U. S. Government Printing Office | Office of Inspector General

SEMIANNUAL REPORT TO CONGRESS

October 1, 2008 to March 31, 2009

U.S. GOVERNMENT PRINTING OFFICE

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 about half 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 GPO OIG 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 these responsibilities, the OIG conducts audits, assessments, investigations, inspections, and other reviews.

CONTENTS

MESSAGE FROM THE INSPECTOR GENERAL

During this reporting period, a new federal administration has put forth an aggressive plan to make Government work more effectively and efficiently through increased transparency, oversight, and accountability. At the GPO OIG, our work has been, and always will be, guided by these principles. We also believe these principles must be translated into real results as exemplified by our work during this reporting period.

First, to increase the transparency of our own work, we have implemented an automatic email alert service that notifies recipients of any new postings on our website (www.gpo.gov/oig). This alert goes beyond what is required by the recently enacted Inspector General Reform Act of 2008.

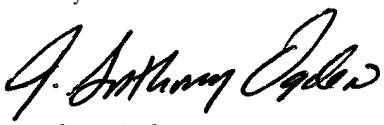
Second, our Office of Audits and Inspections has conducted an extraordinary amount of oversight over the most important and critical GPO programs—the implementation of the Federal Digital System (FDsys) and the GPO Business Information Management System (GBIS–formerly Oracle Business Solutions), and the e-Passport. During this reporting period, the OIG issued five Independent Validation and Verification (IV & V) reports on FDsys with a number of recommendations to strengthen program management, security planning, and implementation to enable successful deployment. In addition, our IV & V work for GBIS noted some difficulties that led to the decision to delay its implementation.

Our audit of GPO's Passport Printing Costs also promoted Agency improvement in accountability and transparency of e-Passport costing. Our audit found that there was adequate documented support for direct costs charged to passports and an adequate cost accumulation process to establish the passport price to the Department of State. However, we identified two specific areas that can be improved upon to be more transparent and accountable to the Department of State in how passport costs are established and how related excess revenue will be invested.

Third, our Office of Investigations has worked hard to find and hold individuals and contractors accountable for their wrongful actions. Indeed, during this reporting period, an investigation of an assault against a GPO employee resulted in three co-workers pleading guilty to one count of assault and resigning from GPO. Another investigation related to the fraudulent use of a Government purchase card resulted in an arrest and a guilty plea on fraud charges. And a GPO contractor who submitted false delivery records to GPO to obtain payment was debarred from doing business with GPO.

Over the last year, this office has attempted to shift our proactive focus to procurement fraud. I am pleased that we are now well on our way to achieving this vision. GPO procured over $750 million of goods and services in fiscal year 2008. With the recent additions of a Special Agent-in-Charge and a senior Special Agent, our office has been engaging in outreach efforts to agency employees involved in procurement to facilitate the identification of fraudulent contractor activities. Because of these efforts, 38% of current open cases are in the area of procurement fraud.

On a final note, during this reporting period, we updated the Agency's significant management challenges. In this update, we note that the Agency has overlooked past recommendations on developing appropriate policies and procedures to protect sensitive information, including personally identifiable information (PII). As identity theft becomes one of the fastest growing crimes in the U.S., we urge the Agency to hold itself accountable before possible identify theft victims do.



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

HIGHLIGHTS OF THIS SEMIANNUAL REPORT

During this reporting period, the OIG continued directing its resources toward those areas of greatest risk within GPO. We provided a variety of services, including program and financial audits, inspections and assessments of key operations, and investigative activity resulting in criminal or administrative actions. We also consulted on a variety of Agency issues and provided comments on proposed legislation affecting the Inspector General community. The work of each of the OIG components is summarized below.

The Office of Audits and Inspections (OAI) issued 8 reports with 40 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency, and continued working with management to close recommendations from earlier reporting periods. During this reporting period, OAI continued its Independent Verification and Validation (IV&V) work related to the implementation of the Federal Digital System (FDsys) and Oracle E-Business Suite and completed six assessment reports addressing various aspects of those two programs.

OAI also completed an audit of GPO Passport Printing Costs and continued to oversee the annual audit of GPO's financial statements conducted by KPMG. Although KPMG found three significant deficiencies, one of them a material weakness, GPO once again obtained an unqualified opinion on the Agency's FY 2008 financial statements.

The Office of Investigations (OI) opened 12 investigations, closed 5, and has 29 ongoing investigations. Procedures for opening cases were revised for enhanced development during the initial stage of an investigation. These new procedures resulted in the opening of 51 "complaint" files, with 12 closed to investigations, 16 closed with no further action, and 23 open complaints at the end of this period. Of the open complaints and investigations, 21 involved allegations of procurement fraud, demonstrating OI's increased efforts to address procurement and financial fraud vulnerability within GPO.

Results for OI this reporting period reflect increased staffing and team building accomplishments. One assault investigation against a GPO employee led to three co-workers agreeing to plead guilty to one count of simple assault as part of a Deferred Sentencing Agreement. As part of the Agreement, the employees also resigned from GPO. In a joint investigation of Government Purchase Card fraud, a search warrant was executed and the defendant pled guilty. A GPO contractor and

the company's owner were also debarred after OI reported the contractor's deceptive practices.

When an investigation into alleged contract fraud revealed possible systemic issues relating to the handling of Personally Identifiable Information (PII) by GPO contractors, a Management Implication Report (MIR) was forwarded to GPO for action. Finally, the Department of Labor upheld its decision for forfeiture of $226,821.74 in workers' compensation to a former GPO employee, who underreported earnings. A cost savings to the Government of $42,000 per year was previously reported ($420,000 in actuary amount over 10 years).

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 that the OIG faces as well as congressional and media relations and requests for information.

During this reporting period, OALC reviewed several audit and investigative reports; assisted OAI with legal questions concerning the nature of GPO's revolving fund under 44 U.S.C. § 309(b); assisted OI with several legal matters related to investigations; oversaw planning for an OIG office reconfiguration and reconstruction as well as replacement of information technology (IT) resources for staff; and completed three congressional and one private request for information.

OALC also supported the IG in his capacity as Acting Chairman of the Legislation Committee of the Council of Inspectors General on Integrity and Efficiency. In this capacity, OALC helped the IG provide comments to several congressional committees on pending legislation affecting the IG community. OALC provided legal advice to the U.S. Capitol Police IG in a variety of matters. OALC continued its active participation in the Council of Counsels to the Inspector General (CCIG) and the coordinated development—with the GPO Web Development and Creative Services Division—for an informational Web site for CCIG. Finally, OALC acted on a variety of matters as the OIG liaison to the GPO General Counsel, including support with GPO litigation matters, and the GPO Office of the Chief of Staff.

OIG MANAGEMENT INITIATIVES

Personnel Update

During this period, the OIG welcomed three new employees to its staff. In December, the OIG welcomed Matthew Elliott as its new Special Agent-in-Charge (SAC) in OI. Matt brings many strengths to OI, developed during his years as a Special Agent for the U.S. Army Criminal Investigations Division and later with the National Archives OIG. Matt has a Master of Science degree in Forensic Science from Lyndon State College in Vermont and an undergraduate degree in Human Services and Counseling from the University of New Haven in Connecticut. Matt also brings to the job an expertise in various types of investigations, including financial and procurement fraud. Just before coming to the OIG, Matt led the investigation of alleged employee misconduct that resulted in the prosecution of multiple defendants in a series of procurement fraud schemes. He has quickly become an invaluable member of the management team.

Natalie Vowell recently accepted a position as senior Special Agent with OI. Natalie was a Special Agent with the U.S. Department of Health and Human Services OIG for more than 10 years and was recognized by the Department of Justice for her success conducting complex provider fraud investigations involving physicians and hospitals. She has also conducted investigations of product false statements for the Federal Trade Commission, Consumer Protection Division. The OIG welcomes Natalie's expertise in managing complex investigations, her relationships in the law enforcement community, and her ability to analyze information through databases. Natalie graduated from the University of Maryland with a dual degree in Criminal Justice and Sociology.

In March, Christen Stevenson joined OAI as an auditor. Christen comes from the Federal Home Loan Mortgage Company (Freddie Mac) where she was a Senior Internal Auditor. Christen previously worked as an internal auditor for both the Federal Reserve Bank of Chicago and LaSalle Bank in Chicago. She graduated from Central Michigan University with a degree in accounting.

Deputy Assistant IG for Audits and Inspections Brent Melson (center) was recognized by the Executive Council on Integrity and Efficiency for his outstanding contribution to the establishment of the Information Technology Audit and Assessment Function at GPO OIG. He is shown with J. Anthony Ogden (right) and Kevin Carson (left), Assistant IG for Audits and Inspections.

Finally, in October, 2008, the Executive Council on Integrity and Efficiency recognized Deputy Assistant Inspector General for Audits and Inspections Brent Melson with an Award for Excellence. Brent was recognized for his "outstanding contribution towards the establishment of the Information Technology Audit and Assessment function" at the GPO OIG. Brent joined the GPO OIG in late 2005 after approximately 15 years of service with the National Aeronautics and Space Administration (NASA) OIG. At the NASA OIG, Brent established and ran the IT Audit Directorate. For his contributions at NASA, Brent received an Award for Excellence from the President's Council on Integrity and Efficiency, and the NASA Medal of Excellence. Prior to NASA, Brent worked at the Federal Reserve Board of Governors as a Senior Auditor. Brent's extensive experience and IT oversight work has been instrumental as GPO seeks to transform itself from an ink-on-paper operation to a digital platform agency with such programs as FDsys, the Oracle E-Business Suite implementation, and GPO's Public Key Infrastructure.

