U.S. GOVERNMENT PRINTING OFFICE I KEEPING AMERICA INFORMED

OIG WorkPlan

U. S. Government Printing Office

Office of Inspector General

Updated:
October 12, 2007

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 and the Nation.

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.[1] In compliance with 44 U.S.C. § 309(e)(1), the Public Printer selects the 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 will ensure that the contractor conducts the audit in compliance 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 on.

[1] 44 U.S.C. § 309(d).

- # Survey of GPO Regional Printing Procurement Office (RPPO) Activities

Background and Objectives

One of the goals of the GPO Regional Printing Procurement Office (RPPO) is to meet the needs of GPO customers in geographic areas away from its central office in Washington, D.C. As the use of fax machines and the Internet have increased, the need for regional offices has decreased but not been totally eliminated. The number of regional offices and employees in the field has declined since a peak in the mid 1980s but the need for contact with customer agencies has continued. RPPOs' purpose is to deliver the best value product or service to the customer on a timely basis, while maintaining the public's trust and fulfilling public policy objectives. The RPPOs strive to satisfy customer agencies in terms of cost, quality, and timeliness of the delivered product or service.

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, Federal laws, and Federal 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) to authenticate digital Federal documents, (2) to 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) to 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) to 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, which is a computer system that will organize, manage, and output authenticated content for any use or purpose. In addition, FDsys will preserve content independent of specific hardware or software so that it can be migrated forward and preserved for the benefit of future generations. 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 release of FDsys operational in the spring of 2008.

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

Activities to be Reviewed

We will conduct IV&V on releases 1C, 2, and 3 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 ensure that GPO meets key system requirements and expectations.

- # HSPD-12 – GPO Compliance with Federal Standards for Personal Identity Verification

Background and Objectives

Homeland Security Presidential Directive 12 (HSPD-12), which the President signed on August 27, 2004, establishes the requirements for a common standard for identification credentials that Federal agencies issue to employees and contractors when they need to gain physical access to federally controlled facilities and logical access to federally controlled information systems. HSPD-12 directs the Department of Commerce to develop a Federal Information Processing Standard (FIPS) publication defining a common identification credential. In response to the directive, the Commerce Department's National Institute of Standards and Technology (NIST), issued FIPS 201, "Personal Identity Verification of Federal Employees and Contractors," on February 2005. FIPS 201 specifies architecture and technical requirements for a common identification standard—in other words, "smart cards" that use integrated circuit chips to store and process data with a variety of external systems throughout the Government. The goal of HSPD-12 is to achieve security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical and logical access.

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 system that will validate GPO employees and contractors requesting physical access to GPO facilities.

Activities to be Reviewed

For this review, we will determine whether GPO is in compliance with HSPD-12. We will evaluate adequacy of the vendor operations for the GPO smart card, including compliance with the GPO contract and adequate physical and logical security controls over smart card production.

Anticipated Benefits

The review will provide GPO and its smart card customers with assurance that GPO is using a personal identity verification system that complies with FIPS and that controls over production of the cards are adequate.

• Review of the GPO Strategic Real Estate Plan

Background and Objectives

GPO's real estate holdings consist of several, mostly contiguous, parcels of land totaling 8.5 acres between G Street and H Street, NW, on North Capitol Street, NW, in Washington D.C. Improvements on these parcels include four buildings with a combined area of 1.5 million square feet. To meet the continuing printing needs for Congress and Agency customers as well as provide for a modern information processing environment, the strategic vision for GPO calls for relocating the operations to a new facility that is better sized and equipped for the Agency's future requirements.

GPO proposed in its strategic vision to move its current facilities, which are considered uneconomic and functionally obsolete, to new facilities designed and equipped to meet its current mission and flexible enough to meet future requirements. This proposed trade of facilities was based on four general assumptions: (1) proceeds from transactions would pay all costs associated with new buildings, equipment, and moving expenses, (2) a new operating environment would lower GPO operating costs so that appropriation burdens would be reduced and sufficient cash flow generated to meet ongoing capital requirements, (3) financial transactions would be structured in a way that would permit the Federal Government to retain title to the real property situated on the west side of North Capitol Street and that any issues would be acceptable to Congress, and (4) GPO would retain a presence in the existing facilities, so that its headquarters would remain in the North Capitol Street complex.

Activities to be Reviewed

We will review GPO plans for a new primary facility to ensure that the plans are based on supported and documented economic assumptions and that the Government's future interests are adequately protected.

