as statute requires, and more on providing cost-effective, electronic dissemination of congressional information. The impact of this legislation would primarily affect GPO's Official Journals of Government operation, which oversees printing and publication of the *Congressional Record*, *Federal Register*, and bills and resolutions. In fiscal year (FY) 2010, GPO received approximately \$94 million in appropriations for congressional printing and binding, of which approximately \$25 million was for *Congressional Record* products and \$6 million for bills, resolutions, and amendments.

GPO MANAGEMENT CHALLENGES



The Government Performance and Results Act (GPRA) Modernization Act of 2010 defines major management challenge as “programs or management functions, within . . . agencies, that have greater vulnerability to waste, fraud, abuse, and mismanagement where a failure to perform well could seriously affect the ability of an agency or the Government to achieve its mission or goals.” With this new definition, we update the list of management challenges we believe are critical for the Agency to address.

1. CUSTOMER SERVICE

To achieve its objectives as a 21st Century information processing and dissemination operation, GPO management must maintain the appropriate focus, staffing, and alignment with the Agency’s Strategic Vision. During this reporting period, the Agency updated the goals of its Strategic Plan. Its first goal is “It’s All About the Customer”—to “understand, anticipate and meet the needs” of its customers. The Agency’s second goal is to promote a more open and transparent Government by working with its customers to disseminate information through the use of all available technology. The culture and focus of customer service efforts must reflect a new way of thinking, and customers should come to GPO because they want to—not

GPO’S TOP 10 MANAGEMENT CHALLENGES

1. Customer Service.
2. Human Capital Operations and Management.
3. Federal Digital System.
4. Information Technology Security Management.
5. Acquisitions and Print Procurement.
6. Continuity of Operations.
7. Internal Controls.
8. Protection of Sensitive Information.
9. Financial Management and Performance.
10. Sustainable Environmental Stewardship.

because they must. Transformation of the traditional GPO customer relationship requires a continuing evolution toward what the Agency has called “world-class customer service.”

During this reporting period, Congress introduced various bills to reduce or eliminate printing of the *Congressional Record* and bills or resolutions as cost-saving measures. The winner of the President’s 2010 SAVE Award [Securing Americans’ Value and Efficiency Award] suggested that GPO cease printing and mailing thousands of copies of the *Federal Register* because most customers use the online version. During this challenging fiscal time, more than



ever GPO customers will be looking for cost-effective products. This presents an opportunity for GPO to continuously evolve and provide customers with cost-effective services and technologically advanced methods of information dissemination.

One continuing challenge for GPO in providing “world-class customer service” is customer agency billing and payments. Since 2001, GPO has relied in large part on the Department of Treasury’s Intra-governmental Payment and Collection (IPAC), an electronic Internet-based collection and payment system for Federal agencies, to bill customer agencies for printing services. In the normal order and billing process, GPO first receives a request from a customer agency for printing and/or binding on a Standard Form (SF)-1, “Request for Printing and Binding.” GPO awards a contract to a vendor/contractor to provide the printing. The print job is then delivered to the customer agency, and, after paying the contractor, GPO prepares the IPAC transaction documents to charge the agency. At the end of each month, GPO personnel access IPAC and retrieve the total costs due. IPAC transactions immediately affect GPO’s revolving fund and the customer agency’s respective accounts in the U.S. Treasury.

In 2004, the OIG reviewed the emerging issue of “chargebacks” by customer agencies, that is, agencies

taking back funds electronically through IPAC from GPO’s Revolving Fund. In FY 2004, the level of chargebacks exceeded \$24 million. Our review found that incorrect customer billing code information, lack of purchase order documentation available to the agencies, and lax IPAC controls over chargebacks by customer agencies contributed to the problem. We specifically found that the “amount of staff time and resources expended—by both GPO and customer agencies—in performing duplicative activities, processes, or functions by having to re-charge agencies for appropriate costs is both inefficient and a waste of federal funds.” Management accepted our recommendations to resolve these issues.

Unfortunately, the chargeback problem has not abated. In fact, as of March 2011, the IPAC chargeback balance exceeds \$28 million. In April 2008, the IPAC chargeback balance was approximately \$29 million. GPO management conducted a chargeback analysis during this reporting period. Based on at least seven previous studies or reviews on this issue (including our 2004 report), GPO management found that chargebacks are a “symptom of numerous process breakdowns,” including incorrect order and billing information, inadequate and ineffective communication both inside the Agency on how to resolve this issue and outside with customers on how to provide correct order and billing information.¹

One troubling finding is that GPO frequently double-bills customer agencies and “no root cause has been discovered.” Such practices, the management analysis found, “impacts GPO’s ability to provide effective customer service . . . and damages relationships with customer agencies.”

The management analysis provides a general framework on how to move forward to tackle the chargebacks issue both in the short-term and long-term. The OIG intends to ask KPMG, the independent financial statement auditor, to once again review this issue as part of this fiscal year’s financial statement audit.

¹ An April 2007 GPO survey of agency customers found that almost 46 percent were “dissatisfied” with GPO’s billing process.

2. HUMAN CAPITAL OPERATIONS AND MANAGEMENT

The issues facing Human Capital (HC) operations and management at GPO have been identified as a significant management challenge for several semiannual reporting periods. HC operations are at the heart of effectively accomplishing an agency's mission. In essence, HC provides services necessary to recruit, hire, develop, and retain the most precious and important source of productivity—its employees.

The Government Accountability Office (GAO) identified four critical areas related to Strategic HC Management that the OIG believes are relevant to GPO:

- **Leadership.** Top leadership must provide committed and inspired attention needed to address human capital transformation issues.
- **Strategic Human Capital Planning.** HC planning efforts must be fully integrated with mission and critical program goals.
- **Acquiring, Developing, and Recruiting Talent.** Agencies need to augment strategies to recruit, hire, develop, and retain talent.
- **Results-oriented Organizational Cultures.** Organizational cultures must promote high performance and accountability, empower and include employees in setting and accomplishing programmatic goals, and develop and maintain inclusive and diverse workforces reflective of all segments of society.²

We are encouraged that during this reporting period, HC continued implementing a reorganization plan and added new staff to address the four areas that GAO cites to transform HC operations and management. During the previous reporting period, the Office of Personnel Management (OPM) issued audit findings about GPO's delegated competitive examining (DE) operations. OPM found that while most of the DE operations are being conducted compliantly, a "lack of a viable accountability system" contributed to two illegal appointments and resulted "in inconsistent operations as well as inefficiencies."

² GAO Report GAO-09-632T, <http://www.gao.gov/new.items/d09632t.pdf>.

Among the significant findings of the OPM audit were that GPO (1) did not have a fully functioning accountability system that ensures efficient and compliant DE operations; (2) had significant problems in transaction processing, particularly regarding the critical "on-boarding process" that establishes new hires; (3) lacks consistent updated guidance concerning DE processes; (4) used HC Specialists in DE work before completing certification training, which is prohibited by the Interagency DE Agreement with OPM; and (5) did not use annual trend data regarding opportunities to hire veterans, or the results of annual self-audits to improve program operations.

HC management acknowledged problems with timeliness and accuracy in its operations, particularly the time it takes from position announcement to on-boarding and transaction processing. HC management is addressing those issues, in part, through implementation of EmpowHR, an electronic system of HC processing, and by establishing employee performance goals that emphasize accuracy, timeliness, and customer service. We believe that for HC to successfully transform to a high-performing business unit, it must produce a change in its culture to achieve results-oriented, customer-focused, and collaborative HC solutions.

We also believe that the Agency faces challenges in effectively managing its workforce during a time when fiscal austerity and lean operations will be of paramount importance to the Agency. Our ongoing audit of payroll operations uncovered a significant level of overtime pay and employees on Leave Without Pay (LWOP) and Absent Without Leave (AWOL). In FY 2009, GPO expended \$9.5 million in overtime pay and almost \$11 million during FY 2010. Those totals amount to almost 4 percent of total payroll in FY 2009 and 4.6 percent in FY 2010. In addition, the number of employees on LWOP for significant periods of time has remained above 400 during both FY 2009 and FY 2010, a remarkable 20 percent of the workforce at GPO. In FY 2010, 413 employees were on LWOP for a total of 56,715 hours, or 7,089 days. Finally, a high number of employees were also listed as AWOL during the past two fiscal years: 114 in FY 2009 for a total of 5,983 hours and 83 in FY 2010 for a total of 4,804 hours.

As part of our payroll audit, the results of which we expect to issue during upcoming reporting periods, we will be looking at the reasons for elevated levels of overtime, LWOP, and AWOL and making recommendations on how to effectively manage and decrease these labor costs and the resulting loss of productivity.