COUNCIL OF INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

On October 14, 2008, the Inspector General Reform Act of 2008, Public Law 110-409, statutorily established the Council of Inspectors General on Integrity and Efficiency (CIGIE). The mission of CIGIE is to address integrity, economy, and effectiveness issues that transcend individual Government agencies and increase professionalism and 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.

To accomplish its mission, the CIGIE will identify, review, and discuss areas of weakness and vulnerability in Federal programs and operations for fraud, waste, and abuse, and develop plans for coordinated Government-wide activities that address those problems and promote economy and efficiency in Federal programs and operations.

The IG became the Acting Chairman of the CIGIE Legislation Committee in January 2009. In this representative capacity, the IG wrote letters to several Committees on various legislative matters affecting the IG community, particularly provisions relating to oversight of stimulus funds in the American Recovery and Reinvestment Act of 2009. CIGIE efforts resulted in substantial changes to the original provisions related to the power and composition of the Recovery Accountability and Transparency Board that provide for better coordination with the IG community through the CIGIE.

The IG also wrote a letter to the Senate Committee on Homeland Security and Governmental Affairs as well as the House Committee on Oversight and Government Reform to recommend an amendment to the Paperwork Reduction Act (PRA). The PRA requires that collections of information, such as surveys, covering more than 10 nonfederal persons must be approved by an agency senior official and the Office of Management and Budget. These requirements have hampered the ability of IGs to conduct independent and comprehensive audits, inspections, and evaluations. The proposed amendment would exempt Federal IGs from the PRA procedural and approval requirements for collecting information of nonfederal persons.

Legislative Branch IGs continued to meet quarterly in response to a Senate Appropriations Committee request that the IGs throughout the Legislative Branch communicate, cooperate, and coordinate with one another on an informal basis. The meetings continue to improve communications and contact between the Legislative Branch IGs. During this reporting period, Legislative Branch IGs discussed possible suggestions to their organic statutes to accomplish changes in the recent passage of the IG Reform Act of 2008.

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 of GPO. It then makes recommendations in each semiannual report on the impact of such legislation or regulations on the economy and efficiency of programs and operations administered or financed by GPO. To assist the Agency in achieving its goals, we will continue to play an active role in that area.

Although there were no legislative proposals relating to GPO programs and operations, as noted above, as Acting Chairman of the CIGIE Legislation Committee, the IG commented on the American Recovery and Reinvestment Act of 2009 to several Committees and recommended a proposed amendment to PRA that would exempt Federal IGs from current procedural and approval requirements.

GPO MANAGEMENT CHALLENGES

GPO is well into its digital platform transformation, having established several key initiatives that will help the Agency meet its mission in the ever-changing digital environment. Substantial and challenging risks that could affect successful implementation of the programs and initiatives will continue. In our April 2007 Semiannual Report to Congress, the OIG provided management a list of issues identified as most likely to hamper the Agency's efforts if not addressed with elevated levels of attention and resources. In this report, we reevaluate and update the Agency's management challenges as the Agency moves forward in its transformational efforts.

1. 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 central to his administration "the call to sustainable environmental stewardship" and to attempt to be "green" in virtually every step of the printing process. The Public Printer has outlined a proactive plan of action so that GPO becomes a more efficient operation that makes better use of the resources under its control. Some of the initiatives include moving from web offset presses to digital equipment, accelerating the re-engineering of business processes, conducting energy audits, using paper that goes beyond

GPO'S TOP 10 MANAGEMENT CHALLENGES

1. Sustainable Environmental Stewardship.
2. Management of Human Capital.
3. Improved Financial Management.
4. Continuity of Operations.
5. Internal Controls.
6. Security and Intelligent Documents.
7. Protection of Sensitive Information.
8. Information Technology and Systems Management.
9. Business Development and Customer Service.
10. Acquisitions.

minimum requirements for recycled content, and installing a "green" roof.

We previously reported management's concerns that the GPO facility is too large (contains three times more space than needed), is too operationally inefficient (functions are spread over four buildings and multiple floors), and is too expensive to operate given its size, age, and condition. Accordingly, GPO has proposed a new facility that would more appropriately meet Agency needs and be more energy efficient. This also fits with the Agency's environmental stewardship initiative.

On February 20, 2009, the Government Accountability Office (GAO) released a report entitled "Government Printing Office: Issues Faced in Obtaining a New Facility."[1] GAO found that GPO "followed leading practices for capital decision making during analyses of options [for a new facility] but did not conduct cost-benefit analyses that explored a full range of options for obtaining a new facility." GAO also noted two key issues impeding the efforts to obtain a new facility: GPO lacks the legislative authority to outlease property and retain and use the proceeds from an outlease and its lack of expertise in managing leases as a landlord.

In light of the proposal in the stimulus package to convert government facilities to "High-Performance Green Buildings," we believe that GPO would be well served by conducting a complete cost-benefit analysis to fully explore the best options for a new facility that would potentially reap economic as well as environmental benefits. While an aggressive goal, this would be in line with the Agency's objectives and with the environmental and economic objectives of the Congress and President Obama.

The Public Printer has outlined an aggressive, and we believe achievable, environmental stewardship plan for GPO. However, we urge management to promote and incorporate "green thinking" into all business processes and advance through performance metrics, reward programs, and other means, a new culture of green thinking throughout the Agency.

[1] GAO-09-329R, accessible at http://www.gao.gov/new.items/d09392r.pdf.

As an example, we would urge an integrated approach to green acquisition by incorporating green thinking into the entire procurement process. This and other efforts will require a top to bottom and bottom to top commitment. Employee empowerment will be absolutely necessary for the Agency to achieve its goals and sustain them.

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 to reduce emissions, energy consumption, and energy costs. We look forward to working with Agency personnel in achieving a long-term and sustainable environmental stewardship program.

2. Management of Human Capital. We continue to highlight the challenges the Agency faces in "right sizing" its workforce while at the same time attracting employees with the right skill sets for the new GPO. The Chief Human Capital Officer will continue confronting significant issues related to transformation of the GPO workforce and must also advance creative solutions that will help the Agency meet its ongoing workforce needs—in part by building a diverse, qualified applicant pool.

We previously completed a congressionally requested audit of GPO's diversity programs, particularly those related to establishing a more diverse population in senior leadership positions. The audit showed that while GPO has voluntarily adopted several components for establishing a model Federal Government diversity program, improvements can be made toward enhancing diversity of the Agency's corps of senior-level employees. Management has not yet provided the OIG with a detailed implementation plan of its recommendations. Nevertheless, we continue to monitor the audit's recommendations related to establishing a model diversity program that will assist GPO in creating an environment that helps diminish barriers for protected groups and helps attract and retain capable employees from diverse backgrounds.

Although GPO has made strides with respect to establishing and maintaining a diverse workforce, improvements are still needed in other areas. For example, the Office of Personnel Management (OPM) completed a Human Capital Management Review of the GPO in late 2008. The objectives of the review were to determine GPO adherence to merit systems principles as well as compliance with applicable laws and regulations, and assess efficiency and effectiveness in administering human capital and human resources management programs and systems.

Among the significant findings of the OPM evaluation were that GPO (1) had not finalized its long-term strategic goals and objectives, (2) had not conducted a workforce analysis to identify its mission-critical occupations and competencies, (3) had no indication that the existing human capital function had the capacity and data structure needed to partner strategically with managers to conduct workforce analysis and planning, and (4) was not assessing its organizational, occupational, and individual needs or evaluating the training offered to determine how well it meets short- and long-range program needs. While management did not fully agree with the OPM findings, the Agency has either planned or initiated actions that address the recommendations.

3. Improved Financial Management. GPO has been migrating current business, operational, and financial systems, including associated work processes, to an integrated system of Oracle enterprise software and applications known as the Oracle E-Business Suite. The new system will provide GPO with integrated and flexible tools that help successfully support business growth and customer technology requirements for products and services. To oversee and support such a complex effort, the GPO Oracle Program was created. Although investment in the integrated system presents opportunities for enhanced efficiency and cost savings, such an investment brings with it significant risk in the event the system does not meet user requirements.

The OIG continued IV&V activities associated with implementation of the Oracle E-Business suite. IV&V provides GPO with an independent assessment of project status, satisfaction of user needs, and project cost effectiveness. During both fiscal year (FY) 2008 and FY 2009, IV&V efforts focused on the GPO Business Information Management System (GBIS) project, formerly known as the Oracle Release 2 project. The main goal of GBIS is to implement Project Costing and Project Billing. Additional capabilities will be added to Purchasing, Inventory, Accounts Payable, Receivables, and other implemented Oracle modules. To date, IV&V has resulted in several recommendations designed to improve management of the project as well as future Oracle projects.

During this reporting period, the OIG issued a report that provides a summary of the key risks and issues identified with GBIS regarding the processes, artifacts, and products related to development, and with particular emphasis on data conversion, user preparation, user acceptance testing, and deployment planning. We also note that implementation of GBIS continues to be delayed because of those issues. Such continued implementation delay could potentially materially affect the Agency's FY 2009 financial statement audit.