Anticipated Benefits

An independent review of GPO plans for acquiring new facilities will ensure that all applicable laws and regulations are followed, that Congress is kept informed, and that key decisions and assumptions that management made were thoroughly analyzed and documented.

• GPO Enterprise Projects (Oracle) Release 2 – Independent Verification and Validation

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. This 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.

As part of GPO Enterprise Projects Release 2, GPO will convert to Oracle systems that maintain information and data for inventories, cost ledger functionality, and procurements. Integrated inventories supporting plant production are intended to improve cash management and allow for improved control of inventory flows. Conversion of the cost ledger functionality to Oracle should improve the efficiency of procurement business processes. It will also enable GPO to provide procurement services to Congress and other customers in an emergency. Implementation of the remaining purchasing processes will allow for purchasing to be initiated through Oracle.

Activities to be Reviewed

Our ongoing IV&V efforts will continue to examine stakeholder issues, concerns, and expectations associated with implementation of the Oracle inventory and procurement modules. We will review costs, schedules, and risks associated with the inventory and procurement implementations during the IV&V.

Anticipated Benefits

IV&V will help identify any risks and offer recommendations for mitigation that should aid in successful implementation of the remaining Oracle modules. IV&V will also provide GPO management with timely identification of project vulnerabilities that, if not corrected, could result in failure of the software to meet GPO expectations. IV&V should increase the probability that project implementation is successful and that data have integrity.

• Public Key Infrastructure Certificate 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) Certificate Authority (CA).[2] In addition, GPO's PKI recently became cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification requires that the GPO PKI undergo an annual compliance review.

Activities to be Reviewed

For this review, we will conduct a WebTrust[3] CA assessment that satisfies annual compliance review requirements. We 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 GPO PKI CA system is being operated in accordance with its published Certificate Policy and Certificate Practice Statement.

Anticipated Benefits

The WebTrust assessment will help maintain GPO's certification with the FBCA. The assessment will also enable GPO to be included in the Microsoft Web cache that allows automatic signature authentication through Microsoft. 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.

---

[2] A PKI is defined as a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, which enable the creation and validation of secure digital signatures. These digital signatures provide secure confirmation to receivers of information that the information is authentic and official. A CA is the authority, comprised of Agency hardware, software, and operating personnel, that issues and manages the Public Key Certificates. The GPO Certificate Policy and Certificate Practice Statement defines the role of the CA in more detail. For more information please see *http://www.main.gpo.gov/its/pki/gpo_ca_cp_v1.0.1_20041001_latest.doc.*

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

- # Passport Inventory Tracking System

Background and Objectives

GPO is implementing an inventory tracking system (ITS) as part of the Passport Production System. The ITS will use the GPO PKI CA to pre-initialize chips embedded in Passports. The network infrastructure for GPO will enable ITS to communicate with chip manufacturers as well as the Department of State to coordinate and manage efficient production and tracking of Passports. The OIG conducts an annual assessment of GPO's CA.

Activities to be Reviewed

For this review, we will examine adequacy of the controls implemented through the ITS to track and account for Passport production, including chip inventory and unusable passport books.

Anticipated Benefits

This review will help ensure that the Passport production program meets Department of State and GPO requirements.

- # Review of Workers' Compensation at GPO

Background and Objectives

The Federal Employees' Compensation Act (FECA) establishes a comprehensive and exclusive workers' compensation program that pays compensation for disability or death of a Federal employee who sustains an injury on the job.[4] FECA, which the Office of Workers' Compensation Programs (OWCP) at the Department of Labor administers, provides benefits and compensation for total or partial disability, schedule awards for permanent loss or dismemberment of specified parts of the body, related medical costs, and vocational rehabilitation. GPO manages and administers its workers' compensation program in accordance with FECA. As of September 30, 2006, the estimated workers' compensation liability for the GPO was approximately $69.95 million.

Audits of workers' compensation programs for other agencies have identified issues that include inadequate monitoring of medical status and long-term cases, missed opportunities to return employees to work, improper payments related to schedule awards, and claimants earning and failing to report non-Federal wages. Those types of problems, if found to exist within the GPO program and if management adequately addresses them, could result in significant cost savings.

Activities to be Reviewed

For this audit, we will evaluate adequacy of the controls over the GPO workers' compensation program. We will determine whether (1) GPO complies with applicable Department of Labor laws and regulations relating to FECA, (2) documentation is appropriate and supports employee claims, and (3) GPO has sufficient return-to-work programs.

