U.S. GOVERNMENT PRINTING OFFICE I KEEPING AMERICA INFORMED

OIG WorkPlan

U. S. Government Printing Office

Office of the Inspector General

Updated:
July 28, 2006

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 to facilitate the accomplishment of its statutory mission. The work plan is an important OIG management tool used to plan and communicate audit and inspection objectives, allocate resources, and monitor progress. Quality planning is an essential factor in maintaining a successful agency audit and inspection program.

In developing this plan, the OIG staff evaluates the various issues and realities facing the GPO and its OIG. Senior OIG managers engage in constant outreach with GPO leaders, Congressional staffs and other stakeholders to solicit their ideas and suggestions about potential areas for review. This plan reflects those discussions. For each of the audits or inspections in this work plan, three basic types of information are provided:

1. **Background and Objectives.** What we intend to accomplish by the audit or inspection.

2. **Activities to be Reviewed.** What areas of GPO will be examined 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 to focus our efforts and keep us on target, given our mandate and available resources. We also want to emphasize that we see this plan as a "living document" that we will regularly revisit and revise when appropriate to ensure that it will continue to reflect the needs of the GPO and the nation.

Types of OIG Reviews

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

Audits

Audits may include performance audits, contract-related audits, and financial statement audits. Performance Audits address the efficiency, effectiveness, and economy of the agency's programs, activities, and information technology (IT) systems. Contract-related audits review the agency's procurement activity, including compliance with laws, regulations, and 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 and generally overseeing the independent accounting firm tasked with performing the audit.

Inspections

Inspections are reviews of agency activities that are typically focused more broadly than an audit and are 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/Administrative Investigations are conducted in response to allegations or suspicions of wrong-doing by agency employees or contractors. Investigations that uncover a violation of agency rules and/or Federal law can result in administrative sanctions and/or criminal or civil prosecution.

• Fiscal Year 2006 Audit of GPO's Financial Statements

Background and Objectives:

In compliance with Section 309(e) of Title 44, United States Code (U.S.C.), an independent external auditor selected by the Public Printer has audited the GPO's financial statements annually since FY 1997. Prior to the passage of the General Accounting Office (GAO) Act of 1996 (Public Law 104-316, October 19, 1996), the GAO was required by 44 U.S.C. 309(d) to audit GPO's financial statements at least once every three years. GPO has received an unqualified opinion for each year for which an audit was completed since FY 1982, the first year a financial statement audit of GPO was performed by the GAO. Since 1992, financial statement audits have been performed by an independent public accounting firm.

Activities to be Reviewed:

The OIG is responsible for monitoring and overseeing the progress of the audit and for accepting the contractor's work. Specifically, an OIG auditor serves as the Contracting Officer's Technical Representative (COTR), overseeing the progress of the audit and the contractor's performance. The COTR serves as 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 established by the American Institute of Certified Public Accountants (AICPA) and the Financial Accounting Standards Advisory Board (FASAB).

Anticipated Benefits:

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

• Survey of GPO Acquisition Activities

Background and Objectives:

One of the goals of GPO's Acquisition Services organization is that the agency will acquire all needed goods and services in an efficient manner using state of the art acquisition techniques and tools. The vision of GPO's Acquisition System is to deliver on a timely basis the best value product or service to the customer, while maintaining the public's trust and fulfilling public policy objectives. The GPO Acquisition Regulation states that the system will: (1) satisfy the customer in terms of cost, quality, and timeliness of the delivered product or service by, for example— (i) maximizing the use of commercial products and services; (ii) using contractors who have a track record of successful past performance or who demonstrate a current superior ability to perform; and (iii) promoting competition; (2) minimize administrative operating costs; (3) conduct business with integrity, fairness, and openness; and (4) fulfill public policy objectives.

A review of purchase card activities at GPO identified several weaknesses related to controls over acquisitions using the cards. These weaknesses potentially increase the exposure of the GPO to instances of fraud, waste, or abuse. The potential exists that weaknesses in the acquisition area could lead to an even more significant exposure of the GPO to potential fraud, waste, and abuse.

Activities to be Reviewed:

We plan to conduct an overall survey of GPO acquisition activities to include reviewing proper use of competition, justification for sole source acquisitions, contract administration, subcontracting, and product and contractor quality. We also will review the acquisition activities of the GPO Regional Printing Procurement Offices, specifically the area of printing procurements for other Government agencies. It is anticipated that the completed survey will identify several potential future audits in the acquisition area.

