U.S. GOVERNMENT PRINTING OFFICE I KEEPING AMERICA INFORMED

OIG WorkPlan

U. S. Government Printing Office

Office of Inspector General

Updated:
March 13, 2009

732 North Capitol Street, NW ■ Washington, DC 20401-0001 ■ www.gpo.gov/oig

Introduction

The U.S. Government Printing Office (GPO) Office of Inspector General (OIG) maintains and periodically updates a work plan that helps fulfill its statutory mission. The work plan is an important OIG management tool and is used for planning and communicating audit and inspection objectives, allocating resources, and monitoring the progress of activities. Effective planning is an essential factor in maintaining a successful Agency audit and inspection program.

In developing this plan, the OIG staff evaluated the issues and realities facing GPO and its OIG. Senior OIG managers engage in constant outreach with GPO leaders, congressional staffs, and other stakeholders to solicit their ideas and obtain suggestions about areas for review. This plan is the result of such discussions. For each of the audits or inspections in this work plan, three basic types of information are presented:

1. **Background and Objectives.** What we intend to accomplish with each audit or inspection.

2. **Activities to be Reviewed.** Which area of GPO we plan to examine as part of the audit or inspection.

3. **Anticipated Benefits.** What value the audit or inspection is expected to provide to GPO.

We developed and updated this work plan to serve as a ready reference for focusing our efforts and keeping us on target. We see this plan as a "living document" that we will regularly revisit and revise when appropriate so it continues to reflect the needs of GPO.

Types of OIG Reviews

Federal Government OIGs are statutorily obligated to conduct audits, evaluations, inspections, and investigations. Only through such a broad array of tools can an OIG adequately review the variety of programs and operations in any department or agency, including GPO. Our precise approach differs depending on the particular program or problem of interest.

Audits

Audits may include performance audits, contract-related audits, or financial statement audits. Performance audits address the efficiency, effectiveness, and economy of an agency's programs, activities, and information technology (IT) systems. Contract-related audits review an agency's procurement activity, including compliance with laws, regulations, award terms, adequacy of internal controls, allowance of costs, and overall compliance with Federal procurement law. Financial statement audits are performed annually in accordance with Federal law, with the OIG acting as the Contracting Officer's Technical Representative (COTR) and overseeing the independent accounting firm that performs the audit.

Inspections

Inspections are reviews of agency activities, typically focused more broadly than an audit and designed to give agency managers timely and useful information about operations, including current and anticipated problems. Inspections are also sometimes referred to as evaluations, reviews, or assessments.

Investigations

Criminal, civil, or administrative investigations are conducted in response to allegations or suspicions of wrongdoing by agency employees or contractors. Investigations that uncover a violation of agency rules or Federal law can result in either administrative sanctions and criminal or civil prosecution, or both.

• Audit of GPO Financial Statements (Annual)

Background and Objectives

Federal law requires that GPO obtain an audit of the Agency's financial statements annually. In compliance with section 309(e)(1), title 44, United States Code, the Public Printer selects an independent public accounting firm to conduct the audit of the GPO financial statements.

Activities to be Reviewed

For this audit, we will monitor and manage the progress of the financial statement audit, including accepting the contractor's work. An OIG auditor will serve as COTR, overseeing the progress of the audit and the contractor's performance. A COTR is the principal liaison between the contractor and GPO management officials and ensures that when conducting the audit, the contractor complies with Generally Accepted Government Auditing Standards (GAGAS) and generally accepted auditing standards and attestation standards that the American Institute of Certified Public Accountants (AICPA) and the Financial Accounting Standards Advisory Board (FASAB) establish.

Anticipated Benefits

An unqualified opinion on its financial statements allows GPO to ensure its customers and the taxpayers that its financial operations are free from material misstatements and that its financial reports can be relied upon.

• Audit of GPO Regional Printing Procurement Office (RPPO) Activities

Background and Objectives

GPO's Regional Printing Procurement Offices (RPPOs) procure printing and binding for Federal agencies located in 10 Federal printing regions. Each of GPO's 15 RPPOs is responsible for developing and advertising specifications, awarding and administering contracts, and ensuring contract compliance.