The OIG also continues to oversee activities of KPMG LLP (KPMG), the Independent Public Accountant (IPA) conducting the annual financial statement audit. During this period, KPMG

completed the FY 2008 financial statement audit of GPO. KPMG issued an unqualified opinion on the GPO FY 2008 consolidated financial statements, stating that the Agency's financial statements were presented fairly, in all material respects, and in conformity with generally accepted accounting principles. KPMG did, however, identify three significant deficiencies, one of which—financial reporting controls—was considered a material weakness. Failure to adequately address and mitigate this material weakness could also potentially prevent the Agency from obtaining future unqualified opinions on its financial statements.

4. Continuity of Operations. Development of the Agency's Continuity of Operations (COOP) capabilities will continue as a top management challenge. A previous OIG review of COOP planning contained several recommendations designed to improve the overall COOP posture of the Agency, including most fundamentally that GPO adopt planning requirements and critical elements identified in Federal Preparedness Circular 65, "Federal Executive Branch Continuity of Operations." GPO developed a comprehensive COOP plan based on the Federal Emergency Management Agency template of key COOP components. The plan discusses issues such as essential functions, interoperable communications, delegations of authority and testing, training, and exercises. The Agency also developed an Occupant Emergency Plan (OEP) as a companion to its COOP. The OEP presents appropriate responses for emergencies and discusses known or anticipated categories of emergencies.

The Agency continues to take the necessary steps for enhancing its COOP posture, including planning and conducting exercises with scenarios that tested alternate production facilities and procedures for notifying essential personnel. The Agency's business continuity manager has also continued to work directly with GPO's various business units in support of the COOP program. Accomplishments during the most recent period included defining requirements to develop or locate an alternate COOP site outside the Washington, D.C., area to process and publish congressional documents. Various COOP exercises were completed, including an exercise of the passport production capabilities of the Secure Production Facility (SPF) at the Stennis Space Center in Mississippi. Also completed was a schedule of COOP exercises for 2009 as well as identification of the top issues impacting COOP.

5. Internal Controls. GPO management establishes and maintains a system of internal controls for effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Almost all OIG audits include assessments of a program, activity, or function's applicable control structure. Several ongoing audits of GPO activities are assessing internal controls.

The annual financial statement audit that KPMG conducts also addresses internal control issues and provides management with recommended corrective actions. Although management recognizes the need for improving the internal control environment to successfully implement its strategic vision and planned future initiatives, Agency action is important because of implementation of Statement on Auditing Standards (SAS) No. 112, "Communicating Internal Control Related Matters Identified in an Audit." SAS No 112 establishes standards and provides guidance on communicating matters related to an entity's internal control over financial reporting identified in a financial statement audit. The standard requires that the auditor communicate control deficiencies that are "significant deficiencies" and "material weaknesses."

As noted above and in more detail in the OAI section, during this reporting period, as part of its financial statement audit KPMG found three significant deficiencies related to internal control: (1) over financial reporting, which it considered a material weakness; (2) over the processing of human resources information; and (3) over information technology general controls. We urge that management spend the necessary resources to correct current and past deficiencies and invest in a robust program of continuous internal control reviews and improvement.

6. Security and Intelligent Documents. As the Federal Government's leading provider of secure credentials and identity documents, management regards Security and Intelligent Documents (SID) as a business unit best exemplifying the Agency's transformation toward high-technology production. During the first half of FY 2009, SID reported the successful manufacturing for the Department of State of more than 5.8 million electronic passports in their Washington D,C., SPF. Established as a COOP site, the SPF at Stennis produced more than 1.6 million passports.

SID continued to operate a newly established, Washington, D.C., based Secure Credential Center (SCC) to support the Department of Homeland Security's Customs and Border Protection (DHS/CBP) Trusted Traveler Program (TTP). During this period, SCC produced and personalized secure access credential cards for the Joint Congressional Committee on Inauguration Ceremonies and the U.S. Capitol Police. The SID also worked with the Department of Health and Human Services' Center for Medicare and Medicaid Services' to produce, personalize, and distribute Medicare identification cards to citizens of Puerto Rico.

During this reporting period, the SID also reported initiation of two critical process improvement methodologies in the Washington, D.C., and Stennis SPFs, as well as SCC. The first process, known as 5S, is a series of defined steps and audits to achieve efficiencies in manufacturing process flows, in equipment use and placement, and in work environment housekeeping standards. The SID reported that the 5S program yielded significant and noticeable changes in the production spaces and created safer and more streamlined process flows. Additionally, SID reported initiatives designed to refine existing written work instructions and standard operating procedures for manufacturing processes to underpin the efforts and lay foundation for the ISO 9000 certification at a future date.

Finally, GPO faces the challenge of deploying its own Homeland Security Presidential Directive-12 (HSPD-12) infrastructure and issuance of identity credentials to employees and contractors. The overall responsibility for a GPO-wide HSPD-12 program lies with GPO's Chief Management Officer and Security organizations. The SID designs, prints, personalizes, and distributes the card. While not legally required to comply with HSPD-12, we continue to recommend that the Agency strive toward voluntary compliance. To that end, several control objectives are critical for meeting the security, efficiency, fraud prevention, and privacy protection goals that HSPD-12 requires, and the Agency must maintain throughout the life cycle of deployment.

Whatever its intentions, the Agency should employ the best practices established by HSPD-12 and begin addressing several of the control objectives, including separating duties for registering and issuing credentials; using original identity source documents; using appropriate background investigations; and using smart cards as person-identity-verification credentials. The OIG will continue to monitor Agency efforts regarding internal deployment of HSPD-12 and conduct audits as necessary for Agency compliance with Federal Information Processing Standards (FIPS) Publication 201 (FIPS-201), "Personal Identify Verification of Federal Employees and Contractors."

7. Protection of Sensitive Information. GPO must establish rules of conduct and appropriate administrative, technical, and physical safeguards to ensure that sensitive information is adequately identified and protected. Failure to do so 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 the breach of personally identifiable information (PII). This includes PII contained in information systems as well as paper documents. In accordance with Office of Management and Budget (OMB) Memoranda 06-15 and 07-16, Executive Branch agencies have had to implement policies and procedures to protect and respond to the breach of PII as far back as the middle of 2007.

The OIG has advised GPO on numerous occasions of its concerns regarding the protection of PII. As reported in OIG Report 07-09 *GPO Compliance with the Federal Information Security Management Act*, dated September 27, 2007, while GPO's Information Technology and System's division is making progress in protecting PII contained in information systems, much work remains, including full use of privacy impact assessments and increased data encryption. Indeed, in 2007, we forwarded to Human Capital and other senior management, a copy of OMB Memorandum 07-16 and urged adoption of OMB recommendations to identify and mitigate the unnecessary use of sensitive PII, specifically Social Security numbers.

During this reporting period, we had significant reason to believe that the recommendations were overlooked. As an example, Human Capital continues to distribute resumes and personal documents with sensitive PII and has not formally developed plans to eliminate the unnecessary use of PII on agency forms and documents. Human Capital also recently mailed employees notices containing their sensitive PII in contravention of Federal guidance.

Moreover, two recent investigations involving breaches of sensitive PII by GPO vendors resulted in recommendations that GPO immediately identify any contracts and contractors handling PII, review security requirements, request security plans, conduct on-site surveys and inspections, and appoint a GPO Privacy Officer to establish and oversee a comprehensive protection program.

As identity theft becomes one of the fastest growing crimes, taking the "we-have-always-done-it-this-way" approach to handing PII is no longer acceptable – for GPO employees as well as its customers. We urge management to develop the policies, procedures, and training necessary to address this most serious issue. The OIG will continue to monitor GPO's progress in addressing the protection of sensitive information.

8. Information Technology and Systems Management. As GPO transforms from an ink-on-paper operation to a highly efficient and secure multimedia digital environment, management of the Agency's IT resources is critical to the success of its vision and mission. Acquisition, implementation, and sustainment of engineering issues associated with Information Technology and Systems (IT&S), including security issues, provide GPO with new management challenges.

Noteworthy challenges for the IT&S function include establishing a top level Enterprise Architecture and support for a number of significant initiatives, including FDsys, the e-Passport system, digital publication authentication using a Public Key Infrastructure (PKI), information system management, implementation of the Oracle E-Business Suite, and implementation of digital human resources systems. To create a plan that will help mitigate risks on aging legacy systems, IT&S initiated an analysis of legacy applications and its impact on business operations. Legacy systems increasingly inhibit Agency ability to respond to customer needs and must be replaced. IT&S recently completed a 5-year strategy that should help guide the Agency through implementation of new systems and retirement of legacy systems. FDsys, human resource systems, and certain Oracle E-Business modules are scheduled to be operational during FY 2009.

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. Complying with FISMA presents additional challenges for IT&S, including protecting sensitive Agency systems, information, and data. During FY 2007, the OIG conducted an assessment of compliance with FISMA to identify any gaps and deficiencies in GPO's overall information security program, including critical systems. We initiated a follow-on FISMA assessment in FY 2008, which was being finalized during this reporting period. We also initiated our

annual independent assessment of the GPO enterprise network infrastructure to evaluate the level of security controls in place that help protect IT resources from unauthorized access and compromise.

