

**U. S. Government Printing Office**  
**Office of Inspector General**  
**Office of Audits and Inspections**

**Updated:  
July 7, 2010**



# OIG WorkPlan

## 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.



# OIG WorkPlan

## Types of OIG Reviews

Federal Government OIGs are statutorily obligated to independent and objective performance audits, financial audits, and special reviews. 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.



- **GPO Regional Printing Procurement Office (RPP0) 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.

These audits will be conducted at various RPPOs. The overall objective of each audit is to determine whether the RPPO fulfilled its mission to its Federal customer agencies. The three specific objectives of the audit are to determine whether (1) the RPPO is fulfilling the printing needs of the customer agencies in a timely manner and at a fair and reasonable price, (2) the system of controls in place to detect and prevent fraud, waste, abuse, and mismanagement is adequate, and (3) the procurement and related contracting practices of the RPPO are in compliance with GPO printing procurement regulations and other applicable guidelines.

**Activities to be Reviewed**

We will determine whether the RPPOs are operating within the framework of GPO's printing procurement regulations. Specifically, 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.

**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.



# OIG WorkPlan

- **Control and Accountability of GPO Laptop Computers**

## **Background and Objectives**

Government issued laptop computers (laptops) are at risk of loss and theft due to their portability, ease of concealment and the ability to hold large amounts of data. Lost or stolen laptops can result in waste of funds and exposure of sensitive personal and government information, including personally identifiable information (PII). The inability to account for laptops has been a prevalent issue throughout the Federal government. Between 2005 and 2009, GPO issued 629 laptop computers worth \$1,393,856.00.

Our audit will determine whether GPO can account for all of its laptop purchases and whether GPO has adequate controls in place to prevent loss and theft of laptops.

## **Activities to be Reviewed**

We will research Federal and GPO property management criteria and evaluate GPO policies, procedures, and processes for laptop delivery, storage, and disposition. We will test a statistically valid sample of issued laptops to determine if they can be located.

## **Anticipated Benefits**

This audit should help GPO improve controls over its laptop inventory and help prevent the loss or exposure of sensitive information and data.



# OIG WorkPlan

## • 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.



# OIG WorkPlan

## • 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 needs. Once a printing job is completed, 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.



# OIG WorkPlan

## • **Federal Digital System (FDsys) Contract Administration**

### **Background and Objectives**

The GPO Federal Digital System (FDsys) will be a comprehensive information life-cycle management system that will ingest, preserve, provide access to, and deliver content for the three branches of the Federal Government. The system is envisioned as a comprehensive, systematic, and dynamic means of preserving electronic content. FDsys will have three major subsystems: the content management subsystem and the content preservation subsystem (accessible to GPO internal users only); and the access subsystem for public content access and dissemination.

In order to develop and implement FDsys, GPO hired various contractors, including a contractor to be the Master Integrator. During performance of the Master Integrator contract, GPO made the decision to assume the role of the Master Integrator. The objective of this audit is to determine whether GPO effectively administered the FDsys Master Integrator contract, including adherence to the Materials Management Acquisition Regulation and other applicable laws, rules, regulations, and guidance.

### **Activities to be Reviewed**

We will evaluate policies, procedures and practices utilized by GPO to award the contract, monitor contract performance, modify the contract, and close the contract. We will also review costs incurred to determine if they are allowable, reasonable, and justifiable. The audit will be conducted by GPO OIG audit staff as well as the Defense Contract Audit Agency.

### **Anticipated Benefits**

This audit may identify contract administration weaknesses that can be improved in future GPO contracts. It may also identify funds owed to or due from the contractor.



# OIG WorkPlan

- **Independent Verification and Validation of GPO's Federal Digital System (FDsys)**

## **Background and Objectives**

The GPO Federal Digital System (FDsys) will be a comprehensive information life-cycle management system that will ingest, preserve, provide access to, and deliver content for the three branches of the Federal Government. The system is envisioned as a comprehensive, systematic, and dynamic means of preserving electronic content. FDsys will have three major subsystems: the content management subsystem and the content preservation subsystem (accessible to GPO internal users only); and the access subsystem for public content access and dissemination.