This survey will examine the system of internal controls for the procurement of printed materials and conduct general testing to evaluate the appropriateness and effectiveness of key controls at specific RPPOs.

The overall objective of the survey will determine whether the RPPO fulfilled its mission to its Federal customer agencies. The three specific objectives of the audit are to determine (1) whether the RPPO is fulfilling the printing needs of the customer agencies in a timely manner and at a fair and reasonable price, (2) the adequacy and effectiveness of the system of controls in place against fraud, waste, abuse, and mismanagement, and (3) whether the procurement and related contracting practices of the RPPO are in compliance with the Printing and Procurement Regulations (PPR) and other applicable guidelines.

Activities to be Reviewed

We plan to survey the RPPOs and determine whether they are operating within the framework of GPO's Printing Procurement Regulation (GPO Publication 305.3). To that end, we will review acquisition activities and the proper use of competition, justification for sole-source acquisitions, contract administration, subcontracting, and product and contractor quality. We will also review contractors and their compliance with GPO regulations. We anticipate that the survey will identify several potential areas for future audits at the RPPOs.

Anticipated Benefits

This audit should identify opportunities for improving controls over RPPO acquisition activities and provide assurance that the activities are accomplished not only economically and efficiently but also in accordance with applicable GPO instructions and Federal laws and regulations.

• Digital Content Management System (FDsys) Independent Verification and Validation

Background and Objectives

The GPO digital information system is designed "to organize, manage, and output authenticated content for any use or purpose and to preserve the content independent of specific hardware or software so that it can be migrated forward and preserved for the benefit of future generations." Thus, the objectives of this system are: (1) authenticate digital Federal documents, (2) develop a responsible digital repository for all Federal documents—past, present, and future—that are within the scope of the Federal Depository Library Program (FDLP) of permanent preservation for public access, (3) have a single authoritative source from which masters can be made to create printed or digital copies of documents to meet Government, library and public needs, and (4) have the flexibility to expand beyond text to include other future formats such as full motion video and sound.

To achieve this goal, GPO is developing the Future Digital System, or FDsys. FDsys will be a comprehensive life-cycle management system developed by a joint GPO and master integrator team using a multi-release integration deployment. GPO committed to having the first public release of FDsys operational in January 2009.

The OIG is the Independent Verification and Validation (IV&V) agent for implementation of FDsys. We are conducting the IV&V through a contract with an outside vendor.

Activities to be Reviewed

We will conduct IV&V on all releases of FDsys to determine whether system implementation is consistent with the project plan and cost plan, and whether the delivered system meets GPO requirements. We will evaluate and monitor development as well as program management practices and processes for possible issues.

Anticipated Benefits

This IV&V activity will not only help GPO identify problems before the system is fully operational but should also help GPO meet required key system expectations.

• HSPD-12 – GPO Compliance with Federal Standards for Personal Identity Verification (PIV)

Background and Objectives

Homeland Security Presidential Directive 12 (HSPD-12) establishes the requirements for a common standard for identification credentials that Federal agencies issue to employees and contractors to gain physical access to federally controlled facilities and logical access to federal information systems. In response to HSPD-12, the National Institute of Standards and Technology (NIST) issued Federal Information Processing Standards (FIPS) No. 201, entitled "Personal Identity Verification of Federal Employees and Contractors," (FIPS 201). FIPS 201 specifies the architecture and technical requirements for a common identification standard, specifically "smart cards" that use integrated circuit chips to store and process data with a variety of external systems across Government. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical and logical access. FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications. In addition, a number of guidelines, reference implementations, and conformance test have been identified.

GPO plans to obtain the services of an in-house smart card vendor to produce smart cards for marketing to the Federal Government community. GPO will also use the vendor's services to implement a FIPS-compliant personal identity verification (PIV) system that will validate GPO employees and contractors requesting physical access to GPO facilities. The overall objective of this review is to determine whether GPO implemented a PIV system compliant with FIPS 201.

Activities to be Reviewed

The OIG will review controls over the PIV front-end subsystem and the PIV card issuance and management subsystem. We will review the adequacy of various GPO PIV processes, including (1) identity proofing, and registration, (2) card production, activation, and issuance, (3) card suspension, revocation, and destruction, and (4) card re-issuance to current PIV credential holders. We will also review the security certification and accreditation of the GPO PIV system.