As the Agency fulfills its mission in the vital arena of electronic information dissemination and e-Government, GPO established a PKI that serves the needs of the Agency, its legislative branch partners, and other Federal partners.[2] The PKI is cross-certified with the Federal Bridge Certificate Authority—a substantial and necessary step toward using PKI for the benefit of a variety of customers. PKI will serve as an important contributor for future revenue-generating activities within GPO. To partially meet PKI certification provisions, the OIG conducts interim and annual compliance reviews that determine whether assertions related to the adequacy and effectiveness of the controls over GPO's PKI Certificate Authority operations are fairly stated based on underlying principles and evaluation criteria. Finally, the OIG will continue to lead IV&V activities associated with the ongoing implementation of the Oracle E-Business Suite and implementation of FDsys.

9. Business Development and Customer Service. As the Agency continues to move closer to its goal of transforming to a 21st Century information processing and dissemination operation, customer services for GPO must reflect and advance that transformation. To ensure success in the future, management must maintain the appropriate focus, staffing, and alignment with the Agency Strategic Vision. The culture and focus of customer service efforts must reflect a new way of thinking, and customers should come to GPO because they want—not because they must. Transformation of the traditional GPO customer relationship requires a continuing evolution toward state-of-the-art customer relations management.

During this reporting period, GPO undertook reorganization of several business units to better serve its various Government customers. Specifically, the Agency created three new business units to improve service. Elements under the previous Customer Services business unit were realigned

[2] By encrypting information, PKI ensures the highest level of protection for electronic information that travels over ordinary, nonsecure networks.

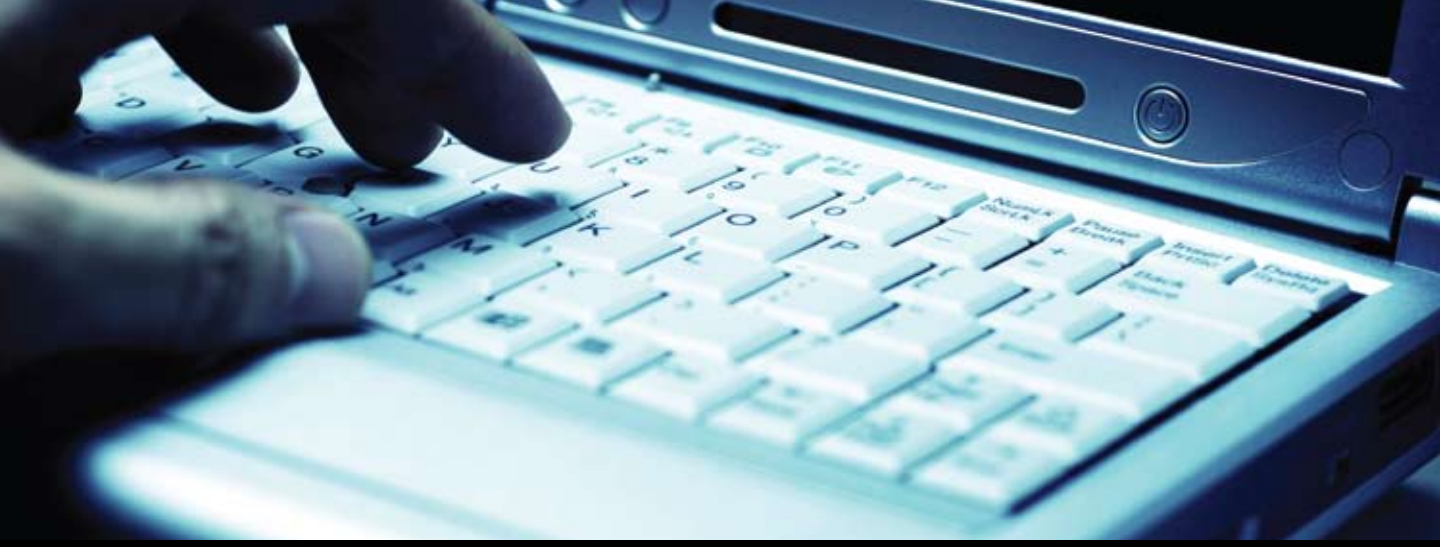
into two separate business units: Print Procurement and Sales and Marketing. Print Procurement was formed to handle the transaction process on behalf of Federal customers to commercial vendors whereas Sales and Marketing will provide Web services, creative services, marketing research, and consultation to Federal customers. The third new business unit, Operations Support, will include engineering and environmental services. This business unit will provide technical maintenance expertise, in house support, safety procedures and environmental compliance to the GPO manufacturing operations. This realignment of business units should help streamline processes, strengthen customer relationships, and develop new sales opportunities.

The Employee Communications Office also conducted a survey of focus groups within customer services to identify key strengths that could be leveraged and key barriers to improving service to customers. While many strengths and barriers were identified, the most common of them across the focus groups was the need for standard operating procedures which, if properly developed, would ensure that GPO customers receive the same quality service regardless of what team or individual within the Agency is providing it.

10. Acquisitions. As with other Federal agencies across the Government, GPO faces challenges in its acquisition function. Acquiring goods and services, especially those necessary to transform the Agency and to provide services to its Federal customers, in an efficient, effective, and accountable manner is essential. With over $750 million in acquisitions during FY2008, the OIG remains concerned that the Agency has not devoted the resources necessary to conduct assessments of the acquisition function to clearly identify gaps in effective performance and implement a plan to resolve critical issues, as required for Executive Branch agencies under the Services Acquisition Reform Act of 2003 and OMB guidelines.

Last year, OMB provided guidelines to Executive Branch agencies to conduct internal reviews of the acquisition function required under OMB Circular A-123. OMB used the GAO "Framework for Assessing the Acquisition Function at Federal Agencies" as the standard approach to assess each agency's acquisition function.[3] Although GPO is not required to follow OMB guidelines in this area, we believe that the Agency would greatly benefit from performing that acquisition review process and urge management to undertake this initiative.

[3] GAO-05-218G, September 2005, accessible at http://www.gao.gov/new.items/d05218g.pdf.



OFFICE OF AUDITS AND INSPECTIONS (OAI)

As the IG Act requires, OAI conducts independent and objective performance and financial audits relating to GPO operations and programs, and oversees the annual financial statement audit an IPA firm under contract performs. OAI also conducts short-term inspections and assessments of GPO activities generally focusing on issues limited in scope and time. OIG audits are performed in accordance with generally accepted government auditing 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 eight new audit and assessment reports. Those 8 reports contained 40 recommendations for improving GPO operations, including strengthening internal controls throughout the Agency. OAI continued its work with management to close open recommendations carried over from previous reporting periods. As of March 31, 2009, 32 recommendations were open.

B. Federal Digital System (FDsys) – Independent Verification and Validation

The FDsys will be a comprehensive information life cycle management system that will ingest, preserve, provide access to, and deliver content of 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. It will have 6 clusters (Content Management, Content Preservation, Content Access, Content Delivery, Content Submission, and Infrastructure), which comprise 25 or more functional areas. A multiyear, multirelease integration effort is being used to design, procure, develop, integrate, and deploy selected technologies and components of FDsys.

The OIG is responsible for IV&V work associated with developing and implementing FDsys. We contracted with American Systems to conduct the evaluations. American Systems has extensive IV&V experience with the Federal sector, and IV&V work will determine whether system implementation is consistent with the FDsys project plan and cost plan and meets GPO requirements. Additionally, IV&V will monitor development and program management

practices and processes to anticipate potential issues. Specific IV&V tasks include:

Program Management – IV&V includes activities regarding the cost, schedule, and risk associated with development and implementation to evaluate overall program management effectiveness.

Technical – IV&V includes activities regarding the resources, system requirements, architecture and design documents, and other critical deliverables associated with FDsys development and implementation.

Testing – IV&V includes activities regarding the Design Validation Test Plan and test efforts performed by the implementation team to verify adequacy and completeness of testing activities.

During this reporting period, GPO launched a public Beta version of FDsys. The Beta version contains the following collections:

- Compilation of Presidential documents (1993 to present)
- Congressional bills (103rd Congress to present)
- Congressional documents (104th Congress to present)
- Congressional hearings (105th Congress to present)
- Congressional Record (1994 to present)
- Congressional reports (104th Congress to present)
- Federal Register (1994 to present)
- Public and Private Laws (104th Congress to present)

The Agency anticipates migration of the remaining collections to FDsys toward the end of FY2009.

In Section E, we discuss our reports during this reporting period resulting from IV&V efforts, which are ongoing and will continue throughout the life of the project.

C. GPO Business Information Management System (formerly Oracle Release 2) – Independent Verification and Validation

GPO is implementing the Oracle E-Business Suite in a series of phased releases with incremental functional capabilities. GPO has completed some early implementation start-up projects to become familiar with Oracle technology and work processes and to develop successful project implementation skills. The GBIS project is implementing the Oracle Projects module, which consists of project costing and project billing. Other capabilities will be added to Purchasing, Inventory, Accounts Payable, Receivables, and other implemented Oracle modules.

The OIG oversees IV&V work associated with implementation of the Oracle E-Business Suite. We contracted with Noblis, a nonprofit science, technology, and strategy organization, to conduct IV&V evaluations of GBIS. Noblis has extensive IV&V experience with the Federal sector. Our IV&V work noted that the GBIS project has had several difficulties resulting in implementation delays, including difficulty with requirements gathering, "to-be" process definitions, and testing. The IV&V team supported management's decisions to delay implementation. In Section E, we highlight our report for this period resulting from these IV&V efforts, which are ongoing and will continue throughout the life of the project.