3. FEDERAL DIGITAL SYSTEM

The Federal Digital System (FDsys) was originally designed to be a comprehensive information life-cycle management system that will ingest, preserve, provide access to, and deliver content from the three branches of the Federal Government. The system is envisioned as a comprehensive, systematic, and dynamic means of preserving electronic content free from dependence on specific hardware and/or software. Because FDsys replaces GPO Access as the Agency's official information management system for electronic Government documents, the Agency must ensure that the system is robust, effective, and provides as much functionality

as the increasing demands of electronic Government information require.³

FDsys has three major subsystems: the content management subsystem, the content preservation subsystem (accessible to GPO internal users only), and the access subsystem for public content access and dissemination. A multi-year, multi-release integration effort is being used to design, procure, develop, integrate, and deploy selected technologies and components of FDsys.

The OIG is responsible for Independent Verification & Validation (IV&V) work associated with developing and implementing FDsys. Under the supervision and direction of the OIG, American Systems conducts independent programmatic and technical evaluations of the FDsys program to verify whether system implementation is consistent

³ In June 1994, GPO launched GPO Access, which provides online access to information from all three branches of the Federal Government.



with the FDsys project and cost plan and meets GPO requirements. Additionally, IV&V monitors development and program management practices and processes to anticipate potential issues and validates its findings through quarterly reports.

Background

The FDsys program has undergone substantial changes since its inception. During the fall of 2007, the schedule and scope for the first release was changed significantly and a final release with a reduced scope was planned for late 2008. In early 2008, GPO implemented a reorganization of the program with respect to Government and contractor participation and responsibilities, and implemented a new design for FDsys. The GPO FDsys Program Management Office (PMO) assumed the role of the Master Integrator previously held by a contractor. The PMO also assumed the responsibility for designing and managing system development. The original Master Integrator contractor and other contractors were assigned system development roles under the overall guidance of the PMO.

In January 2009, GPO deployed a public beta version of the FDsys access subsystem, containing 8 of the 55 data collections in the GPO Access system. The content management and content preservation subsystems was released in late March 2009. Since deployment, the PMO has continued to update/upgrade the beta system and correct deficiencies identified during testing. In September 2010, the PMO announced that Release 1 was complete. However, while all coding and development was complete, several tasks remained outstanding, including completion of a Continuity of Operations (COOP) Instance and completion of a number of testing activities, including performance testing. In December 2010, the Public Printer announced that FDsys was the “official system of record” for GPO, 3 and one-half years later than originally planned.

Current OIG Concerns

Reduced Functionality. The declaration of FDsys as GPO’s “official system of record” signified that all of the official versions of GPO content, along with the source data, resided in and was available in FDsys.

Nevertheless, many of the services and functionality envisioned in Release 1, such as Library community requirements, have not been realized.

The initial requirements to be contained within Release 1 (for June 2007) totaled 1,835. When FDsys was declared GPO’s official system of record in December 2010, the systems contained approximately 1,171 requirements, which was substantially less functionality than originally anticipated. In addition, at the end of this reporting period, there were 715 Program Tracking Reports (PTRs) documenting issues with the system. A majority of these were attributable to Release 1. Addressing that many problems will require diverting resources that could otherwise be used on further development of requirements.

Quality: Inconsistent and Incomplete Testing. A continuing concern for the FDsys program is the quality of the deployed system. Reliable testing is important to determine if FDsys can function appropriately and effectively as it receives more traffic from users. Though the testing effort has improved, it is maligned due to incomplete requirements and resource issues.

The initial System and Integration Testing did not adequately test the Release 1 system requirements, and did not encompass all the functionality and capabilities incorporated into the deployed system. For example, Section 508⁴ compliance testing was only partially successful and the more difficult Section 508 compliance testing requirements are still outstanding. Furthermore, testing verification was

⁴ Section 508 of the Rehabilitation Act of 1973, as amended (title 29, section 794d of the United States Code) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Although Section 508 does not apply to GPO, the Agency has voluntarily adopted its requirements.

not completed, thus making it impossible to determine the percentage of tests that passed or failed or whether all of the allocated requirements were successfully tested.

Increased Costs. The total FDsys contract costs incurred as of the end of February 2011 was approximately \$45 million. Most of those costs were attributable to Release 1. The original contract to design and develop Release 1 was approximately \$16 million. Substantial investments will continue to be required to complete the FDsys that was originally envisioned. Additionally, one of the goals of FDsys was to replace GPO Access. As this has taken longer than anticipated, it has necessitated the need for GPO Access to remain operational. Therefore, GPO is running GPO Access in parallel at a significant cost to the Agency. The Agency now estimates that GPO Access will become an archive-only system in Spring 2011, and fully retired in late 2011.

Inadequate Program Management. The FDsys program lacks program management experience and does not consistently use proven and accepted standard program management practices. The PMO has not embraced techniques that would give the program more insight into progress, enabling better management and better opportunity for successful deployment within scope, cost, schedule, and quality goals. For example, while the PMO committed in response to an OIG recommendation to use Earned Value (EV) analysis to measure progress against cost and schedule, they have not done so. If used effectively, EV can provide an early warning of project performance problems while time is available for corrective action.

While continuing to have concerns regarding implementation of FDsys, we don't want to imply that the FDsys program lacks effort or has failed to produce a viable product. The FDsys Release 1 has received praise and notoriety for its look, feel, and ease of use. The PMO has also dealt with external commitments/requests (for example, availability of bulk data) that have altered internal priorities and resulted in the delay of work on the development of all the capabilities envisioned for the release. In addition, the migration of data from GPO Access to

FDsys has been an extremely difficult undertaking and required more time and resources than the PMO originally anticipated.

We continue to believe that the primary challenges for the FDsys program are in the areas of program management, system engineering leadership, technical direction, and an adequate test program for the FDsys system. The goal of our on-going IV&V work is to report key risks and issues to the PMO and management and provide value-added recommendations that will help mitigate risks.

4. INFORMATION TECHNOLOGY SECURITY MANAGEMENT

Because GPO provides services to executive branch agencies that must comply with the Federal Information Security Management Act (FISMA) of 2002, GPO chose to substantially comply with the principles of the Act. The purpose of FISMA is to improve information security at Government agencies and Government contractors. Complying with FISMA continues to present additional challenges for GPO, including protecting sensitive Agency systems, information, and data.

During FY 2007, the OIG conducted a baseline assessment of compliance with FISMA to identify any gaps and deficiencies in GPO's overall information security program, including critical systems. We



completed a full FISMA assessment in FY 2009. The scope included evaluating GPO progress in complying with FISMA based on the 2007 assessment. Our most recent assessment noted that while GPO has made some progress in complying with FISMA, additional improvements are needed. During this reporting period, the Information Technology and Systems (IT&S) office continued to make progress in addressing recommendations made in our 2009 assessment.

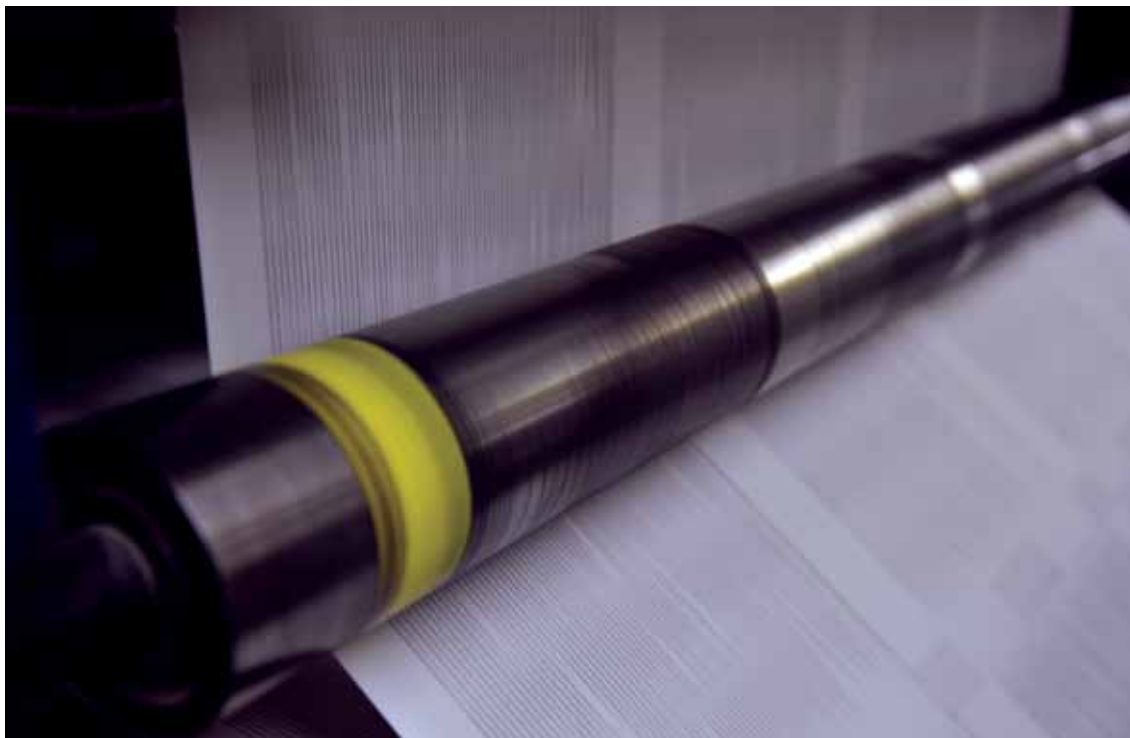
The Federal Government is shifting its IT security strategy from periodic security reviews to continuously monitoring and remediating IT security vulnerabilities. In February 2010, the National Institute of Standards and Technology (NIST) published Special Publication 800-37 Revision 1; *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*. The publication transformed the traditional Certification and Accreditation (C&A) process, which required detailed audits and inventories of Federal agency information systems. While providing a baseline of security controls for information assets, the C&A process did not address the

real-time nature of threats to information systems.