Anticipated Benefits:

This audit should identify opportunities to improve controls over GPO's acquisition activities and provide assurance that these activities are being accomplished not only economically and efficiently, but also in accordance with applicable GPO instructions and federal laws and regulations.

• Digital Content Management System Independent Verification and Validation

Background and Objectives:

GPO's strategic plan, *A Strategic Vision for the 21st Century*, contains as one of the GPO's primary goals to "develop a flexible digital information content system for Federal documents to have (1) a single authoritative resource to authenticate digital Federal documents, (2) 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) 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) the flexibility to expand beyond text to include other future formats such as full motion video and sound.

The strategic vision further states that GPO's future operations will revolve around the GPO developed Digital Content System 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. In May 2005, GPO received approval from Congress to reprogram $23.7 million in unexpended prior year appropriations and transfer the funds to the GPO revolving fund where they would be earmarked for acquisition of the Digital Content System (designated by GPO as "FDsys"). FDsys will be a comprehensive lifecycle management system composed of six solution clusters (Content Management, Content Preservation, Content Access, Content Delivery, Content Submission, and Infrastructure). It will be developed by a joint GPO and Master Integrator (MI) team using a multi-release integration deployment. GPO is committed to having Release 1 operational by July, 2007.

The GPO OIG is responsible for Independent Verification and Validation (IV&V) efforts associated with the FDsys implementation efforts. IV&V for pre-award acquisition work for the MI contract is being conducted by GPO through a contract with an outside vendor.

- **Digital Content Management System Independent Verification and Validation (continued)**

Activities to be Reviewed:

We plan to conduct IV&V on each release of FDsys (Release 1, 2, and 3). Primary IV&V activities will include the review and evaluation of:

- Overall program management effectiveness, including:
    - Validation of development processes, including change management and risk management requirements,
    - Application of Earned Value Management for managing program progress

.

- Design Validation Test Plan and results.
- System security plan and implementation to ensure substantial compliance with Federal requirements for federal information system security.
- Regression testing used to identify the adverse impacts of change.
- Transition of operations to GPO, if required.
- Integration of legacy applications, if required.
- Training for each FDsys release.

Anticipated Benefits:

This review will determine whether the delivered system meets all of GPO's key requirements and expectations.

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

Background and Objectives:

Homeland Security Presidential Directive 12, signed by the President on August 27, 2004 (HSPD-12), established the requirements for a common standard for identification credentials issued by Federal agencies to employees and contractors for gaining physical access to federally controlled facilities and logical access to federally controlled information systems. HSPD-12 directed the Department of Commerce to develop a Federal Information Processing Standard (FIPS) publication to define a common identification credential. In response, the National Institute of Standards and Technology issued FIPS 201 – "Personal Identity Verification of Federal Employees and Contractors", dated February 2005. The standard specified 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.

GPO plans to obtain the services of an in-house smart card vendor to produce smart cards for marketing to the Federal government community. Additionally, GPO will use the services of the vendor to implement a FIPS compliant turnkey personal identify verification system that will validate GPO employees and contractors requesting physical access to GPO facilities.

Activities to be Reviewed:

The review will determine whether GPO has established a FIPS compliant personal identify verification system. In addition the review will evaluate the adequacy of GPO's smart card vendor operations, including compliance with GPO's 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 FIPS compliant personal identity verification system and that controls over the production of smart cards are adequate.

• Review of the GPO Strategic Real Estate Plan

Background and Objectives:

GPO's real estate holdings currently consist of several, mostly contiguous, parcels of land totaling 8.5 acres between G and H Streets on North Capitol Street, NW, Washington D.C. Improvements on these parcels include four buildings with a combined area of 1.5 million square feet. To meet continuing printing needs of Congress and agency customers, and provide for a modern information processing environment, GPO is considering relocating to a new facility sized and equipped for the agency's future requirements. GPO's current buildings are both too large and too antiquated and continue to drain the GPO of vital resources needed for investments in new technology.

As part of GPO's strategic vision, GPO proposes to trade its current facilities, which are not economic and functionally obsolete, for new facilities designed and equipped to meet its current mission and flexible enough to expand or contract to meet future requirements. This proposed trade of facilities is based on the assumptions that the (1) proceeds from the transaction are sufficient to pay all costs associated with new buildings and equipment and moving expenses, (2) new operating environment lowers GPO's operating costs so that appropriation burdens may be reduced and sufficient cash flow is generated to meet ongoing capital requirements, (3) financial transaction be structured in a fashion that permits the Federal Government to retain title to the real property situated on the west side of North Capitol Street, and that any scoring issues be acceptable to Congress, and (4) GPO retains a presence in the existing facilities, so that its headquarters can be said to remain in the North Capitol Street complex. The GPO has retained the services of a consultant to assist in the development process.