Anticipated Benefits

The review should determine whether GPO implemented a PIV system that complies with FIPS 201 and that system controls and PIV processes are adequate.

- # GPO Enterprise Project (Oracle) – Independent Verification and Validation (IV&V)

Background and Objectives

GPO is migrating several legacy computer systems along with applications—business, operational, and financial and associated work processes—to an integrated system of Oracle enterprise software known as the Oracle E-Business Suite. The system can provide GPO with integrated and flexible tools that should help support the Agency's business growth and customer technology requirements for products and services. The migration includes replacing several computer systems and applications with systems software that is supportable and upgradeable. The migration also involves reengineering existing work processes and management reporting requirements, and establishing an IT environment that will accommodate growth, audit compliance, and disaster recovery capability.

The OIG is the IV&V agent for the GPO Oracle Enterprise project. We are conducting the IV&V through a contract with an outside vendor.

Activities to be Reviewed

Our ongoing IV&V efforts will continue to examine stakeholder issues, concerns, and expectations associated with implementation of the Oracle E-Business Suite. We will review costs, schedules, and risks associated with each of the Oracle module implementations.

Anticipated Benefits

The IV&V will identify risks and offer recommendations for mitigation of current and future risks in order to improve the probability of a successful implementation.

• Public Key Infrastructure Certification Authorities Assessment (Annual)

Background and Objectives

GPO's application of its "born digital and published to the Web" methodology for meeting customer expectations regarding electronic information dissemination and e-Government requires digital certification that documents within GPO's domain are authentic and official. To provide this digital authentication and to facilitate trusted electronic business transactions for Federal organizations and other non-Federal entities, GPO has developed a Public Key Infrastructure (PKI) Certification Authority (CA). In addition, GPO's PKI is cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification requires that the GPO PKI undergo an annual compliance assessment.

In addition to maintaining FBCA certification, GPO has submitted an application to the Federal Public Key Infrastructure Policy Authority (FPKIPA) Shared Service Provider Program (SSP) to obtain certification as a Qualified Bidder to provide managed PKI services that meet Government requirements. As part of this application, GPO must submit the results of various audits and assessments. The audit and assessment requirements mandated by the FPKIPA are evolving. The OIG works with GPO's Chief Information Security Officer to ensure that all audits and assessments are conducted as required.

Activities to be Reviewed

To satisfy FBCA requirements, the OIG will conduct a WebTrust[1] CA assessment or other acceptable assessments that meet FBCA requirements. These assessments will determine whether GPO assertions related to the adequacy and effectiveness of controls over its CA operations are fairly stated based on underlying principles and evaluation criteria. We will also determine whether the PKI CA system is being operated in accordance with its published Certificate Policy and Certificate Practice Statement.

Anticipated Benefits

The WebTrust assessment should help GPO maintain certification with the FBCA. The WebTrust assessment results in a WebTrust Seal that GPO can display on its Web site as a method of conferring confidence to a potential client.

[1] WebTrust principles and criteria for CA is a program of the American Institute of Certified Public Accountants.

- # Passport Inventory Tracking Subsystem – Information Technology Controls

Background and Objectives

GPO's e-Passport printing and production system (PPPS) uses commercial-off-the-shelf (COTS) operating systems and applications, and customized applications. The Formscan Sentinel system, a subsystem of PPPS, is a custom-built application that tracks embedded chips throughout the e-Passport production process at GPO. Sentinel also controls the movement of passports throughout their workflow. The application tracks chips from the time they arrive at GPO until they are shipped to the State Department as finished e-Passport books or returned to the vendor as defective. The metadata residing in the chips as shipped by the chip vendor is ingested into the application suite. Once ingestion is complete, GPO establishes and maintains tracking of individual chips. The metadata GPO maintains is designed to provide GPO passport productions meaningful reports, both for work in progress and historical functions.