We plan to initiate our next assessment of GPO's compliance with FISMA in late 2011. Our assessment approach will integrate the new NIST risk management framework and include an evaluation of GPO's ability to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

5. ACQUISITIONS AND PRINT PROCUREMENT

Acquiring goods and services and procuring printing on behalf of the executive branch remain critical challenges as GPO strives to transform the Agency and meet the changing needs of its customers. During FY 2010, GPO procured goods and services valued at more than \$600 million, approximately two-thirds of the Agency's consolidated expenses. Given this financial vulnerability, we are concerned that GPO has not fully assessed its acquisition programs to identify critical performance and oversight issues.



In 2008, OMB issued guidance to executive branch agencies on conducting internal reviews of the acquisition function required under OMB Circular No. A-123. Although not required to follow those guidelines, GPO manages and oversees procurement and production of printing on behalf of its executive branch customers. We, therefore, believe GPO (and its customers) would benefit greatly from an internal review of Customer Services (formerly Print Procurement) and Acquisition Services. In his June 7, 2010, letter to Congress, the former Public Printer stated that GPO would finish an independent assessment of Acquisition Services by the end of FY 2010. The OIG recently became aware that GPO has not conducted any such assessment. Agency management stated, however, that it plans to conduct an assessment in the near future.

GPO also faces ongoing challenges with Agency contract management, as evidenced in part by our ongoing audit of FDSys contract administration and our continuing procurement fraud investigations. The rise in procurement fraud-related investigations and referrals by OI for suspension and debarment consideration further illustrate the need for greater contract oversight and contract officer training. During this reporting period, OI referred to management four complaints related to failures by contractors to follow the terms of GPO contracts. Through more efficient contract management and greater use of administrative contract remedies, GPO might have avoided the violations substantiated in those complaints. OI did not receive any formal response to those referrals.

Improving acquisitions by strengthening accountability, eliminating waste, improving performance, and targeting fraud and mismanagement are all necessary to protect the best interests of the taxpayers. In a time of budget cuts and constraints, GPO must do its part to effectively manage and protect procurement funds.

6. CONTINUITY OF OPERATIONS

GPO's ability to continue its mission essential functions during a disruption in operations continues to be a significant area of concern. GPO Directive 825.40, "Continuity of Operations Plan (COOP),"

dated November 21, 2008, states that the agency established a COOP plan to provide for continuation of the Agency's essential functions and operations. The plan requires that activities be operational within 12 hours and that operations be sustained for up to 30 days. The Agency's essential functions are supporting the printing and electronic publishing requirements of Congress and production of the online Federal Register for the Office of the Federal Register, and blank passports for the Department of State.

The Agency has made considerable progress in relation to COOP actions and identified assorted risks and problems that it continues to work to resolve. As of February 2011, there were a total of 25 identified risks and problems. Of the 25, the top 7 strategic risks for GPO include (1) not being able to support Congress at an ad hoc location, (2) not "Day 1" ready for a COOP incident, (3) not prepared for telework, (4) incomplete COOP plans and documentation, (5) insufficient COOP training at all levels, (6) COOP not an essential part of the GPO Strategic Plan, and (7) COOP responsibilities not included in performance plans of key staff personnel. The Agency must continue to address those risks and problems as it moves forward with establishing and ensuring that essential functions can continue during any COOP scenario.

7. INTERNAL CONTROLS

GPO management establishes and maintains a system of internal controls for effective and efficient operations, reliable financial reporting, and compliance with laws and regulations. As the GAO notes in its *Standards of Internal Control in the Federal Government*, internal control "also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud." Almost all OIG audits include assessments of a program, activity, or function's control structure. Agency action to make internal controls the responsibility of all employees, but especially managers, must continue as a priority.

Our audits continue to identify issues related to internal controls. For example, the OIG issued an audit report during this reporting period that identified internal control weaknesses related to controlling

and accounting for Agency-issued laptop computers. The audit identified that the Agency could not account for between 150 and 213 laptops with a total purchase price value of between \$331,500 and \$470,730. Further, Agency management could not provide an explanation as to the location of the missing laptops, in part because management did not establish standard operating procedures to implement written policies on property control and accountability for laptops.

Internal controls within GPO for preventing loss of laptops need improvement, as evidenced by the inability of the Agency to produce reports of either acquisition or disposition of laptops or account for laptops from purchase to final disposition. Such a lack of controls over laptops may have resulted in the inadvertent exposure of sensitive GPO business information about acquisitions and human capital, as well as the manufacture and issuance of security documents such as U.S. passports.

The annual financial statement audit also addresses internal control issues and provides management with recommendations for corrective actions. Although issuing an unqualified opinion on GPO's FY 2010 financial statements, KPMG identified three significant internal control deficiencies, which it did not consider material weaknesses. Those deficiencies

were controls over special journal entries, control over human resource data, and IT general and application controls. Those deficiencies will be followed up on during the FY 2011 financial statement audit, which will begin during the next reporting period.

8. PROTECTION OF SENSITIVE INFORMATION

After several recommendations from this office, GPO has begun to establish rules of conduct and appropriate administrative, technical, and physical safeguards that adequately identify and protect sensitive information. Failure to have such rules and safeguards could result in harm, embarrassment, inconvenience, or unfairness to individuals and GPO, including possible litigation. Of particular importance is the need to safeguard against and respond to any breach of personally identifiable information (PII), including personal information in both information systems and paper documents.

FISMA requires that each agency establish rules of conduct for persons involved with PII, establish safeguards for PII, and maintain accurate, relevant, timely, and complete PII information. As reported in OIG Report 07-09, "GPO Compliance with the Federal



Information Security Management Act (FISMA),” dated September 27, 2007, and again in our FISMA Report 10-03, dated January 12, 2010, GPO is progressing with efforts to protect PII contained in information systems. GPO Directive 825.41, “Protection of Personally Identifiable Information,” issued March 30, 2010, establishes a framework for protecting PII at GPO.

In response to recommendations included in a February 2009 Management Implication Report regarding the handling of PII, the Public Printer appointed a senior-level manager as Privacy Officer (PO). GPO also hired a new privacy program manager to help the PO implement GPO Directive 825.41. Our next FISMA assessment, which is scheduled to begin in late 2011, will evaluate GPO’s implementation of GPO Directive 825.41 to protect sensitive information.

9. FINANCIAL MANAGEMENT AND PERFORMANCE

Federal agencies continue to face challenges providing timely, accurate, and useful financial information and managing results. Better budget and performance integration has become even more critical for results-

oriented management and efficient allocation of scarce resources. OIG auditors and contractors they oversee are vital in keeping the Federal Government’s financial information and reporting transparent, valid, and useful to agency decision-makers and other stakeholders.

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG conducted the FY 2010 audit under a multiyear contract for which OAI serves as the Contracting Officer’s Technical Representative (COTR). KPMG issued an unqualified opinion on GPO’s FY 2010 financial statements, stating that the Agency’s financial statements were fairly presented, in all material respects, and in conformity with generally accepted accounting principles. KPMG identified three significant deficiencies, which it did not consider material weaknesses. Those deficiencies were: (1) controls over special journal entries, (2) control over human resource data, and (3) IT general and application controls.

Although not affecting the audit opinion, some issues continue to hamper the Agency with respect to financial management and performance. For example, as mentioned in the “Customer Service”



management challenge, customer agency billing and payments continues to be an issue, which potentially affects the Agency's financial performance. Specifically, as of March 2011, the IPAC chargeback balance is more than \$28 million.

The Agency stated in its 2010 Financial Statements that GPO billed customers about \$958 million for printing and binding services, including congressional services funded by appropriations, during FY 2010. The U.S. Department of the Treasury's IPAC System was used to collect about \$741.5 million, or 77.4 percent of this debt from customers. Additionally, about \$77.4 million, or 8.1 percent of this debt, was collected from funds held in customer Printing and Binding Deposit Accounts maintained by GPO and another \$17.2 million, or 1.8 percent, was collected through credit card transactions. Such electronic-based methods allow prompt collection of funds, rather than the more traditional methods of collection.