Activities to be Reviewed:

We will review GPO's plans for both a new primary facility and backup facility to ensure that they 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's plan for acquiring new facilities will ensure that all applicable laws and regulations are followed, that Congress is kept appropriately informed and that key decisions and assumptions made by management have been thoroughly analyzed and appropriately documented.

- # GPO Enterprise Projects (Oracle)

Background and Objectives:

GPO is migrating current business, operational, and financial systems, including associated work-processes, to an integrated system of Oracle enterprise software and applications with the strategic purpose of providing GPO with integrated and flexible tools to successfully support business growth and customer technology requirements for products and services. This migration will include replacing current legacy systems and applications with supportable and upgradeable integrated systems software and applications, reengineering existing legacy work processes and management reporting requirements, and, establishing an IT environment to enable growth, audit compliance, and disaster recovery capability. The OIG will conduct a minimum of two reviews including a risk assessment, and at least one independent validation and verification (IV&V) effort to expose and mitigate risks.

Activities to be Reviewed:

a) **Oracle Enterprise Project Risk Assessment**
The risk assessment will examine stakeholder issues, concerns, and expectations, as well as project integration/ implementation and execution.

b) **Oracle Enterprise Project IV&V (Phase 1)**
This phase will examine costs, schedules and risks associated with the implementation of the HR SF-52 application and its interface to NFC Payroll, as well as the implementation of the sub-store 9916 “procure-to-pay” project.

c) **Oracle Enterprise Project IV&V (Phase 2)**
This phase will examine the Incremental Operating Capability (IOC), including review of applicable master schedules, milestones, implementation requirements, design documents and other deliverables to ensure successful deployment.

Anticipated Benefits:

These inspections will identify risks and recommend mitigation efforts to ensure successful implementation of the GPO Enterprise program. The risk assessment will provide management a list of project vulnerabilities that, if not corrected, may result in the failure of the software to meet the expectations of the stakeholders and the Public Printer. The IV&V work will ensure that project implementations are successful, ensure the integrity of data, and advise management as to the reliability of the data.

- **Blank Passport Security**

Background and Objectives:

The GPO OIG has issued several reports concerning blank U.S. passport manufacturing, transportation, and security. Significant issues concerning the security of blank passports continue to require the attention of the OIG. Senator Susan Collins, Chairman of the Senate Committee on Homeland Security and Governmental Affairs, recently observed that:

> Fraudulent travel documents are essential to terrorists, and the U.S. passport is the gold card of travel documents. As the 9/11 Commission found: 'For terrorists, travel documents are as important as weapons.' Protecting the integrity of the U.S. passport is essential to protecting our citizens from those who would do harm to our nation. In fact, former Secretary of State Colin Powell said that ensuring a failsafe passport system is "a critical component of our global effort to fight terrorism."

Protecting the integrity of the U.S. passport cannot be done without first ensuring the security and integrity of the manufacturing process. Due to the increasing threat of a natural or other disaster, GPO bears significant responsibility to ensure a "failsafe passport system."

Activities to be Reviewed:

In the next several months, the OIG intends to examine several issues including the options available for storage of excess blank passports to ensure their security and availability in the event of a natural or other disaster, GPO's ongoing ability to manufacture blank U.S. passports in the event of a natural or other disaster, and other potential risks associated with passport production.

Anticipated Benefits:

Determination that systems and storage are secure and continuing operations protocols are in place so that the Department of State will have an adequate supply of blank U.S. passports for issuance to citizens of the United States.

• E-Passport Inventory Tracking System

Background and Objectives:

GPO plans to implement an inventory tracking system (ITS) as part of the Passport Printing and Production System. GPO expects to have hard requirements established by the end of July, 2006. This review will examine the adequacy of controls implemented through the ITS to track and account for e-passport production. GPO's Public Key Infrastructure Certificate Authority (CA) is one of the subsystems to be used by the ITS to pre-initialize chips embedded in the e-Passports. GPO's network infrastructure will enable the ITS to communicate with the chip manufacturers as well as the Department of State. The OIG is currently conducting an audit of GPO's CA.

Activities to be Reviewed:

TBD – Upon finalization of ITS requirements, the OIG workplan will be updated accordingly.