D. Financial Statement Audit (Audit Report 09-06, issued January 15, 2009)

Federal law requires that GPO obtain an independent annual audit of its financial statements, which the OIG oversees. KPMG conducted the FY 2008 audit under a multiyear contract for which OAI served as the Contracting Officer's Technical Representative (COTR). The oversight ensured that the audit complied with generally accepted government auditing standards. OAI also assisted with facilitating the external auditor's work as well as reviewing the work performed. In addition, OAI provided administrative support to the KPMG auditors and coordinated the audit with management.

KPMG issued an unqualified opinion on GPO's FY 2008 consolidated financial statements, stating that the Agency's financial statements were presented fairly, in all material respects, and in conformity with generally accepted accounting principles. However, KPMG identified three significant deficiencies including (1) financial reporting controls; (2) controls over processing human resource information; and (3) IT general controls.

As a result of improperly functioning management internal controls, KPMG concluded that the following significant deficiencies related to financial reporting controls when viewed in the aggregate, constitute a material weakness. Specifically, the auditors found that (a) additions to general property, plant, and equipment were recorded in the subsidiary and general ledgers based on when cash disbursements were made for the assets instead of when the asset was received and accepted; (b) several invoices for internal use software were improperly expensed rather than capitalized; (c) an estimated product warranty was being recorded for e-Passports despite GPO not having experienced a claim for spoilage since inception of the e-Passport program in 2007; (d) passport work-in-process inventory was improperly recorded as unbilled receivables; (e) management review of the consolidated financial statements needs to be strengthened because the existing process for compiling the consolidated financial statements was complex and difficult to review and there were no written procedures documenting how GPO's consolidated financial statements are compiled; and (f) key reconciliations of Fund Balance with Treasury, accounts payable, payroll, and expenses were not always performed timely and when performed; differences noted were not consistently investigated and resolved in a timely manner.

KPMG reported as a significant deficiency that there is no application control to prevent Human Capital Assistants and Specialists from making changes to their own personnel files. In addition, no supervisory review of personnel action changes exists that will ensure accuracy and completeness before being uploaded to the National Finance Center (NFC). Further, for those employees whose pay rates do not follow the General Schedule, HC Assistants and Specialists can bypass the NFC payroll system's edit checks with no compensating review. KPMG also reported as a significant deficiency the design and/or operation of controls that continue to exist in the areas of entity-wide security, access controls, system software, and service continuity.

KPMG made recommendations that GPO address each of these deficiencies. The OIG further

recommended that GPO follow Appendix A, "Internal Control over Financial Reporting," of the Chief Financial Officer (CFO) Council's Implementation Guide for OMB Circular A-123, "Management's Responsibility for Internal Control," to develop a comprehensive corrective action plan to address the material weakness.

Except for KPMG's finding on product liability, management concurred with all of the findings and recommendations and has either planned or initiated responsive corrective actions. Management believes that it is reasonably possible and potentially probable that some of the approximately 10 million e-passports not yet personalized as of September 30, 2008, could have latent defects for which GPO is responsible for fixing or replacing. Based on experience to date, management reduced the product warranty to about 29 percent of the original estimate.

E. Audit and Inspection Reports

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

As previously noted, 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 this reporting period, GPO launched a public Beta version of FDsys containing a limited number of collections. The Agency anticipates migration of the remaining collections to FDsys toward the end of FY2009.

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. The report contains recommendations intended to further strengthen management of the FDsys program. Management concurred with each of the recommendations and proposed responsive corrective actions.

2. Audit Report 09-02 (Issued December 22, 2008)

Audit of GPO's Passport Printing Costs

GPO is the sole source for producing, storing, and delivering blank U.S. passport books (passports) for the Department of State. During the first 8 months of FY 2008, GPO produced 18.6 million passports and realized revenue from passport sales of more than $275 million, including $71.5 million in net income. The OIG conducted an audit of Passport Printing Costs to assess GPO's basis for establishing the price the agency charges the Department of State (DOS) for each blank passport book produced.

The audit identified that in conjunction with the DOS, GPO established a price of $14.80 that it charges the DOS for each passport produced. The price of $14.80 includes the cost of material, labor, overhead, inventory, and future capital expansion.[4] GPO established the price in accordance with 44 U.S.C. § 309(b) "Revolving fund for operation and maintenance of Government Printing Office," The price was mutually agreed to with the DOS through a Memorandum of Understanding. The audit also concluded that GPO had adequate documented support for all direct costs charged to passports and had a cost accumulation process that was sufficient for the Agency to base its passport price.

OIG auditors identified two specific areas where GPO can improve the accountability and transparency of its passport costing process to better prepare the Agency for any future audits or reviews by outside entities and promote good customer relations with the DOS. First, through the May 2008 audit time period, we found that GPO generated more than $43 million in excess cash from passport sales to the DOS beyond what was necessary to recover costs and provide for mutually agreed upon future capital expansion. That condition occurred because GPO did not revise its original passport pricing structure and did not reach final agreement with the DOS on a capital investment plan to earmark the excess cash.

Auditors also found that GPO, at its discretion, changed its indirect overhead cost allocation methodology for passport costs without documenting the justification and analysis for the change. As a result, the Agency increased the amount of indirect overhead allocated to passport costs from 5.65 percent, or $4 million, in FY 2007, to 52 percent, or $40 million, through May 2008. We recommended that GPO (1) finalize its capital investment plan and proposed addendum to the

[4] The DOS currently charges the public $100 for an adult passport. This fee, effective February 1, 2008, for persons 16 years and older, consists of $75 for the passport application and $25 for processing.

Memorandum of Understanding with the DOS regarding passport pricing, to better account for the excess cash generated from passport sales, (2) document and explain the Agency's change in the indirect overhead cost rate allocation to the cost of passports to explain the increase in indirect overhead allocated to passports, and (3) revise the passport pricing structure to be more reflective of the current passport costing and production process. GPO management concurred with each of the report's recommendations and has either taken or plans to take responsive corrective actions.

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

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

This fifth quarterly report provides a 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. The report contains 10 recommendations intended to further strengthen management of the FDsys program. 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. While we disagreed with management's position on the remaining four recommendations, we accepted management's proposed alternative corrective actions.

4. Assessment Report 09-04 (Issued December 24, 2008)

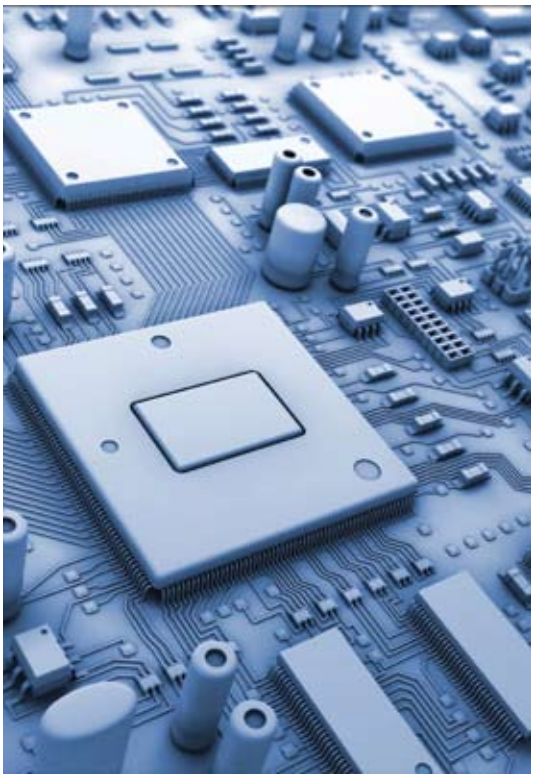
Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Security Analysis Report

This report provides an overview of key risks and issues identified by the FDsys IV&V team as a result of their review of the revised FDsys system security plan. The IV&V team concluded that the revised system security plan was a greatly improved document reflecting a positive effort to include relevant security controls. However, the IV&V team concluded that the revised systems security plan did not adequately detail the security controls in place, or those planned to be in place for the protection of confidentiality, integrity, and availability of the systems data and associated resources. The report contains five recommendations intended to strengthen FDsys system security planning and implementation. Management concurred with each of the recommendations and proposed responsive corrective actions.

5. Assessment Report 09-05 (Issued December 24, 2008)

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – Release R1C.2 Pre-Deployment Status Report

This report provides an overview of key risks and issues identified by the FDsys IV&V team that could adversely impact deployment of GPO's first public release of FDsys (Release R1C.2). The team concluded that while progress was being made



on FDsys, a number of key activities needed to be completed for the program to be successfully deployed. The report reiterated two recommendations made in previous IV&V quarterly reports regarding testing, requirements traceability, and documentation. Therefore, we did not request a formal response from management.

6. 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

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. The report contains recommendations intended to further strengthen management of the FDsys program. Management concurred with each of the report's recommendations and proposed responsive corrective actions.

7. Assessment Report 09-08 (Issued March 31, 2009)

Oracle E-Business Suite Release 2 Independent Verification and Validation (IV&V) - Technical

The OIG contracted with Noblis to conduct IV&V for Oracle Release 2. Release 1 was initiated to begin taking advantage of GPO's investment in Oracle technologies and allowing GPO to create a model for future implementation activities. Release 2 adds additional functionality to the original Oracle modules as well as introducing new business processes. The OIG contract tasks Noblis to assess program management, technical, and testing activities associated with the Release 2 implementation. Noblis is required to issue summary reports for program management, technical, and testing IV&V.