Activities to be Reviewed

The OIG will examine the adequacy of IT controls implemented, intended to ensure functionality, security, and integrity of the system. The OIG will:

1. Review the functionality of the production application and determine if the subsystem meets GPO needs as well as if it was designed and implemented within contractual requirements. We will review (a) application facilities and employment for data persistence, (b) data encryption within the application suite, (c) failover capacity, (d) performance issues that may hinder Agency ability to query the system and generate production reports, and (e) gaps in the automation of manual processes

2. Review technical controls built into the application and determine whether controls meet the requirements of GPO, the Federal Government, and industry best practices. The OIG will determine whether technical controls were adequately tested before deployment.

3. Assess the security posture of the applications suite.

Anticipated Benefits

This review will help ensure that the PPPS inventory tracking subsystem meets GPO needs and is adequately protected from unauthorized compromise.

- # Production of Secure Federal e-Credentials – Information Technology (IT) Security Controls

Background and Objectives

As a provider of secure Federal e-Credentials to the Department of Homeland Security's Customs and Border Patrol Trusted Traveler program, GPO established an e-Credential production capability and related system. The system includes traveler data transmission capability, databases for temporary storage of traveler information, personalization capability, and other components.

Activities to be Reviewed

The OIG will examine the security posture of the system to ensure that the system and data, including any personally identifiable information, are adequately protected against unauthorized access and compromise. The OIG will review operating system security, database security, and telecommunications security as part of the assessment.

Anticipated Benefits

This review will help ensure that the system meets GPO and Federal IT security requirements.

• Review of the GPO Self-Service and General Stores

Background and Objectives

The GPO Self-Service Store has a variety of supplies and general items available for purchase for use throughout the Agency. GPO employees must be granted approval and authorization for using the store through the Self-Service Store access system. To use the store, an employee's supervisor requests authorization with a memorandum or e-mail. That document must include the employee's name, payroll number, and appropriate cost code. Once this information is entered in the access system, the employee can then use the store to make purchases by simply presenting their employee badge.

GPO also maintains an inventory of supply items that cannot be obtained from the Self-Service Store. Using the Customer Access Screen of the Materials Management Procurement and Control System (MMPCSII),[2] authorized users can order supplies, which are referred to as General Stores. This function allows users to search the General Stores Division inventory for stock items.

A recent investigation identified that an unauthorized GPO employee repeatedly obtained high-dollar items from the Self-Service Store and sold items outside GPO for personal gain. Although possibly an isolated incident, the potential does exist that the controls in both of the activities are not sufficient to prevent further fraud, waste, or abuse.

Activities to be Reviewed

For this audit, we will evaluate the Self-Service Store and the General Stores to determine whether adequate controls are in place that will prevent fraud, waste, and abuse. We will review any corrective actions management has taken since the theft of the items and whether the actions they took will prevent future thefts.

Anticipated Benefits

This audit should identify opportunities for improving controls over both the GPO Self-Service Store and the General Stores. The audit should further identify whether the two activities are being operated economically and efficiently.

[2] GPO uses both MMPCSII and Oracle for its inventory system.

• GPO Compliance with the Federal Information Security Management Act (Annual)

Background and Objectives

Building on the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Information Technology Management Reform Act of 1996, the Federal Information Security Management Act (FISMA) provides the basic statutory requirements for securing Federal computer systems. FISMA requires that each agency in the executive branch inventory its major computer systems. The goal of such an inventory is to identify and provide appropriate security protections as well as develop, document, and implement an agency information security program. FISMA also requires that each year executive branch agencies conduct an independent evaluation of their security programs. The evaluation must include an assessment of the effectiveness of the program, plans, practices, and compliance with FISMA requirements. FISMA requirements also extend to any systems that a contractor uses to support an executive branch agency.

FISMA has been deemed a critical best practice for Federal Government agencies. Although it has no specific congressional mandate, GPO should abide by the best practices of the Federal Government. Moreover, to the extent GPO is a "contractor" for agencies of the executive branch, those agencies require that GPO comply with FISMA.

Activities to be Reviewed

We conducted compliance assessments in fiscal years (FYs) 2007 and 2008 to identify ways that would help the Agency comply. Significant emphasis was placed on evaluating the GPO systems that service the executive branch. Our FY 2009 assessment will evaluate GPO compliance with FISMA as well as determine the extent to which GPO has implemented the recommendations in the previous assessments. As guidance, the assessment will use the FISMA requirements published by Office of Management and Budget (OMB) and NIST.