In January 2009, however, KPMG wrote in its management letter of the financial audit that internal controls over the IPAC billing process needed to be strengthened. KPMG observed that the major reason for the chargebacks was that GPO "is not gathering and/or validating key customer billing information" in the ordering process, which causes the agency being billed to reject the IPAC invoice. KPMG noted that the chargeback problem could "overstate accounts receivable in the consolidated financial statement" and also takes an inordinate amount of time and resources to investigate and resolve.

IPAC chargebacks, included in accounts receivable, totaled approximately \$26.4 million at the end of FY 2010 and were approximately \$28 million as of the end of this reporting period. The OIG intends to request that KPMG revisit this issue as part of its FY 2011 financial statement audit.

Finally, we note that the Improper Payments Elimination Improvement Act was signed into law on July 22, 2010. The 2010 Act amends the Improper Payments Information Act of 2002 by requiring that executive branch agencies periodically identify and review programs and activities susceptible to significant improper payments and report on actions that would reduce or recover improper payments in accordance with guidance OMB plans to issue.



Although GPO is not covered by law, we urge management to undertake this type of review so that it can develop actions that will reduce or recover improper payments. We expect to review efforts by the Agency in this area in the future.

10. SUSTAINABLE ENVIRONMENTAL STEWARDSHIP

As the largest industrial manufacturer in the District of Columbia, GPO has always faced challenges to become more environmentally sensitive. The Public Printer has made environmental stewardship and a sustainable future Agency goals and committed to integrate environmental values into GPO processes.

We continue to urge adoption of principles consistent with sustainable environmental stewardship objectives. First, we encourage management and Congress to renew efforts to evaluate a new facility that would more appropriately meet Agency needs and be more energy efficient. A more energy efficient and environmentally conscious facility not only fits with the Agency's environmental stewardship initiative but also meets the environmental and economic

objectives for Congress and the Administration.

We also continue to encourage management to promote and incorporate “green thinking” into all of its business processes through performance metrics, reward programs, and other means. For example, the OIG has recommended an integrated approach to green acquisition such as that espoused in Executive Order 13514, which sets sustainability goals for Federal agencies and focuses on making improvements in their environmental, energy, and economic performance. Although not required to adhere to the Executive Order, we believe that it is beneficial for management to adopt its tenets and develop written policies for purchasing environmentally sustainable goods and services, monitor compliance annually and fix shortcomings, and provide training on making purchases that are environmentally sound and comply with the spirit of the order.

In our previous report, we noted that GPO’s former environmental executive recommended issues to explore with GPO’s legislative branch counterparts, including:

- Consolidating waste-hauling contracts to obtain a more favorable rate for recycled goods as well as ensure that each agency can participate in recycling efforts.
- Consolidating standard goods purchasing, such as cafeteria supplies, cleaning chemicals, and paper (in all its forms), to reduce cost and ensure each agency is using the “greenest” products available.
- Sharing service contracts to achieve economies of scale and uniformity throughout legislative branch agencies.

To meet those challenges, GPO should have a dedicated environmental executive who will address the issues across Agency business units and directly with officials in other legislative branch agencies.

We have included in our work plan a review of energy use at GPO to determine whether a comprehensive plan exists for implementing energy-related projects, as part of an overall plan that helps reduce emissions, energy consumption, and energy costs. We hope to begin the audit in the near future and look forward to working with Agency personnel in

achieving a long-term and sustainable environmental stewardship program.

OFFICE OF AUDITS AND INSPECTIONS



OAI conducts independent and objective performance and financial audits relating to GPO operations and programs, and oversees the annual financial statement audit conducted by an IPA. OAI also conducts short-term inspections and assessments of GPO activities, which generally focus on issues limited in scope and time. Audits are performed in accordance with Government Audit Standards that the Comptroller General of the United States issues. When requested, OAI provides accounting and auditing assistance for both civil and criminal investigations. OAI refers to OI for investigative consideration any irregularities or suspicious conduct detected during audits, inspections, or assessments.

A. SUMMARY OF AUDIT AND INSPECTION ACTIVITY

During this reporting period, OAI issued six new reports and successfully passed a peer review conducted by the Library of Congress (LOC) OIG. OAI also continued its work with management to close open recommendations carried over from previous reporting periods. GPO management made significant progress during this period in closing open audit and assessment recommendations. As a result, as of March 31, 2011, a total of 28 recommendations from previous reporting periods remain open.

B. FINANCIAL STATEMENT AUDIT

(Audit Report 11-04, Issued December 21, 2010)

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG conducted the FY 2010 audit under a multiyear contract for which OAI serves as the COTR. The oversight provided ensures that the audit complies with Government Audit Standards. OAI also assists with facilitating the external auditor's work as well as reviewing the work performed. In addition, OAI provides administrative support to KPMG auditors and coordinates the audit with GPO management.

OIG oversight of KPMG, as differentiated from an audit in accordance with Government Audit Standards, is not intended to enable us to express, and therefore we do not express, an opinion on GPO's financial statements, the effectiveness of internal controls, or compliance with laws and regulations. However, our oversight, as limited to the procedures outlined earlier, disclosed no instances in which KPMG did not comply, in all material respects, with Government Audit Standards.

KPMG issued an unqualified opinion on GPO's FY 2010 financial statements, stating that the Agency's financial statements were fairly presented,

in all material respects, and in conformity with generally accepted accounting principles. KPMG identified three significant deficiencies, which it did not consider to be material weaknesses. Those deficiencies were controls over special journal entries, control over human resource data, and IT general and application controls. KPMG did not disclose any instances of noncompliance with certain provisions of laws, regulations, and other matters required to be reported under Government Audit Standards.

During this reporting period, KPMG was also awarded the contract to perform the 2011 audit of GPO's consolidated financial statements.

C. AUDIT AND INSPECTION REPORTS

1. Audit Report 11-01 (Issued December 16, 2010)

Government Printing Office's Ethics Program

An agency's ethics program is the formalized means by which senior management can educate and enlighten

agency employees and prevent or detect employee misconduct and violations of ethics regulations. An effective ethics program inspires employees not only to comply with ethics regulations, but also fulfill the highest ideals of public service and provide the public with full faith and confidence that the agency's mission, programs, and functions are fair and impartial.

At GPO, the Agency's ethics program is administered by the Office of the General Counsel (OGC). The ethics program must comply with the Ethics in Government Act of 1978, as well as other statutes as described in GPO Instruction 655.3A, "Standards of Conduct for Government Printing Office Officers and Employees," dated June 10, 1988. The instruction establishes the standards of ethical and financial conduct for GPO employees, consultants, advisers, and other special Government employees, and requires that GPO personnel maintain high standards of moral and ethical conduct; consistently exercise honesty, integrity, and impartiality in the performance of their duties; and avoid any actions that might adversely reflect on the Agency.



An audit of the Agency's ethics program was performed to determine whether GPO complied with applicable Federal ethics guidance and the ethics program at GPO was consistent with Federal Government best practices. Although it did not identify specific instances of ethics violations or noncompliance, the audit did find that GPO did not have an established ethics program consistent with Federal Government best practices. For example, OGC did not have written standard operating procedures for routine ethics officer responsibilities; did not always document its handling of ethics-related matters; and has not updated ethics policies, which are between 22 and 38 years old and refer to offices or procedures that no longer exist.

Further, a majority of Agency employees who completed a survey on GPO's ethical climate and the effectiveness of the ethics program did not believe or were unsure whether GPO's culture and atmosphere promote ethical behavior and conduct. As a result, Agency assets and operations may be at greater risk because of potential misconduct and unethical behavior.

In general, the audit recommended that the Agency require employees to undergo regular ethics training, update ethics policies to reflect Federal Government best practices, and improve administration of the ethics program. The recommendations should improve the Agency's ethics program and, in turn, the Agency's overall ethical culture. Management generally concurred with the recommendations and the planned corrective actions are considered to be responsive.

2. Audit Report 11-02 (Issued December 6, 2010)

Control and Accountability of Laptop Computers

Government-issued notebook or laptop computers are at risk of loss and theft because of their high value, portability, and ease of concealment. Because of their ability to store large amounts of data, lost or stolen laptops also create a risk of exposing PII and sensitive Government information. The inability to account for laptops has been prevalent throughout the Federal Government, and the GPO has experienced instances of missing laptops.

The portability of a notebook or laptop computer makes it a useful tool for teleworking and can thus facilitate the important COOP function. GPO issues laptops to about one in four employees. Between 2005 and 2009, GPO records revealed that employees were issued 629 laptops with a total purchase price of \$1,389,855—an average of \$2,210 per laptop.