The report provides a summary of the key risks and issues identified by Noblis regarding the processes, artifacts, and products related to development of Release 2, with particular emphasis on data conversion, user preparation, user acceptance testing, and deployment planning. The report contains

recommendations intended to strengthen the Oracle Release 2 program. Management concurred with each of the recommendations and proposed responsive corrective actions for each.

F. Status of Open Recommendations

Management officials made progress in implementing and closing many of the recommendations identified during previous semiannual reporting periods. For the 32 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 06-02 (Issued March 28, 2006)

GPO Network Vulnerability Assessment

FINDING

Although GPO has many enterprise network controls in place, improvements that will strengthen the network security posture are needed. During internal testing, we noted several vulnerabilities requiring strengthening of controls. However, no critical vulnerabilities were identified during external testing. Although unclassified, we consider the results of the assessment sensitive and, therefore, limited discussion of its findings. Further details regarding assessment findings can be obtained by contacting the OIG.

RECOMMENDATION

The OIG made four recommendations that should strengthen internal controls associated with the GPO enterprise network. Those recommendations should reduce the risk of compromise to GPO data and systems.

MANAGEMENT COMMENTS

Management concurred with each of the report's recommendations and initiated corrective action.

OIG COMMENTS

As of the end of this reporting period, two recommendations made in this report are open. The OIG continues to work with management to monitor implementation of the remaining two open recommendations, whose status will be further reviewed as part of the OIG's FY 2009 Network Vulnerability Assessment.

2. Assessment Report 06-03 (Issued March 31, 2006)

GPO Oracle Program Stakeholder Analysis

FINDING

The assessment identified several vulnerabilities associated with the GPO Oracle Program and made recommendations that would help mitigate risks associated with those vulnerabilities. The vulnerabilities identified during the assessment included (1) top management support not aligned with program execution; (2) inadequate functional and technical staffing; (3) lack of a methodology for organizational restructuring; (4) lack of targeted performance metrics; and (5) lack of an effective method for managing program progress.

RECOMMENDATION

To help ensure the Oracle Program meets expectations of its stakeholders, the OIG made 13 recommendations in the areas of staffing, management alignment and organizational restructuring, use of performance metrics, and management of program progress.

MANAGEMENT COMMENTS

Management concurred with each of the report's recommendations and agreed to take corrective actions throughout implementation of the project.

OIG COMMENTS

As of the end of this reporting period, six recommendations are open. Management is continuing to work on implementing corrective actions. We anticipate that the recommendations will be closed upon implementation of Oracle Release 2.

3. Assessment Report 07-01 (Issued November 20, 2006)

Report on Early Oracle Implementation: Independent Verification and Validation (IV&V)

FINDING

The OIG initiated IV&V activities beginning with two of the early implementation projects for Oracle. The objective of IV&V is to provide GPO with an independent assessment of project status, satisfaction of user needs, and project cost effectiveness. The OIG issued a sensitive report summarizing vulnerabilities identified during the IV&V activities.

RECOMMENDATION

The report contains 21 recommendations to management for strengthening controls and mitigating risks associated with the vulnerabilities.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed corrective actions.

OIG COMMENTS

As of the end of this reporting period, eight recommendations in this report are open. Management continues to work on implementing corrective actions.

4. Assessment Report 07-09 (Issued September 27, 2007)

Report on GPO's Compliance with the Federal Information Security Management Act (FISMA)

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, the GPO recognizes the need to be FISMA compliant because of the services it provides, including services to Executive Branch agencies. The OIG issued a sensitive report concluding that although the Agency has taken steps to comply with FISMA, additional progress is needed to fully comply.

RECOMMENDATION

The report contains 11 recommendations that if implemented will help move GPO toward FISMA compliance.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed corrective actions.

OIG COMMENTS

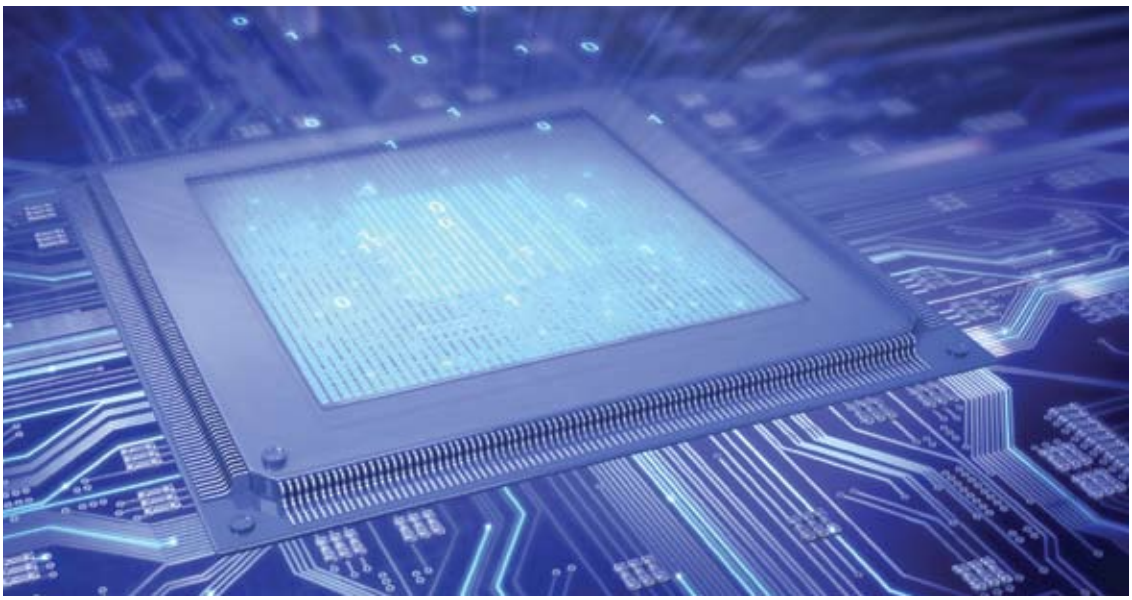
Management continues to work on implementing corrective actions for the seven remaining open recommendations.

5. Assessment Report 07-10 (Issued September 28, 2007)

Report on Perimeter Security Assessment of a GPO Building

FINDING

The Federal Protective Service (FPS), an organization within DHS, provides law enforcement and security services to the General Services Administration for federally owned and leased facilities. At the request of the OIG, FPS conducted a



physical security assessment of a GPO building. The FPS methodology for assessing security of the GPO building included (1) identifying existing countermeasures at the facility, (2) identifying credible threats to the facility, and (3) rating each threat as to potential impact of loss and vulnerability. The sensitive report contains recommendations intended to enhance security of the building.

RECOMMENDATION

The report contains 12 recommendations that if implemented will help enhance security of the building.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed corrective actions.

OIG COMMENTS

During this reporting period, management closed one of the remaining two open recommendations. One recommendation remains open. With proposed corrective actions in place, we anticipate closing the remaining open recommendation during the next reporting period.

6. Assessment Report 08-01 (Issued November 1, 2007)

GPO Network Vulnerability Assessment

FINDING

The OIG completed a vulnerability assessment of the GPO enterprise network infrastructure and evaluated the level of security controls in place that help protect the Agency's IT resources from unauthorized access and compromise. We limited our assessment to the area between GPO's Internet service provider and the outermost firewall interface where the Agency's publicly available network resources, such as GPO Access, are hosted. That area is commonly referred to as the demilitarized zone, or DMZ. We determined whether GPO (1) maintained a robust and effective vulnerability scanning and management program that identified and circumvented common internal and external threats to its network, (2) used passwords in the DMZ strong enough to prevent brute force attacks, and (3) patched systems in the DMZ in a timely and effective manner. The assessment revealed that there was room for improvement and recommended ways that would not only help strengthen security of the publicly available network resources but also reduce the risk of system compromise and loss of availability.

RECOMMENDATION

The report contains seven recommendations that if implemented will not only help strengthen network security but also reduce the risk of system compromise and loss of availability.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed corrective actions.

OIG COMMENTS

Two recommendations remain open. The status of these recommendations will be reviewed as part of the OIG's FY 2009 Network Vulnerability Assessment.

7. Assessment Report 08-04 (Issued March 28, 2008)

Federal Digital System (FDsys) Independent Verification and Validation (IV&V) – First Quarter Observations and Recommendations

FINDING

The FDsys program is a multimillion dollar effort that GPO is funding for modernizing information

collection, processing, and dissemination capabilities it performs for the three branches of the Federal Government. The OIG is conducting IV&V of FDsys implementation through a contract with an IT company. Between July and September 2007, the contractor completed its initial assessment of the FDsys prime contractor's program management practices used for the Release 1.B pilot system. The initial IV&V assessment showed that the prime contractor established a strong basis for good program management practices for Release 1.B. We did, however, identify some weaknesses that could lead to schedule risk and cost overrun for Release 1.C if not addressed in a timely manner. Those weaknesses included the following areas.

- insufficient use of earned value analysis
- lack of an Integrated Baseline Review
- incomplete adherence to risk management program
- risks associated with testing
- lack of system capabilities documentation
- insufficient Configuration Management Plan

RECOMMENDATION

The report contains 14 recommendations designed to strengthen management of the FDsys program.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and proposed responsive corrective actions.

OIG COMMENTS

During this reporting period, we worked with management to close one of the remaining three open recommendations. We anticipate closing the two open recommendations during the next reporting period.