The GPO OIG is responsible for the Independent Verification and Validation (IV&V) work associated with developing and implementing FDsys. The objective of IV&V is to determine whether system implementation is consistent with the project plan and cost plan, and whether the delivered system meets GPO requirements. We are conducting the IV&V through a contract with an outside vendor. The IV&V methodology used for this effort is referenced to the framework established by the Institute of Electrical and Electronic Engineers (IEEE) Standard 1012-2004, the IEEE Standard for Software Verification and Validation.

## **Activities to be Reviewed**

IV&V will review project management as well as technical and testing activities associated with the project and advise GPO on potential risks to the project. We will issue quarterly risk management report to GPO, providing observations and recommendations on the program's technical, schedule, and cost risks as well as requirements traceability of those risks and the effectiveness of the program management processes in controlling risk avoidance.

## **Anticipated Benefits**

This IV&V activity will help GPO (1) identify problems and related risks before the system is fully operational, (2) meet required key system expectations, and (3) build the system in a cost effective manner.



## • GPO's Public Key Infrastructure Certification Authority

### Background and Objectives

GPO has implemented a Public Key Infrastructure (PKI) Certification Authority (CA) to support its “born digital and published to the Web” methodology for meeting customer expectations regarding electronic information dissemination and e-Government, which requires digital certification that documents within GPO’s domain are authentic and official. The PKI also facilitates trusted electronic business transactions for Federal organizations and other non-Federal entities. The GPO CA currently issues, signs and manages the public key certificates in secure facilities based in Washington, D.C. GPO’s PKI is cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification requires that the GPO PKI undergo an annual independent compliance assessment. To satisfy this requirement, the OIG has contracted with an independent public accounting firm to conduct an annual *WebTrust*<sup>1</sup> examination. The examination and resulting report represent an evaluation of whether GPO’s assertions related to the adequacy and effectiveness of controls over GPO CA operations are fairly stated based on underlying principles and evaluation criteria.

### Activities to be Reviewed

We will perform a *WebTrust* CA examination with respect to all *WebTrust* criteria, in accordance with Generally Accepted Government Auditing Standards. We will determine whether the PKI CA system is being operated in accordance with its published Certificate Policy (CP) and Certificate Practice Statement (CPS). We will also measure GPO’s compliance with reporting requirements of the Federal Infrastructure Policy Authority (FPKIPA) and the Shared Service Provider Working Group. The scope of the examination will include:

- CA business disclosures. How GPO defines, documents, communicates, and assigns accountability for its CP/CPS and overall key and certificate lifecycle management.
- Service integrity and management. How GPO verifies the authenticity of the subscriber request and identity. Additionally, how the integrity of the X.509

---

<sup>1</sup> *WebTrust* is a program of the American Institute of Certified Public Accountants (AICPA).



## **GPO's Public Key Infrastructure Certification Authority (continued)**

keys and certificates are issued, maintained and secured for appropriate use, distribution, modification and key destruction.

- Information privacy. How GPO provides notice about its privacy procedures regarding the purposes for which personal information is collected, used, retained and disclosed. Additionally, how management has instituted privacy personnel to conduct privacy assessments around the systems that support the GPO CA and adherence to eGovernment privacy requirements.
- Information security. How GPO protects subscriber information, supporting CA systems/databases and hardware against unauthorized access and disclosure.
- Environmental controls. How GPO ensures the ongoing operations and integrity of the PKI computer and cryptographic systems, facilities and personnel.
- Monitoring and enforcement. How GPO monitors compliance with its stated CP/CPS and events chronicled throughout the key and certificate lifecycle.

### **Anticipated Benefits**

The WebTrust assessment is a critical part of the GPO PKI's cross-certification with the FBCA and authorization as a Shared Service Provider. 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 entity seeking PKI services.