Anticipated Benefits

The FISMA assessment will enable GPO to identify IT vulnerabilities and take appropriate corrective measures. More importantly, the assessment will provide assurance to GPO customers that the Agency fully complies with established best practices.

- # Network Vulnerability Assessment (Annual)

Background and Objectives

The GPO Information Technology and Services (IT&S) environment includes Local and Wide Area Network facilities, an assortment of network servers, Internet-based applications, and a large number of Web sites that GPO maintains for other Federal agencies. Our assessment will determine whether sufficient protection controls were implemented on the GPO networks and related systems. Inadequate network security controls potentially expose the Agency to network instability and unauthorized compromise of systems and data.

Activities to be Reviewed

In our FY 2009 assessment, we will assess networks supporting passport printing and production[3] and GPO's public facing Web servers and evaluate the adequacy of controls on the GPO network from both an external and internal perspective. Our assessment will leverage the benchmarks published by the Center for Internet Security (CIS)[4] as well as network security requirements by the NIST. Our assessment will include (a) routers, (b) firewall policy and rule sets, (c) logging, (d) intrusion detection systems and network monitoring, (e) incident response, (f) Virtual Private Network devices, (g) Unix, Linux, and Windows operating systems, (h) network services, and (i) GPO's vulnerability scanning practices.

The assessment will use a combination of public and commercial assessment tools. Tools will include network device scanners, network-based vulnerability scanners, application-specific vulnerability scanners, and operating system utilities.

We will also follow up on the status of recommendations made in previous network vulnerability assessments. Penetration testing is not within the scope of this assessment.

Anticipated Benefits

This assessment may uncover vulnerabilities within the GPO network environment and inadequate processes over network management and GPO's network vulnerability management program that could put Agency systems and data at risk.

[3] Because of the unusual passport production in FY 2008, and concerns regarding network vulnerability scanning by the system owner and the Chief Information Security Officer, we deferred our assessment of this environment. In FY 2009, passport production declined, and the GPO IT security team will scan at regular intervals.
[4] CIS is a distributor of consensus best practice standards for security configuration. CIS benchmarks are widely accepted by Federal Government agencies, including GPO, for FISMA compliance.

• Audit of Oracle Database Security for GPO's Passport Printing and Production System (PPPS)

Background and Objectives

GPO's PPPS supports two production lines in Washington, D.C., and one production line at the alternative processing facility in Mississippi. PPPS comprises a series of integrated and related Oracle databases. The Formscan Sentinel system, which is a subsystem of PPPS, is a custom-built application integrated and reliant on Oracle databases for effective operation. The primary purpose of Sentinel is to track embedded chips throughout the e-Passport production process at GPO. Sentinel also controls movement of passports throughout their workflow.

Activities to be Reviewed

We will review the following key security controls associated with PPPS Oracle databases:

- Oracle encryption
- Authentication controls
- Security monitoring
- Database backup and recovery
- Vulnerability patch management
- Oracle network controls

Anticipated Benefits

The audit will determine whether GPO is adequately securing PPPS databases (and therefore related passport production data) to prevent unauthorized system and data compromise.

- # GPO Controls for Safeguarding Against and Responding to Breach of Personally Identifiable Information

Background and Objectives

Safeguarding personally identifiable information (PII) in GPO's possession and preventing its breach is essential toward ensuring that GPO retains the trust of its customers and employees. All GPO officials—including the Office of the Chief Information Officer and the General Counsel—share in the responsibility of safeguarding PII of customers and GPO employees. Those officials are accountable for administering operational, privacy, and security programs. FISMA and the Privacy Act require that agencies protect PII. In addition, OMB has issued guidance on PII.

GPO collects data from its customers and employees through the Internet, telephone, and email and physical mail. GPO should comply with laws and directives concerning the safeguarding of such critical data. Data containing PII are stored in various GPO computing systems.