8. Assessment Report 08-06 (Issued March 31, 2008)

Operating System Security for GPO's Passport Printing and Production System

FINDING

The Passport Printing and Production System (PPPS) includes various computer applications

and operating systems that support production of passports. The Agency's Plant Operations Division administers PPPS computer applications while its Chief Information Officer (CIO) is responsible for administering PPPS operating systems. If those operating systems are not configured securely, critical computer applications such as databases and custom applications are vulnerable to compromise. The risk associated with compromise to the operating systems hosting such critical applications could result in services being disrupted, sensitive information being divulged, or even subject to forgery. The OIG assessed the security configuration for selected operating systems that support production of passports to determine whether GPO enforces an appropriate level of security.

RECOMMENDATION

The OIG issued a sensitive report containing eight recommendations designed to not only help strengthen security of the PPPS but also reduce the risk of system compromise.

MANAGEMENT COMMENTS

Management generally concurred with each of the recommendations and proposed responsive corrective actions.

OIG COMMENTS

During this reporting period, the OIG worked with management to close seven of the eight recommendations. One recommendation remains open.

9. Audit Report 08-10 (Issued September 11, 2008)

Diversity Management Programs at GPO

FINDING

The OIG audited diversity management programs at GPO in response to a request from the Chairman of the Subcommittee on Federal Workforce, Postal Service, and the District of Columbia, of the House of Representatives' Committee on Oversight and Government Reform. The audit identified that although not mandated to comply with the guidelines and directives of the Equal Employment Opportunity Commission (EEOC) concerning model affirmative action programs, before the audit was conducted senior officials at GPO began adopting some elements of both EEOC Management Directive-715 (MD-715) and the leading diversity management practices identified by GAO. The audit also showed that opportunities exist for GPO to develop a more diverse population of qualified women and minorities in top leadership positions.

RECOMMENDATION

The OIG made two recommendations in the report: (1) incorporate the remaining essential elements of MD-715, and (2) implement the nine leading practices for diversity management identified by GAO. Such modifications should help the Agency manage its workforce, create an environment that helps diminish barriers for protected groups, and help attract and retain capable employees from diverse backgrounds.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and stated that implementation would require the Public Printer's review and approval.

OIG COMMENTS

The two recommendations remain open. During this reporting period, management has either begun implementing or plans to implement the remaining essential elements of MD-715 and the leading diversity management practices identified by the GAO. We anticipate that these recommendations should be closed during the next reporting period.

10. Assessment Report 08-12 (Issued September 30, 2008)

Assessment of GPO's Transition Planning for Internet Protocol Version 6 (IPv6)

FINDING

The OIG assessed Agency planning for transition from Internet Protocol version 4 (IPv4) to version 6 (IPv6). Internet routing protocols are used to exchange information across the Internet. Protocols are standards that define how computer data are formatted and received by other computers. IPv6 is a developing Internet protocol that will provide many benefits such as more Internet addresses, higher qualities of service, and better authentication, data integrity, and data confidentiality. The OIG assessment identified that GPO plans to transition to IPv6 as part of a broad acquisition plan that will update its IT infrastructure. The Agency has not finalized target dates for the

updates. The OIG believes that the planned transition is an effective long-term approach. In the short term, however, GPO should consider implementing the minimum IPv6 requirement, which should ensure that resources such as FDsys are capable of ingesting information from IPv6 sources.

RECOMMENDATION

The OIG made two recommendations to management that would enhance planning for the IPv6 transition.

MANAGEMENT COMMENTS

Management concurred with each of the recommendations and has either taken or planned to take responsive corrective actions.

OIG COMMENTS

As of this reporting period, one recommendation remains open. The recommendation will remain open pending completion of GPO's ongoing infrastructure refresh and approval of funding to proceed with IPv6.

OFFICE OF INVESTIGATIONS

OI is responsible for conducting and coordinating investigative activity related to fraud, waste, and abuse in GPO programs and operations. While concentrating our efforts and resources on major fraud investigations, the activities investigated can include possible wrongdoing by GPO contractors, employees, program participants, and others who commit crimes against GPO. Special Agents in OI are Federal Criminal Investigators (general schedule job series 1811) and are designated as Special Police Officers. Investigations that uncover violations of Federal law or GPO rules or regulations may result in administrative sanctions, civil action, and/or criminal prosecution. Prosecutions may result in court-imposed prison terms, probation, fines, or restitution. OI may also issue Management Implication Reports (MIR), which identify issues uncovered during an investigation it believes warrant management's prompt attention.

OI is responsible for investigations at all GPO locations, including the 15 GPO Regional Printing Procurement Offices (RPPOs) nationwide. OI also maintains a continuing liaison with the GPO Security Services and Uniform Police Branch, to coordinate efforts impacting these law enforcement programs. Liaison is also maintained with the Department of Justice (DOJ), the National Procurement Fraud Task Force (NPFTF) and other investigative agencies and organizations.

A. Summary of Investigative Activity

During this reporting period, the OI case tracking system was revised to create "complaint" files for conducting preliminary investigations. OI opened 51 complaint files; upon preliminary review 12 were converted to investigations, and 16 were closed with no further action. At the end of the last reporting period, 22 investigations were open and 5 of those are now closed. Ongoing at the end of this reporting period are 29 investigations and 23 complaints.

OI investigative activities and accomplishments are reported in the following categories below: Procurement Fraud, Workers' Compensation Fraud, Employee Misconduct, and Miscellaneous.

B. Procurement Fraud Investigations

OI seeks to uncover any wrongdoing by GPO contractors or employees during administration of GPO

contracts. Violations can include false statements, false claims, kickbacks, product substitution, collusive bidding, bribery, and financial conflicts of interest. GPO procures more than $750 million of goods and services each year through contracting. With this vulnerability in mind, OI has shifted much investigative development to procurement fraud. The inventory of procurement fraud complaints/investigations has increased from 7 last period to 21 procurement matters.

PROACTIVE EFFORTS

During September 2008, the OI staff attended the National Procurement Fraud Training in Richmond, Virginia, sponsored by the NPFTF. OI also provided procurement fraud presentations to GPO contracting personnel. Presentations were given to the following groups: GPO Print Procurement Managers, including regional management, Print Procurement Teams at GPO Headquarters, and RPPOs in the Columbus, Ohio and Chicago, Illinois offices.

Each presentation resulted in broad participation by attendees and valuable discussion about procurement fraud vulnerabilities at GPO. OI plans to provide the fraud presentation to the remaining RPPOs during the next semiannual period. Several proactive and audit projects are under consideration, based on input from GPO procurement personnel participating in the fraud briefings.

In March 2009, the OI staff met with an Agency procurement official who provided a detailed presentation on electronic procurement records at GPO. Additional training sessions are planned that should improve the effectiveness of OI procurement fraud investigations.

The Assistant Inspector General for Investigations and the SAC met with officials of the DOJ Antitrust Division, to facilitate development of investigations of interest to their office. Further discussions on specific investigations are anticipated.

ACCOMPLISHMENTS

An investigation of a GPO contractor resulted in the 3-year debarment of the company and company owner from doing business with GPO as a contractor, subcontractor, or contractor's representative.

The investigation revealed that the company submitted false delivery records to GPO to obtain payment before the actual production and/or delivery of completed products.

One investigation determined that during the performance of the contract, a vendor may have inappropriately disclosed PII. Because of the possible systemic nature of the issues identified, in February, the IG issued an MIR to the Public Printer. The OIG recommended that GPO identify any contracts and contractors handling PII, review security requirements, request security plans, conduct on-site surveys and inspections, and appoint a GPO Privacy or Data Security Officer to ensure integrity in the handling of PII. Although a response was due to the OIG in March, 2009, by the end of this reporting period, management had not provided its response.

Another OI investigation, worked in coordination with several other law enforcement entities, revealed fraudulent GPO and other Government purchase card transactions. OI participated in executing a search warrant at the target's residence. One individual has been charged, arrested, and pled guilty to fraud charges.

During this reporting period, three presentations were made to the DOJ for potential criminal and/or civil prosecution of OI procurement fraud investigations. Of those decisions, two are pending and the other resulted in a civil declination.

C. Workers' Compensation Fraud

OI investigates GPO employees who allegedly submit false claims or make false statements to receive workers' compensation benefits. We are working on six investigative matters involving possible fraudulent claims for workers' compensation.

OI's continued proactive, investigative approach and its working relationship with the GPO Health Unit and the Office of Workers' Compensation has also resulted in keeping Agency Sick Injured Administrative costs under $20,000 per month.

ACCOMPLISHMENTS

As reported earlier, an OI investigation resulted in a Department of Labor determination that an Office of Workers' Compensation Programs (OWCP) claimant—a GPO employee—made false statements from 2003 to 2007, claiming no earnings. The investigation revealed the employee owned rental property and that since 1998 had been acting as property manager, locating renters, collecting rents, and completing small repairs. A forfeiture of $226,821.74 was assessed, and the individual taken off OWCP rolls. A cost savings to the Government of $42,000 per year will also be realized ($420,000 in actuary amount over 10 years). During this period, OI provided additional information in response to questions from the Department of Labor Hearing Representative during an appeal. The Department of Labor decision was upheld.