## • **Secure Card Personalization System (SECAPS) Information Technology Security Controls**

### **Background and Objectives**

GPO is a provider of secure Federal e-Credentials to the Department of Homeland Security's Customs and Border Protection Trusted Traveler program, as well as the Department of Health and Human Services Center for Medicare and Medicaid Services. GPO established an e-Credential production capability and related system. The system, known as the Secure Card Personalization System (SECAPS) encompasses a personal (e.g. traveler) data transmission capability, databases for temporary storage of personal 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 (PII), are adequately protected against unauthorized access and compromise. We will examine security controls associated with:

- System interconnections and the transmission of PII
- Operating systems supporting SECAPS
- Databases supporting SECAPS
- Purging of PII
- Physical security of SECAPS.

We will evaluate SECAPS information technology security controls against applicable GPO Directives, Federal security requirements and guidelines, and industry best practices. We will test security controls using manual procedures and available software interfaces. We will not review SECAPS controls at the application level.

### **Anticipated Benefits**

This audit will help ensure that the system meets GPO and Federal IT security requirements, including the protection of PII.



## • GPO's PURL Server Failure

### Background and Objectives

On August 23, 2009, GPO's Persistent Uniform Resource Locator (PURL)<sup>2</sup> server failed, causing a significant disruption for Federal depository libraries across the United States in disseminating U.S. government information. GPO did not have a failover capability and could not provide the necessary software application support for the rebuild process. While the capability was ultimately restored with the help of an external organization, GPO outsourced the building of a bridge of stability for the current system until the Federal Digital System can address the persistent identification of content requirements.

### Activities to be Reviewed

We will conduct an inspection of the PURL server failure to determine:

- The reason(s) for server failure
- Why no failover capability was available
- Why GPO could not support the software rebuild process

### Anticipated Benefits

This inspection may identify lessons learned to help prevent similar incidents from occurring on GPO information technology systems in the future.

---

<sup>2</sup> PURLs are Web addresses that act as permanent identifiers for changing Web Infrastructure. PURLs are persistent because once established, a PURL does not change although a Web page may change.



# OIG WorkPlan

## • **Audit of GPO Financial Statements**

### **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 the Contracting Officer's Technical Representative (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.



# OIG WorkPlan

## • **Audit of the GPO Purchase Card Program**

### **Background and Objectives**

The GSA, through a contract with Citibank, provides GPO with commercial purchase threshold of \$2,500 for official government use. GPO uses the purchase cards for various purposes, including purchasing supplies and services, emergency requirements, or to support production and field activities. Prior to FY 2008, the purchase card program was handled through Bank of America.

No audits have been conducted by GPO OIG since the changeover in banks. Recent discussions with the Comptroller revealed that while the program has more cardholders and has an average quantity of transactions in the range of \$250-300,000 per month, internal controls over this program have not improved. Problems identified in past audits (with the previous bank), which included split purchases, charges over the monthly/annual limits, and allegations of other potential card abuse, have remained.

The overall objectives of the audit will be to evaluate the effectiveness of GPO's purchase card program, with special attention/consideration given to the change in contracted banks. The specific audit objectives will include determination of whether (a) GPO has implemented appropriate management controls over the use of purchase cards, and (b) purchase cards are being utilized in compliance with applicable laws, regulations, policies and procedures.

### **Activities to be Reviewed**

These activities should include:

- Purchase card SOPs, as prescribed by both GPO and Citibank
- Training programs for card usage, and training documentation
- Tests for potential split purchases and other over-the-limit (OTL) transactions
- Review of allowable and unallowable charges (e.g. travel)

### **Anticipated Benefits**

The audit will determine whether the revised system of controls, as well as the interaction with the new bank, are adequate and effective and meet the needs of GPO. Our audit will identify better opportunities to manage the purchase cards.



## • GPO's Management of Single-Points-of-Failure in the e-Passport Production Process

### Background and Objectives

GPO is the sole source for producing, storing, and delivering blank U.S. passports for the Department of State (DOS). As electronic, machine-readable passports become the “gold standard” in identification, the absence of adequate supply chain security leaves the integrity of e-Passports vulnerable to a variety of threats. The Congress, GPO, and DOS have each stressed the need for robust security over the e-Passport supply chain.