Due in part to previous investigations of the security and inventory control lapses in the management of Agency laptop computers, we conducted an audit of the control and accountability of laptop computers at GPO. The objectives of the audit were to determine whether GPO could account for all Agency laptop purchases, and had adequate controls in place that would prevent the loss or theft of laptops.

The audit found that based on our testing of a statistical sample of laptops issued to personnel between 2005 and 2009, we estimated with 99-percent confidence that GPO could not account for between 150 and 213 laptops. The total purchase price value of the missing laptops was between \$331,500 and \$470,730. Agency management could not provide an explanation as to the location of the missing laptops. The audit further showed that GPO could not account for the laptops in part because management did not establish standard operating procedures to implement written policies on property control and accountability for laptops.

In addition, internal controls within GPO for preventing the loss of laptops need improvement as evidenced by the inability of the Agency to produce reports of either acquisition or disposition of laptops, or to account for laptops from purchase to final disposition. GPO also did not meet its objectives outlined in GPO Instruction 705.29, "IT End User Asset Management," November 5, 2005, for maintaining a centralized end user asset management program that verifies duplicative purchases are not made, and gathers information for disaster recovery planning. While the actual impact of the missing laptops is not known, failure to adequately account for laptops could have resulted in inadvertent exposure of sensitive GPO business information about acquisitions and human capital as well as the manufacture and issuance of security documents such as U.S. passports.



In general, we made seven recommendations to develop standard operating procedures for laptop acquisition, management, and cradle-to-grave inventory tracking and disposition. If implemented, the recommendations should help improve control and accountability over laptops. Management concurred with each of the report's recommendations and we consider the planned corrective actions responsive to the recommendations.

3. Assessment Report 11-03 (Issued December 15, 2010)

Federal Digital System (FDsys) Independent Verification and Validation – Thirteenth Quarter Report on Risk Management, Issues, and Traceability

The FDsys program is intended to modernize the information collection, processing, and dissemination capabilities GPO performs for the three branches

of the Federal Government. During this reporting period, the OIG continued to oversee the efforts of American Systems as it conducted IV&V for public release of FDsys. As part of its contract with the OIG, American Systems is assessing the state of program management, technical and testing plans, and other efforts related to the rollout of Release 1. The contract requires that American Systems issue a quarterly Risk Management, Issues, and Traceability Report, and provide to the OIG observations and recommendations on the program's technical, schedule, and cost risks as well as requirements traceability of those risks and the effectiveness of the program management processes in controlling risk avoidance.

The thirteenth quarterly report covers the period from August 1, 2010, through October 21, 2010. During the review period, IV&V did not identify any new technical, cost, or schedule risks. The report does, however, discuss issues and concerns brought to management's attention as the PMO implements the remaining efforts to complete Release 1 and shut down GPO Access. The issues and concerns were already encompassed by open recommendations provided to the PMO in previous IV&V Quarterly Reports.

4. Assessment Report 11-05 (Issued March 29, 2011)

Federal Digital System (FDsys) Independent Verification and Validation – Fourteenth Quarter Report on Risk Management, Issues, and Traceability

The fourteenth quarterly report on FDsys covers the period from October 22, 2010, through March 11, 2011. During the fourteenth quarter, FDsys replaced GPO Access as GPO's official system of record. Specifically, on December 20, 2010, the Public Printer approved the declaration that makes FDsys the trusted source of authentic and official Government publications, that is, FDsys is now the GPO's official system of record.

This declaration was made based on the official GPO content being available in FDsys rather than development and fulfillment of specific criteria; there is no Industry Standard or Best Practices to be followed to designate a system as the official system of record.

The PMO developed a Release 1 Master Plan (the Plan), which delineates tasks and activities that had to be completed before designation of FDsys as the official system of record. However, the Plan also depicts a number of tasks not yet completed. For example, the Requirements Traceability Verification Matrix (RTVM) was not completed, and the performance and capacity testing that was demonstrated did not meet one of the key requirements allocated to Release 1. Those items were significant because they demonstrate the stability, extensibility, and availability of the FDsys.

GPO Access will continue to run in concert with FDsys because a number of other tasks still needs to be completed. Those tasks include processing quarantined packages and performance of an audit that will ensure all content was migrated from GPO Access to FDsys.

During the period, IV&V did not identify any new technical, cost, or schedule risks. The report does discuss issues and concerns that we are bringing to management's attention as the PMO implements the remaining efforts to complete Release 1 and shut down GPO Access. The issues and concerns were already encompassed by open recommendations provided to the PMO in previous IV&V Quarterly Reports.

5. Audit Report 11-06 (Issued March 31, 2011)

Secure Card Personalization System Information Technology Security Controls

GPO provides personalized smartcards and identity cards for customers throughout the Federal Government. The Secure Card Personalization System (SECAPS) is the automated system used for producing the cards. SECAPS was developed by GPO through a contract with General Dynamics Information Technology and designed to create personalized embossed identity cards, Homeland Security Presidential Directive No. 12 (HSPD-12) compliant smartcards, and high-frequency radio frequency identification cards. GPO produces cards for the Department of Homeland Security's Customs and Border Protection's Trusted Traveler Program and for the Center for Medicare and Medicaid Services in the Department of Health and Human Services.

SECAPS receives and maintains PII for purposes of card production. Recent breaches of PII at several Federal agencies increased the level of scrutiny over the handling of that type of sensitive information. To help protect against breaches as well as maintain an appropriate level of security, Federal programs must ensure that controls over PII data are in place.

The audit of SECAPS was performed to determine whether a requisite level of IT security controls in SECAPS maintained system integrity, confidentiality, and availability. Specific audit objectives included determining the adequacy of controls associated with the SECAPS operating system, databases, physical security, system interconnections and the transmission of PII, and purging of PII.

We issued a sensitive report that identifies opportunities to strengthen IT security controls and further reduce the potential risk of system compromise. Management concurred with each of the report's recommendations and has either taken or proposed responsive corrective actions.

D. ONGOING WORK

OAI has several audits and assessments ongoing whose results should be published during the next reporting period. Those assignments include:

An audit of GPO's Administration of the FDsys Master Integrator Contract will determine whether



GPO effectively administered the contract. The audit will specifically determine whether GPO adhered to the Materials Management Acquisition Regulation and other applicable laws, rules, regulations, and guidance related to (1) contract award; (2) monitoring of contract performance; (3) contract modifications; (4) verification of costs incurred; and (5) contract closeout.

An audit of the GPO Express Program will evaluate management controls over the program, including whether (1) GPO Express cards were adequately controlled and issued, (2) contract terms between FedEx Kinkos and GPO were complied with, and (3) revenues reflected program activity.

Agency management requested that the OIG assess compliance of GPO's payroll operations with applicable laws, rules, and regulations. The audit will determine whether GPO complied with applicable guidance related to the (1) request and approval of LWOP; (2) request, approval, calculation, and administration of advanced annual leave;

(3) request, approval, calculation, and administration of daily and weekly overtime; (4) calculation and administration of bi-weekly and annual earnings limits and salary caps; and (5) calculation, payment, and administration of the GPO Goal Sharing Program.

An assessment of GPO's Electronic Passport Tracking System Application Controls will evaluate whether application-level controls in the passport inventory tracking system are effective to track and report the status of e-Passport production.

E. STATUS OF OPEN RECOMMENDATIONS

Management officials made progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. For the 28 recommendations still open, a summary of the findings and recommendations, along with the status of actions for implementing the recommendation and OIG comments, follow.



**1. Assessment Report 09-01
(Issued November 4, 2008)**

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability

FINDING

The OIG contracted with American Systems, a company with significant experience in the realm of IV&V for Federal civilian and Defense Agencies, to conduct IV&V for the first public release of FDsys. As part of its contract, the contractor is assessing the state of program management, technical and testing plans, and other efforts related to this public release. The contractor is required to issue to the OIG a quarterly Risk Management, Issues, and Traceability Report providing observations and recommendations on the program's technical, schedule and cost risks, as well as requirements traceability of those risks and the effectiveness of the program management process in controlling risk. During the period the report covers, GPO launched a public beta version of FDsys containing a limited number of collections. This fourth quarterly report provides an overview of the key risks and issues identified by the FDsys IV&V team from April through June 2008, including security requirements and risk management.

RECOMMENDATION

The OIG made five recommendations to management intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

One recommendation remains open for which management continues to work on implementing corrective actions.

**2. Assessment Report 09-03
(Issued December 24, 2008)**

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fifth Quarter

Report on Risk Management, Issues, and Traceability

FINDING

This fifth quarterly report provides an overview of the key risks and issues identified by the FDsys IV&V team from July through September 2008, including those related to the FDsys detail design and system integration testing as well as technical, schedule, and cost risks the program faces.