D. Employee Misconduct

OI investigates allegations involving GPO employee misconduct. Allegations generally include misuse of Government computers, theft, assaults, drug violations, gambling, and travel voucher fraud. OI has nine open investigative matters involving alleged misconduct.

ACCOMPLISHMENTS

As a result of an OI investigation, three GPO employees agreed to plead guilty to one count simple assault, as part of a Deferred Sentencing Agreement executed on February 26, 2009, in Superior Court of the District of Columbia. The agreement requires that each defendant not violate any law or be rearrested, perform 40 hours of community service, not have any contact with the victim, and submit a resignation to GPO. The Factual Proffers state that in 2006 and 2007 one defendant pulled and twisted the victim's nose, pushing the victim's glasses into his face, another drew with red marker on the victim's neck, and the last hit the victim with a mallet. These are the final actions in this matter.

Another GPO employee was arrested after OI learned of an outstanding warrant for his arrest on assault charges. The employee failed to notify GPO of a court action, and GPO took administrative action against the employee.

After confirming the misconduct of a GPO employee, another administrative matter was referred to management for appropriate action.

When a related complaint was received, the matter was coordinated with the GPO Police and referred. No response is anticipated.

E. Miscellaneous

OI investigates miscellaneous administrative allegations and other types of investigations that do not fall into one of the categories above. Examples of such investigations include theft of Government property, illegal hacking, or request for investigations by other legislative agencies. OI has 16 open investigations involving miscellaneous allegations.

ACCOMPLISHMENTS

At the request of another legislative agency, OI investigated an alleged time card fraud by an employee of the other agency. The investigation confirmed the allegations, and the employee was terminated. The DOJ declined to prosecute.

In December, officials at GPO reported that 1 box from a shipment of 24 was not delivered to its destination. The box contained documents manufactured for the Department of Homeland Security (DHS) with sensitive PII. At the request of GPO officials, Special Agents from OI coordinated with the U.S. Postal Inspection Service, the U.S. Postal Service OIG, and the DHS OIG to assess the possibility of criminal wrongdoing. It was determined that the 24 boxes were misrouted and efforts to find the location of the missing box were expedited. The box was returned several weeks later, unopened, and intact. No evidence of criminal wrongdoing was identified.

An investigation determined that an independent contractor working in the GPO main building has an extensive criminal record and that an incorrect social security number was reported to GPO to obtain access to the building. After confirming the employee had never worked on GPO programs, the matter was referred to GPO security and the U.S. Capitol Police OIG to address possible security and systemic concerns. No official responses have yet been received.

After preliminary review, three incidents involving potential Title 44 violations were referred to the appropriate OIGs for action. The complaints alleged that other agencies may be in violation of Government printing laws and the Anti-Deficiency Act. Section 501, Title 44, United States Code requires that, with limited exceptions, GPO print all Government documents, including that of executive departments and agencies. In addition, section 207 of the Legislative Branch Appropriations Act, supplements section 501, by specifically prohibiting use of appropriated funds for most Government printing procured outside of the GPO. No official responses have been received.

F. Work-In-Progress

Other significant OI matters are pending as of the end of this reporting period. Disposition and results of those investigations will be provided in future reports.

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(s) is completed by the time agreement is reached.

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(s) of the finding(s) identified by the IG to take advantage of an opportunity.

Resolution - An agreement reached between the IG and management on the corrective action(s) 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
CCIG	Council of Counsels to the Inspector General
CFO	Chief Financial Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
DHS/CPB	Department of Homeland Security/ Customs and Border Patrol
DMZ	Demilitarized Zone
DOJ	Department of Justice
DOS	Department of State
ECIE	Executive Council on Integrity and Efficiency
FDsys	Federal Digital System
EEOC	Equal Employment Opportunity Commission
FIPS-201	Federal Information Processing Standard Publication 201
FISMA	Federal Information Security Management Act
FPS	Federal Protective Service
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
IPv6	Internet Protocol version 6
IT	Information Technology
IT&S	Information Technology and Systems
IV&V	Independent Verification and Validation
MIR	Management Implication Report
NFC	National Finance Center
OALC	Office of Administrative/Legal Counsel
OAI	Office of Audits and Inspections
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OWCP	Office of Workers' Compensation Programs
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PPPS	Passport Printing and Production System
PRA	Paperwork Reduction Act
RPPO	Regional Printing Procurement Office
SAC	Special Agent-in-Charge
SAS	Statement on Auditing Standards
SCC	Secure Credential Center
SID	Security and Intelligent Documents
SPF	Secure Production Facility
TTP	Trusted Traveler Program

Appendix B: Inspector General Act Reporting Requirements

Inspector General Act Citation	Requirement Definition	Cross-Reference Page Number(s)
Section 4(a)(2)	Review of Legislation and Regulations	6
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	7–14 15–26
Section 5(a)(2)	Recommendations for Corrective Actions	18–26 27–30
Section 5(a)(3)	Prior Audit Recommendations Not Yet Implemented	21–26
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	27–30
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)	15–21
Section 5(a)(8)	Statistical table showing the total number of audit reports and the total dollar value of questioned costs	35
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	36
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	1	$8,495
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	1	$8,495
■ 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

Audit Reports	Funds Put To Better Use
Report on Federal Digital System (FDsys) Independent Verification and Validation (IV&V) - Fourth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-01, issued November 4, 2008)	$0
Report on Audit of GPO's Passport Printing Costs (Audit Report 09-02, issued December 22, 2008)	$0
Report on FDsys IV&V – Fifth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-03, issued December 24, 2008)	$0
Report on FDsys IV&V – Security Analysis Report (Assessment Report 09-04, issued December 24, 2008)	$0
Report on FDsys IV&V – Release R1C.2 Pre-Deployment Status Report (Assessment Report 09-05, issued December 24, 2008)	$0
Report on the Consolidated Financial Statement Audit of the GPO for FYs Ended September 30, 2008 and 2007 (Audit Report 09-06, issued January 15, 2009)	$0
Report on FDsys IV&V – Sixth Quarter Report on Risk Management, Issues, and Traceability (Assessment Report 09-07, issued March 20, 2009)	$0
Report on Oracle E-Business Suite Release 2 IV&V – Technical (Assessment Report 09-08, issued March 31, 2009)	$0
Total	$0

Table C-4: Investigations Case Summary

Total New Hotline/Other Complaints Received during Reporting Period	51
No Formal Investigative Action Required	16
Cases Opened by OI during Reporting Period	12
Cases Open at Beginning of Reporting Period	22
Cases Closed during Reporting Period	5
Cases Open at End of Reporting Period	29
■ Cases Referred to GPO Management	3
■ Cases Referred to Other Agencies	9
■■ Cases Referred to OAI	0

Current Case Openings by Allegation	29	
Contract and Procurement Fraud	11	38%
Employee Misconduct	4	14%
Workers' Compensation Fraud	6	21%
Miscellaneous	8	27%

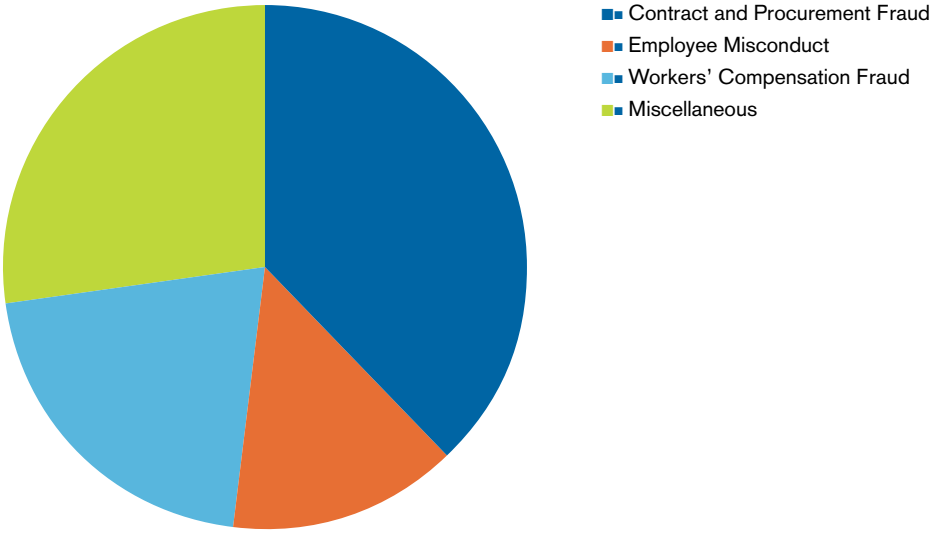


Table C-5: Investigations Productivity Summary

Arrests	2
Total Cases Presented to Prosecuting Authorities	3
Criminal	2
Criminal Declinations	0
Indictments	0
Guilty Pleas	4
Probation (days)	0
Jail Time (days)	0
Restitutions	$0
Civil	1
Civil Declinations	1
Amounts Recovered Through Investigative Efforts	$0
Total Agency Cost Savings Through Investigative Efforts	0
Total Administrative Referrals	4
Contractor Debarments	2
Contractor Suspensions	0
Contractor Other Actions	0
Employee Suspensions	0
Employee Terminations	0
Employee Warned/Other Actions	3
Other Law Enforcement Agency Referrals	8

OFFICE OF INSPECTOR GENERAL

732 North Capitol Street, NW, Washington, D.C. 20401
202.512.0039 I www.gpo.gov/oig
OIG HOTLINE 1.800.743.7574 | gpoighotline@gpo.gov