Anticipated Benefits:

TBD

- **PKI Certification and Accreditation (Shared Service Provider)**

Background and Objectives:

General Services Administration (GSA) has created the Shared Service Provider (SSP) Program to provide strong government oversight of government and commercially managed PKI service providers. Per Office of Management and Budget (OMB) policy, the SSP program will require federal agency use of an SSP in lieu of individual agency PKI stand up. Accordingly, since GPO has an existing PKI Certificate Authority, it is imperative for GPO to become an SSP. Third party audit is an integral requirement to SSP certification.

Activities to be Reviewed:

The OIG will conduct a "Webtrust" audit to include technical qualification assurance testing of the GPO PKI operation.

Anticipated Benefits:

Principally, the Webtrust audit will allow GPO to expand its PKI services to other agencies, to include the HSPD-12 deployment in the Federal Government. In addition, the Webtrust audit would enable GPO to be included in the web cache for Microsoft. The practical effect of this inclusion would be automatic signature authentication through Microsoft which will facilitate easy and cost-effective use of the GPO PKI Certificate Authority.

- # GPO's Revenue and Expense Account #6612

Background and Objectives:

The GPO Office of Finance and Administration establishes the agency's listing of revenue and expense accounts and object classes for its financial statements and general ledger. Account 6612 is for "General Supplies and Materials." Various GPO departments charge an annual average of approximately $7 million to this account. Because of a continuing increase in expenses charged to this account, the GPO Chief Financial Officer (CFO) requested that the OIG review charges to the account to determine their appropriateness and ensure that they were properly charged to the account.

Activities to be Reviewed:

The overall objective of the audit is to evaluate the appropriateness of transactions within GPO General Supplies and Materials Account #6612. The specific audit objectives are to (1) determine whether GPO has implemented appropriate management controls over transactions charged to the account; (2) evaluate the effectiveness of the procedures used to reconcile the account; and (3) determine whether the account is being used in compliance with applicable laws, regulations, policies, and procedures.

Anticipated Benefits:

An audit of this account will help ensure that only appropriate charges are made to account #6612. Further, the audit should identify whether any GPO organizations are incorrectly charging expenses for items such as travel and training to the account and whether the account accurately represents appropriate charges.

• Review of Worker's Compensation at GPO

Background and Objectives:

The Federal Employees' Compensation Act (FECA), 5 U.S.C. 8101 et seq., establishes a comprehensive and exclusive workers' compensation program which pays compensation for the disability or death of a federal employee resulting from personal injury sustained while in the performance of duty. The FECA, administered by the Office of Workers Compensation Programs (OWCP) at the Department of Labor, provides benefits for wage loss compensation for total or partial disability, schedule awards for permanent loss or loss of use of specified members of the body, related medical costs, and vocational rehabilitation. It is the policy of GPO to manage and administer its Workers' Compensation Program in accordance with FECA. As of September 30, 2005, the total workers compensation liability estimate for the GPO is approximately $76.1 million.

Examples of findings from audits of other agency workers' compensation programs 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. These types of problems, if found to exist within the GPO program, and if adequately addressed by GPO management, could result in significant cost savings.

Activities to be Reviewed:

The overall objective of the audit is to evaluate the adequacy of controls over GPO's workers compensation program. Specific objectives will be to determine whether (1) GPO complies with applicable Department of Labor laws and regulations relating to FECA, (2) documentation is appropriate to support employee claims, and (3) GPO has sufficient return-to-work programs.

Anticipated Benefits:

The audit will help ensure that appropriate controls are in place over the workers' compensation program at GPO. The audit will determine whether employees receiving workers' compensation are legally taking part in the program and whether return-to-work or switching the employee to the Federal retirement system is an appropriate course of action.

• Review of GPO Payroll

Background and Objectives:

The Human Capital process of the GPO consists of detailed transactions associated with the hiring of an employee 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 GPO employees in addition to the related deductions and employer contributions to others on behalf of the employees.

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

Activities to be Reviewed:

The overall objective of the audit is to evaluate the adequacy of controls over payroll processing by the NFC. Specific objectives will be to determine whether (1) reconciliations of payroll submitted to NFC and actually paid are performed, (2) controls are in place over placing and removing employees to and from payroll, and (3) employees are being paid at the appropriate rates of pay.

Anticipated Benefits:

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

- # Passport Transportation Follow-Up

Background and Objectives:

This inspection will follow-up a previous inspection report entitled "Blank Passport Transportation Security." The review will evaluate the implementation of several recommendations made to GPO management.

Activities to be Reviewed:

The OIG will review the delivery process at various passport facilities. More specifically, the OIG will examine the transportation and delivery process, as well as examine the ability to track and monitor the delivery process.