RECOMMENDATION

The OIG made 10 recommendations to management intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with six of the recommendations, partially concurred with one, and nonconcurred with three. Management proposed responsive corrective actions to six of the recommendations. Although we disagreed with management's position on the remaining four recommendations, we accepted management's proposed alternative corrective actions.

OIG COMMENTS

One recommendation remains open. Management continues to take responsive actions to implement the remaining recommendation.

**3. Assessment Report 09-07
(Issued March 20, 2009)**

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Sixth Quarter Report on Risk Management, Issues, and Traceability

FINDING

This sixth quarterly report provides an overview of the key risks and issues identified by the FDsys IV&V team from October 2008 through January 9, 2009, including security, and the state of program activities required for deployment, as well as technical, schedule, and cost risks.

RECOMMENDATION

The OIG made four recommendations intended to further strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

Two recommendations remain open. Management continues to take responsive actions to implement the two open recommendations.

4. Assessment Report 09-12 (Issued September 30, 2009)

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Seventh Quarter Report on Risk Management, Issues, and Traceability

FINDING

This seventh quarterly report for the period January 1, 2009, through May 8, 2009, identifies critical technical, schedule, and cost risks for the FDsys Program. The report provides a high-level overview of the key risks and issues that IV&V identified during the reporting period. The report also discusses IV&V assessments covering FDsys security and the state of program activities required for deployment performed over the same time period.

RECOMMENDATION

The OIG made 25 recommendations designed to strengthen FDsys program management, particularly for future FDsys releases.

MANAGEMENT COMMENTS

Management generally concurred with all recommendations, with the exception of one, and proposed responsive corrective actions for each.

OIG COMMENTS

A total of nine recommendations remain open for which the OIG and IV&V continue to monitor the status of their implementation.

5. Assessment Report 10-01 (Issued December 2, 2009)

Federal Digital System (FDsys) Independent Verification and Validation – Ninth Quarter Report on Risk Management, Issues, and Traceability

FINDING

This ninth quarterly report for the period July 1, 2009, through September 30, 2009, identifies critical technical, schedule, and cost risks for the FDsys Program. The report provides a high-level overview



Table of Open Recommendations

AUDIT	NUMBER OF OPEN RECOMMENDATIONS	NUMBER OF MONTHS OPEN
09-01 Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability	1	28
09-03 FDsys IV&V – Fifth Quarter Report on Risk Management, Issues, and Traceability	1	27
09-07 FDsys IV&V – Sixth Quarter Report on Risk Management, Issues, and Traceability	2	24
09-12 Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Seventh Quarter Report on Risk Management, Issues, and Traceability	9	18
10-01 FDsys IV&V – Ninth Quarter Report on Risk Management, Issues, and Traceability	2	15
10-03 GPO's Compliance With the Federal Information Security Management Act	13	14

of the key risks and issues that IV&V identified during the reporting period. The report also discusses IV&V assessments covering FDsys security and the state of program activities required for deployment performed over the same time period.

RECOMMENDATION

The OIG made 11 recommendations to management designed to strengthen FDsys management.

MANAGEMENT COMMENTS

Management generally concurred with the recommendations and has either taken or proposed responsive corrective actions.

OIG COMMENTS

Two recommendations remain open for which the OIG and IV&V continue to monitor the status of their implementation.

**6. Assessment Report 10-03
(Issued January 12, 2010)**

GPO's Compliance with the Federal Information Security Management Act

FINDING

FISMA requires that each executive branch agency develop, document, and implement an agency-wide program for providing information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Although a legislative branch agency, GPO recognizes the need to be FISMA compliant because of the services it provides, including services to executive branch agencies.

In FY 2007, the OIG contracted with a consulting firm to perform a baseline assessment of GPO's FISMA compliance and to evaluate the design and

effectiveness of the controls over GPO's information security program, policies, and practices. We completed a full FISMA assessment in FY 2009. The assessment was performed using the most recent applicable FISMA requirements and guidelines published by OMB and NIST. Significant emphasis was placed on evaluating the GPO systems used for providing services to client agencies. The OIG issued a sensitive report concluding that GPO made some progress in complying with FISMA, but that additional improvements are needed. In addition, many of the weaknesses identified during the FY 2007 baseline assessment still exist.

RECOMMENDATION

The OIG made a total of 21 recommendations, which, if implemented, will help further move GPO toward FISMA compliance.

MANAGEMENT COMMENTS

Management concurred with each recommendation and proposed responsive corrective actions.

OIG COMMENTS

Management continues to work with the OIG to implement corrective actions on the remaining 13 open recommendations.

OFFICE OF INVESTIGATIONS



O I receives and evaluates complaints and conducts investigations related to fraud, waste, and abuse in GPO programs and operations. OI is focused on procurement fraud investigations, but also investigates allegations of bribery, false statements, theft, and other employee and contractor misconduct.

Investigations that substantiate violations of Federal law, GPO Directives, or contract terms/specifications may result in administrative sanctions, civil action, or criminal prosecution. Such actions can include employee terminations, contractor debarments, and court-imposed prison terms, probation, fines, or restitution. OI may also issue Management Implication Reports to the Agency that detail systemic problems or vulnerabilities and offer recommendations on how to correct them.

OI also conducts investigations at all GPO locations, including its 15 Regional Printing Procurement Offices and potentially thousands of contract print vendors nationwide. It maintains a close relationship with GPO Security Services and the Uniform Police Branch to coordinate law enforcement efforts impacting GPO. Liaison is also maintained with DOJ, the OIG community, and other law enforcement agencies and organizations.

A. SUMMARY OF INVESTIGATIVE ACTIVITY

At the end of the last reporting period, 17 complaints were open. OI opened 32 new complaint files, of which 6 were opened into full investigations. Additionally, 21 complaints were closed with no action, 4 were referred to other law enforcement organizations, 1 was associated with an active investigation, and 14 were referred to management. At the end of the reporting period, three complaints were open.

At the end of the last reporting period, 33 investigations were open. During this reporting period, seven investigations were opened and nine were closed. Seven of the closed investigations were referred to management, and two were closed with the Agency having taken action.

During the last 6 months, OI made 12 presentations to DOJ officials. Those presentations resulted in 10 criminal declinations, 1 civil declination, and 1 civil acceptance. OI continues to work with DOJ on several ongoing investigations.

The IG issued 28 subpoenas to further ongoing criminal, civil, and administrative investigations. Documents requested included financial records, bid preparations, production records, and agreements among contractors and/or affiliated companies.

B. TYPES OF CASES

Procurement Fraud

OI continues to focus its investigative resources on identifying and investigating procurement fraud. The investigations focus on contractor and GPO employee misconduct that adversely impacts the contracting process. Violations include false statements, false claims, product substitution, collusive bidding, bribery, kickbacks, and financial conflicts of interest. In FY 2010, GPO procured more than \$600 million in goods and services through contracting. That figure includes at least \$450 million in contracts awarded to print contractors selected from a pool of thousands of pre-qualified vendors. OI recognizes print procurement as a significant risk area and procurement fraud investigations represent more than 70 percent of the OI case inventory. Including allegations in complaint status, OI has 24 open procurement investigations.

Workers' Compensation Fraud

OI also investigates GPO employees who allegedly submit false claims or make false statements to receive workers' compensation benefits. Investigations may result in criminal prosecutions, civil recoveries, or administrative action levied against employees by GPO or the Department of Labor. OI has four ongoing investigation involving allegations of workers' compensation fraud.

Employee Misconduct

OI routinely investigates allegations of employee criminal and administrative misconduct. Allegations can be violations of Federal and local laws or failures to follow GPO Directives. Penalties for employee misconduct range from verbal counseling to termination and/or criminal prosecution. OI has one open complaint and three full investigations involving alleged employee misconduct.

Proactive Initiatives

While conducting reactive investigations, OI may identify business units, programs, and/or procurements that are vulnerable to fraud. In those instances, OI may open proactive initiatives to identify whether fraud



or other criminal activity has in fact occurred. The findings of proactive initiatives result in Management Implication Reports or spin-off investigations of procurement fraud, employee misconduct, or other types of violations. OI opened one procurement-related proactive initiative during the last reporting period.

Other Investigations

OI conducts other types of investigations that do not fall into one of the previous categories. Examples of those types of investigations include unauthorized use or access to GPO systems, and requests for information or assistance from outside entities. During this reporting period, OI completed one preliminary investigation at the request of another OIG.

C. SUMMARY OF INVESTIGATIVE ACCOMPLISHMENTS

Criminal and Civil Cases

As previously reported, an OI investigation found evidence that a GPO printing contractor failed to comply with critical contract specifications. The case was subsequently accepted for action by DOJ, and the contractor agreed to pay a \$25,000 settlement of U.S. penalty claims. During this reporting period, the contractor and three officers were debarred from doing business with GPO beginning October 31, 2010, and ending October 31, 2012.