Activities to be Reviewed

For this audit, we will identify and evaluate controls for computing systems that support electronic collection of PII of both customers and GPO employees. Using the Business Impact Analysis (BIA) study that the Gartner Group conducted, we will identify PII data flow and related systems. We will interview personnel across GPO business lines involved in collecting, disseminating, and retaining PII in electronic systems. We will also assess for compliance with laws and regulations those systems that collect personally distinguishable information (such as systems supporting GPO Bookstore purchases). We will also evaluate the breach notification policy and processes for GPO.

Anticipated Benefits

Our assessment should help GPO minimize risks associated with the collection and care of PII within the GPO lines of business.

• Review of the GPOExpress Program

Background and Objectives

GPO has initiated a convenience printing contract called GPOExpress. The contract with FedEx Kinko's allows Government personnel to use any FedEx Kinko's Office and Print Center throughout the United States and Canada to take care of small printing requirements. Using a GPOExpress card, agencies receive discounts and other benefits for their printing and finishing needs. Once a job is complete, GPO bills the customer agency.

Activities to be Reviewed

For this audit, we will assess the GPOExpress Program to determine whether the controls in place to prevent fraud, waste, and abuse are adequate. We will also review controls in place for ensuring that GPOExpress cards are adequately controlled and issued, contract terms between FedEx Kinko's and GPO are complied with, and GPO revenues reflect program activity. Finally, we will determine whether controls are adequate to ensure that only legitimate Government documents are being printed and that GPO is receiving copies of all documents being printed for posterity purposes.

Anticipated Benefits

This audit should identify opportunities for improving controls over the GPOExpress Program and determine whether the program is economical and efficient. The audit may also identify opportunities for increased revenues from the program.

- # Supplies and Materials

Background and Objectives

Federal law requires that the OIG audit GPO's financial and operational activities.[5] Although paper is the most significant cost component of supplies and materials used for printing, the category of supplies and materials also includes items such as personal computers, furniture, and office supplies. GPO reported $215 million for supplies and materials on the September 30, 2008, Consolidated Statements of Revenue and Expenses report.

Activities to be Reviewed

The audit will evaluate the increase in this account from $37 million in FY 2006 to approximately $215 million in FY 2008. In addition, the audit will review the appropriateness of transactions and related controls for supplies and materials. Our review will determine if (1) accounting methods used are appropriate, (2) recorded balances are accurately stated, (3) only authorized charges are posted to the general ledger, and (4) expenses are valid and properly supported. We will also evaluate the effectiveness of internal controls; account reconciliation procedures; and whether use of the account complies with applicable laws, regulations, policies, and procedures.

Anticipated Benefits

An audit of this account will help ensure that the Agency only makes charges that are appropriate. The audit should also provide additional assurance for the financial statement audit that information in the account is accurate and complete.

[5] 44 U.S.C. §309(d).

- # Deferred Revenue

Background and Objectives

Federal law requires that the OIG audit GPO's financial and operational activities.[6] Deferred revenues are funds received in advance from customers for the future delivery of goods and services ordered. For example, GPO defers the recognition of revenues for subscription services that will be provided to customers in the future. Customers pay for subscriptions to the Congressional Record, the Federal Register, and other publications in advance of delivery. The revenues from subscriptions are recognized as the periodicals are published and distributed to the subscribers. The unfilled subscription balance will be refunded in instances where the subscription is no longer available for sale, or the customer cancels their subscription.

GPO also defers the recognition of revenues for unfilled customer orders of publications and other information products until the orders are shipped. Additionally, GPO defers the recognition of revenues for advance billings to Federal Government customers. Advance billings are occasionally used to finance the cost of producing large printing and binding jobs. GPO subsequently recognizes the revenue as work is completed. In general, revenue is recorded when a customer delivers goods or when GPO performs a service. GPO reported approximately $89 million of deferred revenue in Note 8 of its September 30, 2008, consolidated financial statements.

Activities to be Reviewed

The audit will evaluate the appropriateness of deferred revenue transactions and the related controls. Our review will determine whether (1) accounting methods used for revenue recognition are appropriate, (2) recorded balances are accurately stated, (3) only authorized revenue is posted in the general ledger, and (4) revenue is valid and properly supported. The audit will also evaluate the effectiveness of internal controls; the account reconciliation procedures; and whether use of the account complies with applicable laws, regulations, policies, and procedures.