Anticipated Benefits

The audit will help ensure that appropriate controls are in place for the workers' compensation program at GPO. The audit will determine whether employees receiving workers' compensation are legally taking part in the program and whether returning to work or switching employees to a Federal retirement system are the appropriate actions.

[4] 5 U.S.C. 8101 et seq.

• Review of the GPO Payroll

Background and Objectives

The Human Capital process at GPO consists of detailed transactions associated with hiring employees and includes salary changes, time and attendance reporting, and preparation of payroll-related journal entries. The Human Capital process accounts for salaries, wages, and personnel benefits paid to employees in addition to the related deductions and employer contributions to others on behalf of the employees.

The National Finance Center (NFC) at the Department of Agriculture has been providing integrated payroll and personnel services to GPO since September 2003 through an interagency agreement. NFC disburses biweekly payroll to employees through either electronic funds transfer to the employee's financial institution or through a U.S Treasury check mailed to the employee's designated address. GPO reimburses NFC for payroll costs.

Activities to be Reviewed

For this audit, we will evaluate adequacy of the controls over payroll processing for which NFC is responsible. We will determine whether (1) reconciliations of payroll submitted to NFC are performed, (2) controls are in place over placing and removing employees to and from payroll, and (3) employees are paid at the appropriate rates of pay.

Anticipated Benefits

The audit will help ensure that appropriate controls are in place over payroll processes at the GPO. The audit will determine whether employees are correctly paid, that only legitimate employees are paid, and that controls are in place to ensure that employees leaving GPO are removed from the payroll system.

- # 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),[5] 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.

[5] 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 an independent baseline assessment of GPO compliance with FISMA in fiscal year 2007 and identified ways that would help the Agency comply. In that review, significant emphasis was placed on evaluating the GPO systems that service the executive branch. Our fiscal year 2008 review will also assess GPO compliance with FISMA as well as determine the extent to which GPO has implemented the recommendations in the baseline assessment. As guidance, the assessment will use the FISMA requirements published by 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.

• Transition Planning for Internet Protocol Version 6

Background and Objectives

Microsoft's Internet Protocol Version 6 (IPv6) is the most recent version available for transferring information from one computer to another.[6] IPv6 is now included as part of the IP support in many products, including major computer operating systems. The GPO network may already contain IPv6-capable software and equipment. One important improvement of IPv6 over IPv4 is relief of an impending shortage of network addresses. Another significant feature of IPv6 is that network security may be enhanced through its use. All agencies in the executive branch are required by June 2008 to use IPv6 on their network backbones. GPO may encounter some complexities, costs, and risks in transitioning from IPv4 to IPv6. The U.S. Computer Emergency Readiness Team (US-CERT) in the Department of Homeland Security has already issued an advisory relating to the security for IPv6.

Activities to be Reviewed

For this assessment, we will determine whether GPO has an adequate strategy and plan for transitioning its network to IPv6 and whether (and when) the agency will mitigate the known security risks. Our review will determine whether GPO is:

- Identifying the most effective transition method allowing GPO to use IPv4 and IPv6 without significant network interruptions
- Evaluating and mitigating security risks associated with IPv6-capable software and devices already in the network
- Developing an inventory of software and hardware to understand the scope of the IPv6 transition and to assist in focusing risk assessments
- Identifying how much IPv6 address space GPO needs
- Developing IPv6 transition policies and enforcement mechanisms
- Estimating costs of the IPv6 transition for projecting costs and integrating IPv6 requirements into acquisition requirements

Anticipated Benefits

Early and effective IPv6 planning should help ensure cost-effective transitions for the network without significant risk to its network and data.

[6] An IP is the method by which data are sent from one computer to another over the Internet. Each host computer on the Internet has at least one IP address that uniquely identifies it from all other computers. An IP is a core component to Federal agency IT infrastructures.

- # 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 this annual assessment, we will evaluate the adequacy of controls on the GPO network from both an external and internal perspective. We anticipate that we may review adequacy of the security controls associated with:

- Routers
- Firewalls
- Intrusion detection systems and network monitoring
- Incident response
- Virtual Private Network devices
- Unix, Linux, and Windows operating systems
- Network services

The assessment will use a combination of public and commercial assessment tools. Tools may 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.