OI continues an investigation into allegations of false statements, false claims, forgery, or bid collusion by GPO print vendors. During the last reporting period, one subject pled guilty to one count of false statements and is pending sentencing. OI has the assistance of the DOJ Antitrust Division, which is in the process of negotiating a plea agreement with a second subject.

OI also continues an investigation of allegations relating to false statements and/or false claims to GPO. During this reporting period OI served 10 subpoenas, and the DOJ Antitrust Division is still evaluating the case for possible criminal or civil action.

OI continues an investigation of allegations relating to false statements and/or false claims to the GPO. During this reporting period, OI served one subpoena and is working with DOJ as they evaluate the case for possible criminal action.

Internal Administrative Cases

OI referred to management the findings of an investigation into allegations that three GPO employees committed time and attendance fraud. The investigation revealed the three employees were absent from GPO for periods of approximately 1 to 4 hours and came back to work intoxicated. Each of the three employees admitted they occasionally exceeded their allotted lunch break and went to strip clubs and drank alcoholic beverages before returning to GPO. Administrative action was proposed against the three employees and their direct supervisor.

During the course of the previous investigation, OI also identified an employee who was allowed to

accrue compensatory time in lieu of overtime in violation of a GPO Directive. The employee maintained a personal record of the compensatory time, which he calculated at a rate of time and a half. OI referred the findings to management, who counseled the employee. OI also referred the information to Finance and Administration who determined that GPO owed the employee \$437.02.

OI referred to management the findings of an investigation into allegations a GPO employee misappropriated and disposed of Government property in violation of GPO Directives. The investigation revealed management allowed the employee to purchase surplus GPO property without proper approval. OI also found that management failed to maintain complete sales records for some purchases made by the employee, including the sale of two forklift trucks for \$50.00. The lack of required documentation prohibited OI from assessing the legitimacy of that purchase.

OI referred to the Office of General Counsel, GPO management, and OAI the findings of an investigation into allegations a manager had a conflict of interest because of previous employment. It was further alleged the employee violated GPO Directives when he changed publication shipment procedures. The investigation found no evidence the manager violated any laws or GPO Directives; however, GPO has no directives pertaining to publication shipment procedures.

OI referred to management the results of an investigation into allegations that prior to being hired a GPO employee made false statements concerning the details of a criminal conviction. OI confirmed that the employee provided false information on his Optional Form (OF) 306, "Declaration for Federal Employment." Additionally, the investigation revealed that after being hired the employee misused his Government-issued travel card. Determination of administrative action is pending.

As previously reported, a GPO employee admitted to knowingly misusing GPO's FedEx account to ship several personal packages over the course of several years. OI referred the findings to management for action, who proposed and sustained a 10-day suspension based on the charge of unauthorized use of Government property.

Also previously reported, an OI investigation substantiated that three employees used a duplicate GPO identification badge to engage in time and attendance fraud. OI referred the case for administrative action and management imposed two 5-day suspensions and one 2-day suspension for failure to cooperate with the GPO Uniformed Police Branch, lack of candor, and inappropriate behavior.

An OI investigation of a GPO employee determined he used his official e-mail to correspond with individuals who subsequently defrauded him of several thousand dollars. OI referred the matter to management for information and appropriate action.

OI also referred to management and OAI the findings of an investigation into allegations that a GPO employee submitted falsified physician's notes to justify his use of Family Medical Leave Act (FMLA)/LWOP. The investigation found no evidence the employee provided false notes; however, the investigation did reveal he used FMLA/LWOP without authorization on numerous occasions over a 3-month period. Administrative action against the employee is pending.

External Administrative Cases

As previously reported, OI referred to the Office of General Counsel for consideration of suspension/debarment the findings of an investigation into allegations that a GPO contractor submitted a fraudulent shipping receipt and invoice to GPO for payment. The investigation revealed the company delivered only a partial shipment, but billed GPO for the full value of the contract. During this reporting period, the contractor and two officers were debarred from doing business with GPO beginning October 31, 2010, and ending October 31, 2013.

OI referred to the Office of General Counsel for consideration of suspension/debarment the findings of the following investigations:

- Allegations that a GPO contractor was operating two businesses from the same location and submitting bids for both companies on the same solicitations. The investigation substantiated that the contractor made false statements to GPO regarding the location of his businesses and submitted bids for both companies on the same solicitations



in violation of GPO contract terms. In addition, the contractor submitted false shipping documentation as a claim for full payment on a contract he knew was incomplete.

- Allegations that a GPO printing contractor submitted falsified Bills of Lading to GPO with invoices for payment. The investigation revealed the contractor altered the shipping dates on 16 Bills of Lading to reflect the materials had been shipped on an earlier date.

OI referred to management the findings of an investigation into allegations that an individual submitted two bids for a fixed-price contract under the names of two different contractors. The investigation substantiated the allegation, but found no other instances that the individual submitted multiple bids for the same GPO solicitation.

OI referred to management information that a GPO vendor defaulted on a contract and then subsequently bid on the resultant re-solicitation as a different company. The OI investigation found no evidence that the vendor made specific false statements to GPO; however, the vendor was found to have violated the requirement for a Certification of Independent Price Determination in GPO Contract Terms.

An OI preliminary investigation into an allegation that a vendor knowingly supplied GPO with inferior ink was found to not have merit. However, as a result of the inquiry, OI identified and referred to management and OAI information concerning paper waste and paper roll mishandling.

D. MANAGEMENT IMPLICATION REPORTS

On November 12, 2010, OI issued a Management Implication Report summarizing concerns and offering recommendations to improve supervisory controls, employee accountability, safety and productivity, and efficient use of human resources in Plant Operations. An OI investigation in part found that Plant Operations management had no general accountability for their second and third shift employees; some supervisors knew that employees frequently were AWOL, but took no disciplinary

action against them; and the second and third shifts are potentially overstaffed, creating the opportunity for employee misconduct.

The OI recommended that management:

- Establish rating criteria in Plant Operations supervisors' performance plans to hold them accountable for managing the performance and conduct of subordinates.
- Develop and implement policies and procedures that define how packers and other Printing Plant workers are used on the second and third shifts and how work is scheduled.
- Require division-level Superintendents to perform and document random inspections of each shift.
- Review staffing and productivity of the different divisions within Plant Operations, to include the number of employees on all shifts, the number of authorized overtime hours, the productivity of each division and shift, and the assignment of work between the shifts.

Although the OIG requested that management respond to the recommendations by January 12, 2011, no Agency response had been issued by the end of this reporting period.

On December 22, 2010, OI issued a Management Implication Report summarizing serious lapses in management of GPO surplus property and offering recommendations to improve the sufficiency of and adherence to GPO Directives. An OI investigation in part found that GPO officials failed to comply with a requirement to report incidents of lost, stolen, or missing property to the Uniform Police Branch; GPO property was disposed of without proper documentation; and GPO Directives pertaining to property disposition either did not exist or needed revision.

The OI recommended that management:

- Hold Property Managers accountable for all improperly disposed property under their control and consider any surplus property disposed of in a manner inconsistent with GPO Directives as misappropriated or stolen.
- Formalize in writing a donation and bidding process for disposing of surplus property items that aligns with 41 CFR § 102.37 and 38, the U.S. General

Services Administration Federal Surplus Personnel Property Program.

- Adopt minimum pricing guidelines that would eliminate subjective and potentially biased pricing methods currently in use.
- Revise and consolidate existing GPO Directives related to surplus property address all outdated, inaccurate, and duplicated information.

Although the OIG requested that management respond to the recommendations by February 22, 2011, no Agency response had been issued by the end of this reporting period.

APPENDICES



APPENDIX A

Glossary And Acronyms

Glossary

Allowable Cost– A cost necessary and reasonable for the proper and efficient administration of a program or activity.

Change in Management Decision– An approved change in the originally agreed-upon corrective action necessary to resolve an IG recommendation.

Disallowed Cost– A questionable cost arising from an IG audit or inspection that management decides should not be charged to the Government.

Disposition– An action that occurs from management’s full implementation of the agreed-upon corrective action and identification of monetary benefits achieved (subject to IG review and approval).

Final Management Decision– A decision rendered by the GPO Resolution Official when the IG and the responsible GPO manager are unable to agree on resolving a recommendation.

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

Follow-up– The process that ensures prompt

and responsive action once resolution is reached on an IG recommendation.

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

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

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

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

Questioned Cost– A cost the IG questions because of an alleged violation of a law, regulation, contract, cooperative agreement, or other document governing the expenditure of funds; such cost is not

supported by adequate documentation; or the expenditure of funds for the intended purposes was determined by the IG to be unnecessary or unreasonable.

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

Resolution– An agreement reached between the IG and management on the corrective action or upon rendering a final management decision by the GPO Resolution Official.

Resolution Official– The GPO Resolution Official is the Deputy Public Printer.