Anticipated Benefits

An audit of this account will help ensure that the Agency only makes charges that are appropriate. The audit should also provide added assurance for the financial statement audit that information in the account is accurate and complete.

[6] 44 U.S.C. § 309(d).

- # Passport Supply Chain Security

Background and Objectives

GPO is the sole source for the production, storage, and delivery of all U.S. passports and is responsible for the security and integrity of producing blank passports from the time the paper leaves the mill, through acquiring additional components, to the point when blank passports are delivered to the Department of State. The Security and Intelligent Documents (SID) business unit is responsible for ensuring the security and integrity of the various passport components as well as the respective supply chain of those components. Previous OIG reviews of legacy passport production identified missing critical core competencies and significant deficiencies with the manufacturing process, security of components, and the internal controls. While these recommendations have been resolved, the new electronic, machine-readable passports (e-Passports) are fast becoming the "gold standard" in identification. Any absence of adequate controls in the management of the supply chain could leave the integrity of e-Passports vulnerable to a variety of threats. Accordingly, the OIG will continue to review GPO's security over its passport components and supply chain to ensure the integrity and security of e-Passports production.

Activities to be Reviewed

The overall objective of the audit is to assess GPO's security over its passport components and supply chain.

Anticipated Benefits

This audit should determine whether GPO has adequate procedures in place including risk management, audits and inspection of various passport component suppliers to ensure that the supply chain is secure and that risks are being identified and mitigated including any single-source suppliers of critical passport components.

- # Passport Transportation Follow-Up

Background and Objectives

GPO's current Memorandum of Understanding (MOU) with the Department of State for manufacturing blank passport books states that title to the blank passport books is transferred to Department of State at the end of the GPO passport production line at the point when the product is transferred into the Department of State's consignment vault located on GPO premises. Despite this provision in the MOU, GPO contracts for secure delivery of blank passports to various Department of State locations where the passports are then personalized. In an earlier review, we identified that the process the GPO used to deliver the blank passports did not meet the increased need for secure delivery. GPO subsequently contracted with a different delivery service for the secure delivery of the passports to the various Department of State locations. This audit will evaluate the security over transportation of blank passports with the new contractor.

Activities to be Reviewed

For this audit, we will review the process for transporting and delivering blank passports from GPO facilities to the Department of State. We will examine the process as well as examine the ability to track and monitor delivery so blank passports are accounted for and delivered securely.

Anticipated Benefits

The audit will determine whether the process for transporting blank passports from GPO to Department of State passport locations is effective and meets the needs of GPO and the Department of State. The audit will also review the MOU provisions regarding transfer of passport title to determine whether GPO is adequately protected from liability during the transport of blank passports.

- # Passport Production Personnel Security

Background and Objectives

In addition to physical safeguards, thorough personnel hiring and clearance procedures are crucial toward guaranteeing the integrity and security of the blank passport process. The System Security Plan for the passport production portion of the PPPS refers to GPO Directive 825.2A, "Personnel Security Program," August 18, 2000, as the security policy for all personnel producing passports. According to that directive, no one is entitled to know, possess, or access national security information solely by virtue of that person's office, position, or security clearance. The directive further states that such information may be entrusted to only those individuals whose official Government duties require that knowledge or possession, and have been investigated and cleared for access. We will evaluate the personnel security process to ensure that those employees involved in producing passports comply with applicable policies and procedures.

Activities to be Reviewed

For this audit, we will identify Federal and Agency security policies that apply to the passport production process and test GPO compliance with those policies and procedures for personnel involved in producing, storing, and transporting passports.

Anticipated Benefits

Our evaluation will determine whether the personnel security process that supports producing, storing, and transporting passports is effective and meets the needs of both GPO and the Department of State.