Anticipated Benefits

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

- # Passport Production Systems – Host Operating System Security

Background and Objectives

The GPO passport production systems include operating systems that support various computing equipment and related software associated with the following:

- Formscan Sentinel Production Control System that serves as a central hub for IT activities
- Production Lines A and B
- Encoder servers
- Data servers

Our assessment of the passport production systems will determine if the Agency is enforcing the required level of security within the host operating systems supporting passport production systems. Security controls for operating systems are the foundation on which applications and other software security controls are built. If an operating system is not secure, then other layers of security within a system may not be effective. We will review the GPO policy for IT operating system security and review key controls for a sample of host operating systems that support passport production.

Activities to be Reviewed

We plan to assess the following security controls within the operating systems including (1) user and group access privileges, (2) local account policy, (3) user rights assignment, (4) system audit policy, (5) logging on and monitoring of system activity, (6) file permissions, and (6) operating system backup and recovery.

We will conduct this assessment using manual procedures and interfaces already available within the operating system.

Anticipated Benefits

The assessment will determine if an adequate level of security exists within the operating systems that support passport production. Weak security could result in a compromise to passport applications and data, including disruption in the production of passports.

- # 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 and 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 by the Internet, telephone, and physical mail, and should comply with laws and directives concerning safeguarding such critical data. The 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 will help GPO minimize the 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 GPOExpress Program 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. GPO awarded a contract to FedEx Kinko's Office and Print Services. 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 adequate controls are in place that will prevent fraud, waste, or abuse. We will review the 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.

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.[7] 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 $37 million for supplies and materials on its September 30, 2006, Consolidated Statements of Revenue and Expenses.

Activities to be Reviewed

For this audit, we will evaluate 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.

[7] 44 U.S.C. § 309(d).

- # Deferred Revenue

Background and Objectives

Federal law requires that the OIG audit GPO's financial and operational activities.[8] Deferred revenues are funds received in advance from customers for the future delivery of goods and services ordered. In general, revenue is recorded when a customer delivers goods or when GPO performs a service. GPO reported about $70 million of deferred revenue in Note 7 of its September 30, 2006, consolidated financial statements.

Activities to be Reviewed

For this audit, we 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.

[8] 44 U.S.C. § 309(d).

- # Invoice Payment Process

Background and Objectives

Federal law requires that the OIG audit Agency financial and operational activities.[9] GPO reported accounts payable and accrued expenses of $84 million on its September 30, 2006, consolidated balance sheet. Invoice payments are for items such as commercial billings, production materials, and services. Invoices for commercial billings are the largest component. The OIG is concerned that vendors do not receive payments timely and that GPO does not take full advantage of vendor discounts.

Activities to be Reviewed

For this audit, we will evaluate GPO processes and procedures that allow customers to be paid timely. Our review will (1) assess adequacy of the system for tracking invoices from receipt through payment of individual accounts payable, (2) determine whether any discounts are taken when presented on the invoice, (3) identify any duplicate invoice payments, (4) identify delays in the timely payment of invoices, and (5) review internal controls for the process.

Anticipated Benefits:

An audit of accounts payable and accrued expenses will identify any obstacles or possible obstacles for paying vendors timely and determine whether GPO takes advantage of vendor discounts. The audit should also identify whether the controls over the payment process are operating effectively.

[9] 44 U.S.C. § 309(d).

- # Blank Passport Security Follow-Up

Background and Objectives

GPO is the sole source for the production, storage, and delivery of all U.S. passports; therefore, loss or theft of any blank passport would have serious ramifications. GPO 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. In an earlier review, we identified missing critical core competencies, deficient processes, and missing infrastructure that would help sustain the long-term development of a security and intelligent document line of business. The OIG also identified significant deficiencies with the manufacturing of blank passports, security of components, and the internal controls for the process. At that time, GPO management conceptually agreed with our findings, but could not implement the recommendations because of monetary constraints and an evolving state of the GPO Security and Intelligent Documents Business Unit. As part of this review, we will reevaluate the security of blank passports.

Activities to be Reviewed

For this review, we will follow up on the recommendations made in the previous review to determine the extent to which GPO management, specifically the Security and Intelligent Documents Business Unit, implemented the critical core competencies, processes, and infrastructure necessary for blank passport security. We will then test the effectiveness of those competencies, processes, and infrastructure as part of this review.

Anticipated Benefits

This audit should determine whether systems and storage for passports are secure and that protocols are in place so that the Department of State will have an adequate supply of blank passports.