Anticipated Benefits:

Updated evaluation of whether the process for transporting blank U.S. passports from the Government Printing Office to the several U.S. Department of State (DOS) passport locations, is effective and meeting the needs of the GPO and DOS.

- # FISMA Review

Background and Objectives:

Building upon 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 Act of 2002 (FISMA) provides the basic statutory requirements for securing federal computer systems. FISMA requires each Executive branch agency to inventory its major computer systems, to identify and provide appropriate security protections, and to develop, document, and implement an agency-wide information security program. FISMA also requires that Executive branch agencies conduct annually, an independent evaluation of their security programs which includes an assessment of the effectiveness of the program, plans, and practices, and compliance with FISMA requirements. The FISMA requirements also extend to contractor systems that support an executive branch agency.

FISMA is a critical "best practice" for federal government agencies. Notwithstanding the absence of specific congressional mandate, in light of GPO's direction and vision, GPO should abide by the best practices of the federal government. Moreover, to the extent GPO is a "contractor" to Executive branch agencies, GPO will be required by such agencies to be in full FISMA compliance.

Activities to be Reviewed:

The OIG will conduct an independent baseline analysis to assess the degree of GPO's compliance with FISMA requirements and to identify the most effective methods for achieving compliance.

Anticipated Benefits:

The FISMA review will enable GPO to identify IT vulnerabilities and take corrective measures as necessary. More importantly, it will enable GPO to provide assurance to its customers that GPO is in full compliance with federal government best practices.

• Transition Planning for Internet Protocol Version 6

Background and Objectives:

Internet Protocol Version 6 (IPv6) is the latest level of the Internet Protocol.[1] It is now included as part of Internet Protocol (IP) support in many products including the major computer operating systems. Therefore, GPO's network may already contain IPv6-capable software and equipment. One of the most significant improvements of IPv6 (over IPv4) is that IP addresses are lengthened from 32 bits to 128 bits. This provides relief of an impending shortage of network addresses. Additionally, network security may be enhanced through use of IPv6.

All Executive branch agencies are required to use IPv6 on their network backbones by June 2008. Additionally, all agency networks must interface with this infrastructure. Various complexities, costs, and risks may be encountered by GPO in transitioning from IPv4 to IPv6. Moreover, the Department of Homeland Security's US-CERT has issued an advisory of issues concerning IPv6. Poorly managed IPv6 capabilities could put GPO's information and systems at risk.

Activities to be Reviewed:

We will determine whether GPO has an adequate strategy and plan for transitioning to IPv6 and whether the agency is mitigating near-term IPv6 security risks. Our review will determine whether GPO is:

- Identifying the most effective transition method to allow GPO to use IPv4 and IPv6 without significant network interruptions.
- Proactively evaluating and mitigating security risks associated with IPv6-capable software and devices already in GPO's network.
- Developing an inventory of software and hardware in order to understand the scope of the IPv6 transition and to assist in focusing risk assessments.
- Identifying how much IPv6 address space is needed by GPO in order to integrate the new technology with GPO's existing enterprise architecture.
- Developing IPv6 transition policies and enforcement mechanisms.
- Estimating costs of the IPv6 transition for budget projection purposes.

[1] The Internet Protocol (IP) is the method by which data is sent from one computer to another on the Internet. Each host computer on the Internet has at least one IP address that uniquely identifies it from all other computers. The Internet Protocol is core to Federal agency IT infrastructures.

- **Transition Planning for Internet Protocol Version 6** (continued)

    - Proactively integrating IPv6 requirements into acquisition requirements to help ensure that GPO's applications are able to operate in an IPv6 environment without expensive upgrades.

Anticipated Benefits:

Early and effective IPv6 planning should help ensure that GPO makes the transition in a cost-effective manner without significant risk to its network and data.

• Network Vulnerability Assessment

Background and Objectives:

GPO's 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 websites which GPO maintains on behalf of other Federal agencies. The objective of this assessment is to determine whether sufficient protection controls have been implemented on GPO's networks and related systems. Inadequate network security controls potentially expose GPO to network instability and unauthorized compromise of systems and data.

Activities to be Reviewed:

This assessment will evaluate the adequacy of controls on GPO's network from both an external and internal perspective. It is anticipated that we may review the adequacy of 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 be conducted using a combination of public and commercial assessment tools. These 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 OIG Report 06-02, "GPO Network Vulnerability Assessment Report," dated March 28, 2006.

Anticipated Benefits:

This assessment may discover vulnerabilities within GPO's network environment that puts GPO systems and data at risk of unauthorized compromise.