• Review of the GPO Ethics Program

Background and Objectives

At its heart, the ethics program ensures management decisions are free of the appearance of any conflicts of interest by employees involved in decisions. Because the integrity of decision-making is fundamental to every Government program, the head of each agency has primary responsibility for day-to-day administration of the ethics program. GPO Directive 655.3A, "Standards of Conduct for Government Printing Office Officers and Employees," June 10, 1988, establishes standards of ethical and financial conduct for GPO employees, including consultants, advisers, and other special Government employees. Employees and special employees are expected to maintain high standards of honesty, integrity, impartiality, and other ethical and moral conduct as well as avoid any actions, whether on or off duty, that could reflect adversely on the GPO or Government service or jeopardize the employee's fitness for duty or effectiveness in dealing with other employees or with the public.

Activities to be Reviewed

For this audit, we will evaluate GPO compliance with applicable Government ethics laws and regulations, including GPO Directive 655.3A. Our review will determine whether GPO complies with applicable Federal ethics guidance related to (1) proscribed actions; (2) gifts, entertainment, and favors; (3) outside employment and activity; (4) financial conflict of interest; (5) misuse of information; (6) use of Government facilities, property, and staff; (7) indebtedness; and (8) general conduct prejudicial to the Government. We will also include a review of the ethics program structure, staffing, and controls to ensure that GPO's ethics program is consistent with best practices in the Federal Government for ethics training and compliance.

Anticipated Benefits

A review of the GPO ethics program will determine whether employees, including consultants, advisers, and other special Government employees, adhere to the standards set forth in applicable Federal guidelines. GPO's ethics program may also be compared against model ethics practices from other Federal agencies.

• Review of Energy Use at GPO

Background and Objectives

The U.S. Capitol Complex, which includes the House and Senate Office Buildings, the Library of Congress, the Botanic Garden, and the GPO building complex, is responsible for approximately 316,000 metric tons of greenhouse gas emissions a year—or the same as emissions from 57,455 cars. In a recently completed review, GAO reported that in the legislative branch fleet of more than 300 vehicles, not one hybrid electric vehicle exists. GAO also found that the largest source of greenhouse gas emissions (63 percent) was electricity purchased from an external provider that relies primarily on fossil fuel combustion. The second largest source of emissions (32 percent) was the combustion of fossil fuels in the Capitol Power Plant, which produces steam for the majority of buildings in the legislative branch. GAO found that a strategy for reducing emissions includes conducting energy audits that will identify and evaluate energy efficiency and renewable energy projects, as well as evaluating other emissions-reduction projects that may fall outside the scope of energy audits.

In 2008, GPO commissioned the Potomac Electric Power Company (PEPCO) to perform an energy conservation review. The purpose of the review was to identify potential energy conservation measures (ECMs) that would reduce energy consumption, energy costs, and develop preliminary costs and energy savings associated with implementing the recommended ECMs.

The preliminary report that PEPCO provided GPO showed that nine ECMs at a cost of approximately $18.5 million that, if implemented, would provide an annual estimated savings to GPO of $3.1 million.

Activities to be Reviewed

For this audit, we will review GPO's use of various energy sources to include whether a plan exists for scheduling and completing energy audits and whether a comprehensive plan exists for implementing energy-related projects, such as those identified by PEPCO, as part of an overall plan to reduce emissions, energy consumption, and energy costs.

Anticipated Benefits

The audit may identify potentially cleaner sources of energy for GPO or the ability to reduce overall energy use and thus resulting costs through and effective program of energy audits, ECMs and targeted projects.

List of Acronyms

AICPA	American Institute of Certified Public Accountants
BIA	Business Impact Analysis
CA	Certification Authority
CIS	Center for Internet Security
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf Software
ECM	Energy Conservation Measures
FASAB	Financial Accounting Standards Advisory Board
FBCA	Federal Bridge Certificate Authority
FDLP	Federal Depository Library Program
FDsys	Future Digital System
FECA	Federal Employees' Compensation Act
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPKIPA	Federal PKI Policy Authority
GAGAS	Generally Accepted Government Accounting Standards
GAO	Government Accountability Office
GPO	Government Printing Office
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IT	Information Technology
IT&S	Information Technology and Systems
ITS	Inventory Tracking System
IV&V	Independent Verification and Validation
MMPCSII	Materials Management Procurement and Control System
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OWCP	Office of Workers' Compensation Program
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PPPS	Passport Printing and Production System
RPPO	Regional Printing Procurement Office
SSP	Shared Service Provider