- # Passport Transportation Follow-Up

Background and Objectives

Transporting blank passports securely is of growing concern as the requirement increases for more passports. The annual Department of State requirement is now at 26 million passports. GPO is responsible for the security and integrity of blank passports while they are produced and until they are delivered to the Department of State. In an earlier review, we identified that the process the GPO contractor was using did not meet the increased needs for secure delivery. We made several recommendations for improving the process—to which GPO management generally agreed. In this review, we will reevaluate the security over transportation of blank passports.

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

Our updated evaluation 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.

- # Secure Production Facility

Background and Objectives

GPO has an agreement with the Department of State to be the sole source for producing, storing, and delivering U.S. passports. GPO and the Department of State have a passport production rate goal of 500,000 each week, or 26 million passports each year. GPO produces the passports at a facility in Washington, D.C. The Department of State has invested tens of millions of dollars in backup capabilities for supporting all aspects of the passport process. Establishing a second facility for producing passport at a secure location outside of the Washington, D.C., area is essential for continued production in the event of a disruption of services. GPO plans to establish a secure production facility utilizing facilities that the Department of Defense base realignment and closure process made available. We will evaluate Agency planning for this secure production facility and determine if the planning ensures that the facility will be completed on schedule, meets GPO requirements, and meets applicable Federal facility requirements.

Activities to be Reviewed

For this audit, we will evaluate GPO and Federal criteria as well as benchmarks for acquisition and facility management, review GPO documentation related to planning and implementing the secure facility, discuss the process with GPO officials, and conduct an on-site inspection of the proposed facility.

Anticipated Benefits

Effective planning for the secure production facility will ensure that the facility meets GPO and Department of State requirements as scheduled and within budget.

- # 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 Passport Printing and Production System (PPPS) refers to GPO Directive 825.2A, "Personnel Security Program," August 18, 2000, as the security policy for all personnel producing passports. According to GPO Directive 825.5A, 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 purpose of an ethics program is to ensure that management decisions are free of even 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 the day-to-day administration of the ethics program. GPO Directive 655.3A, "Standards of Conduct for Government Printing Office Officers and Employees," dated 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 GPO Directive 655.3A. Our review will determine whether GPO complies with the Directive 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 Federal government best practices for ethics training and compliance programs.

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 policy. The review will also determine whether the policy is effective and up to date.

- # Review of the Federal Depository Library Program

Background and Objectives

The Federal Depository Library Program (FDLP) requires that Government publications (with some exceptions) must be available for depository libraries.[10] GPO disseminates U.S. Government publications and information. The mechanism for making information available is the FDLP. Federal Depository Libraries are in the 50 states, the District of Columbia, and U.S. territories. The program provides Government information at no cost to certain depository libraries. These depository libraries, in turn, provide local, no-fee access to Government information in an impartial environment with professional assistance.

Activities to be Reviewed

For this audit, we will review the effectiveness of how the FDLP is run and how efficiently it provides information.

Anticipated Benefits

The review may determine that the FDLP can either be operated and run more effectively or more efficiently, or whether more efficient and effective operations can be used to ensure that depository libraries receive and make official Government documents available to the public.

[10] 44 U.S.C. § 1902.

• Review of Energy Use for 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. Since 1998, the Architect of the Capitol, GAO, and GPO have commissioned 11 energy audits for some of their facilities, but the audits were not generally comprehensive and the agencies varied in the extent to which they implemented the projects identified through the audits. Another part of a strategy for reducing emissions would involve evaluating the cost-effectiveness, emissions reduction, and funding options of projects that fall outside the scope of energy audits, such as acquiring fuel-efficient vehicles on a case-by-case basis.

Activities to be Reviewed

For this audit, we will review GPO 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 as part of an overall plan to reduce emissions that considers cost-effectiveness, the extent to which the projects reduce emissions, and funding options.

Anticipated Benefits

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

List of Acronyms

AICPA	American Institute of Certified Public Accountants
BIA	Business Impact Analysis
CA	Certificate Authority
COTR	Contracting Officer's Technical Representative
FASAB	Financial Accounting Standards Advisory Board
FBCA	Federal Bridge Certificate Authority
FDLP	Federal Depository Library Program
FECA	Federal Employees' Compensation Act
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAGAS	Generally Accepted Government Accounting Standards
GAO	Government Accountability Office
GPO	Government Printing Office
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IPv6	Internet Protocol version 6
IT	Information Technology
IT&S	Information Technology and Services
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
PKI	Public Key Infrastructure
PPPS	Passport Printing and Production System
RPPO	Regional Printing Procurement Office
SSP	Shared Service Provider