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

Unsupported Costs– Questioned costs not supported by adequate documentation.

Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
C&A	Certification and Accreditation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COA	Continuity of Access
COOP	Continuity of Operations
COTR	Contracting Officer’s Technical Representative
DE	Delegated Examining
FDsys	Federal Digital System
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GPO	U.S. Government Printing Office
HSPD-12	Homeland Security Presidential Directive-12
IG	Inspector General
IPA	Independent Public Accountant
IT	Information Technology
IT&S	Information Technology and Systems
IV&V	Independent Verification and Validation
OALC	Office of Administration/Legal Counsel
OAI	Office of Audits and Inspections
OGC	Office of General Counsel
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OWC	Office of Workers’ Compensation
PII	Personally Identifiable Information
PO	Privacy Officer
RPPPO	Regional Printing Procurement Office

APPENDIX B

Inspector General Act Reporting Requirements

INSPECTOR GENERAL (IG) ACT CITATION	REQUIREMENT DEFINITION	CROSS-REFERENCE PAGE NUMBER(S)
Section 4(a)(2)	Review of Legislation and Regulations	8
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	9-25
Section 5(a)(2)	Recommendations for Corrective Actions	22-25
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	27-30
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	33-35
Section 5(a)(5)	Summary of Refusals to Provide Information	n/a
Sections 5(a)(6) and 5(a)(7)	OIG Audit and Inspection Reports Issued (includes total dollar values of Questioned Costs, Unsupported Costs, and Recommendations that Funds Be Put To Better Use)	22-25
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	41
Section 5(a)(9)	Statistical table showing the total number of audit reports and the dollar value of recommendations that funds be put to better use	42
Section 5(a)(10)	Summary of prior Audit and Inspection Reports issued for which no management decision has been made	n/a
Section 5(a)(11)	Description and explanation of significant revised management decision	n/a
Section 5(a)(12)	Significant management decision with which the IG is in disagreement	n/a

APPENDIX C

Statistical Reports

Table C-1: Audit Reports With Questioned and Unsupported Costs

DESCRIPTION	QUESTIONED COSTS	UNSUPPORTED COSTS	TOTAL
Reports for which no management decision made by beginning of reporting period	\$0	\$0	\$0
Reports issued during reporting period	\$0	\$0	\$0
Subtotals	\$0	\$0	\$0
Reports for which a management decision made during reporting period			
1. Dollar value of disallowed costs	\$0	\$0	\$0
2. Dollar value of allowed costs	\$0	\$0	\$0
Reports for which no management decision made by end of reporting period	\$0	\$0	\$0
Reports for which no management decision made within 6 months of issuance	\$0	\$0	\$0

Table C-2: Audit Reports With Recommendations That Funds Be Put to Better Use

DESCRIPTION	NUMBER OF REPORTS	FUNDS PUT TO BETTER USE
Reports for which no management decision made by beginning of reporting period	0	\$0
Reports issued during the reporting period	0	\$0
Reports for which a management decision made during reporting period		
• Dollar value of recommendations agreed to by management	0	\$0
• Dollar value of recommendations not agreed to by management	0	\$0
Reports for which no management decision made by the end of the reporting period	0	\$0
Report for which no management decision made within 6 months of issuance	0	\$0

Table C-3: List of Audit and Inspection Reports Issued During Reporting Period

REPORTS	FUNDS PUT TO BETTER USE
Report on Audit of Government Printing Office's Ethics Program (Audit Report 11-01, issued December 16, 2010)	\$0
Report on Audit of Control and Accountability of Laptop Computers (Audit Report 11-02, issued December 6, 2010)	\$0
Report on Federal Digital System (FDsys) Independent Verification and Validation – Thirteenth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 11-03, issued December 15, 2010)	\$0
Report on the Consolidated Financial Statement Audit of the GPO for the FYs Ended September 30, 2010 and 2009 (Audit Report 11-04, issued December 21, 2010)	\$0
Report on Federal Digital System (FDsys) Independent Verification and Validation – Fourteenth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 11-05, issued March 29, 2011)	\$0
Report on Audit of Secure Card Personalization System Information Technology Security Controls (Audit Report 11-06, issued March 31, 2011)	\$0
Total	\$0

Table C-4: Investigations Case Summary

Total New Hotline/Other Allegations Received during Reporting Period	46
Preliminary Investigations (Complaints) Closed to the File	21
Complaint Referrals to Other Agencies	4
Complaint Referrals to OAI	4
Investigations Opened by OI during Reporting Period	7
Investigations Open at Beginning of Reporting Period	33
Investigations Closed during Reporting Period	9
Investigations Open at End of Reporting Period	31
Referrals to GPO Management (Complaints and Investigations)	21

Current Open Investigations by Allegation	31	
Procurement Fraud	22	71%
Employee Misconduct	3	10%
Workers' Compensation Fraud	4	13%
Proactive Initiatives	1	3%
Other Investigations	1	3%

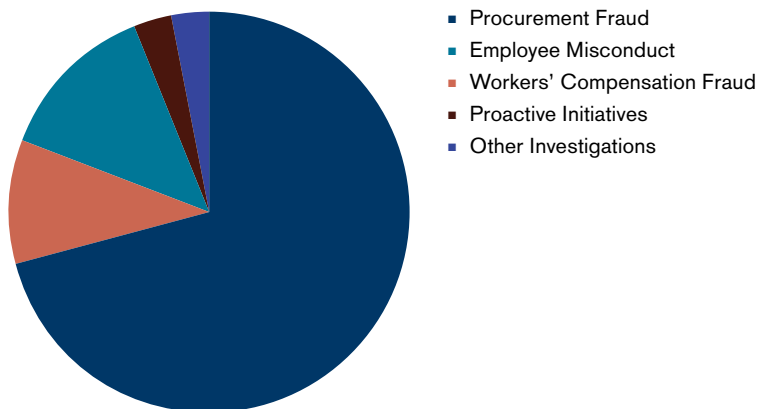


Table C-5: Investigations Productivity Summary

Arrests	1
Total Presentations to Prosecuting Authorities	12
Criminal Acceptances	0
Criminal Declinations	10
Indictments	0
Convictions	1
Guilty Pleas	1
Probation (months)	0
Jail Time (days)	0
Civil Restitutions	0
Civil Acceptances	1
Civil Agreements	0
Civil Declinations	1
Amounts Recovered Through Investigative Efforts	0
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	
Contractor Debarments	7
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions	4
Proposed Employee Suspensions	4
Employee Terminations	0
Inspector General Subpoenas	28

APPENDIX D-PEER REVIEW RESULTS

This appendix complies with Section 5(a)(14)-(16) of the IG Act of 1978, as amended.

A. PEER REVIEW OF THE AUDIT FUNCTION

Under generally accepted government auditing standards, OIG audit functions must have an external peer review at least every 3 years. The LOC OIG conducted a peer review of the GPO OIG audit function during this reporting period. On March 25, 2011, the LOC OIG issued its Peer Review Report of the GPO OIG audit function and found that the system of quality control for the audit function in effect for the 2 years ending September 30, 2010, was suitably designed and complied with, providing the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards. Federal audit organizations can receive a peer review rating of pass, pass with deficiencies, or fail. The GPO OIG received a peer review rating of pass. There are no outstanding recommendations from this peer review. The Peer Review Report is available on the GPO OIG Web site at <http://www.gpo.gov/pdfs/ig/audits/GPO-AuditPeerReviewReport.pdf>.

B. PEER REVIEW OF THE INVESTIGATION FUNCTION

Because it does not derive its statutory law enforcement power from Section 6(e) of the IG Act of 1978,

as amended, the GPO OIG is not required to undergo an external peer review process of its investigative function. Nevertheless, the OIG voluntarily requests external peer reviews of its investigative function.

The National Science Foundation OIG conducted the peer review of the GPO OIG investigative function during this reporting period. On March 11, 2011, the National Science Foundation OIG issued its opinion and found that the system of internal safeguards and management procedures for the investigative function for the year ended 2010 complies with the quality standards established by the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency, the CIGIE, and the Attorney General guidelines. These safeguards and procedures provide reasonable assurance of conforming with professional standards in the conduct of investigations. There are no outstanding recommendations from this peer review. The Peer Review Report is available on the GPO OIG Web site at <http://www.gpo.gov/pdfs/ig/investigations/InvestigationsPeerReview.pdf>.

C. PEER REVIEWS OF OTHER OIGS

The GPO OIG did not conduct a peer review of any other OIG during this reporting period. It has scheduled a peer review of the audit function of the Peace Corps OIG during the next reporting period.

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

732 NORTH CAPITOL STREET, N.W. WASHINGTON, DC 20401

202-512-0039 ■ WWW.GPO.GOV/OIG ■ OIG HOTLINE 1-800-743-7574
GPOOIGHOTLINE@GPO.GOV