GPO's e-Passport supply chain is vast, as the e-Passport book contains over 60 commercially available and uniquely assembled materials; among them cover stock, security paper, security inks, security threads, and security functions, both covert and overt. Suppliers of those materials are located throughout the United States and in several foreign countries. GPO's Office of Security and Intelligent Documents (SID) selects suppliers and materials in collaboration with DOS. DOS also collaborates with SID to perform security assessments of both the suppliers of computer chips for the e-Passport as well as for the subcontractor responsible for inserting the chips into the passport covers. SID is solely responsible for vetting and performing security assessments of the remaining companies that supply e-Passport components.

Several of the materials and operations in the e-Passport supply chain are single-points-of-failure, meaning that any absence of that particular material, or any shut down of that particular operation, would bring the e-Passport production process to a complete stoppage. Some of the more significant single-points-of-failure is the production of passport cover stock and the process of inserting chips into the cover stock.

Our audit objective would be to determine if GPO management has identified all single-points-of-failure in the e-Passport production process, is properly managing those single-points-of-failures, and is actively engaged in trying to eliminate those single-points-of-failures in the e-Passport production process.

### Activities to be Reviewed

We plan to follow-up on our prior audit of the Security of the e-Passport Supply Chain and to conduct discussions with GPO SID and Office of Acquisitions personnel



# OIG WorkPlan

## **GPO's Management of Single-Points-of-Failure in the e-Passport Production Process (continued)**

to identify and document the latest e-passport supply chain. We will then identify all single-points-of-failure in the current e-Passport supply chain and determine what actions GPO is undertaking to manage and ultimately eliminate the single-points-of-failure. We also plan to conduct research of industry standards for supply chain management and the management of single-points-of-failure in particular and determine if GPO is following those standards in its e-Passport supply chain management.

### **Anticipated Benefits**

Our audit will identify opportunities for GPO to better manage its e-Passport supply chain and eliminate all potential shut downs of the e-Passport production process.



- **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 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.



# OIG WorkPlan

- **Photocopier Security**

## **Background and Objectives**

Nearly every digital copier built since 2002 contains a hard drive, such as those on personal computers. The hard drives store an image of every document copied, scanned, or emailed by the copier. These images may contain sensitive agency information, including personally identifiable information (PII). Removal of the hard drives and application of digital forensic computer programs allow subsequent owners to retrieve all documents contained on the hard drive. It is not necessary to extract the hard drive in order to access data. Many copiers have network connections which can be used to view or download files via Telnet, web or FTP.

The objective of this inspection is to determine whether GPO is addressing this potential security problem so that sensitive information may not become available to an unauthorized user.

## **Activities to be Reviewed**

The OIG will research the technology issues associated with this vulnerability, including technology available to sanitize hard drives containing sensitive information. We will inspect GPO policy and contracts with its digital copier vendors. We may physically and logically access a sample of hard drives to determine if sensitive information resides on them. We may also review remote file transfer capabilities to determine if stored images on copier hard drives could be transferred across the GPO computer network.

## **Anticipated Benefits**

This inspection could help prevent the unauthorized disclosure of sensitive GPO information or PII.



## • Audit of GPO Quality Control Program

### Background and Objectives

To meet its mission of providing printing services to all three branches of the Federal Government, GPO purchases paper for in-house printing operations, and procures print services from over 2,500 private sector vendors. In 2007, GPO purchased over 31 million pounds of paper for use in its Washington, DC plant, and procured an additional half a billion pounds of paper and printing services through \$600 million worth of contracts awarded to private sector vendors.<sup>3</sup>

To ensure that the paper used for GPO's in-house printing operations and both the paper and printing services procured through the private sector meet all relevant standards and specifications,<sup>4</sup> GPO has established a paper and print procurement quality control program. Specifically, GPO Instruction 350.1, "The Government Printing Office Quality Control Program," October 1, 1976, establishes the following responsibilities for ensuring that the Agency and its vendors comply with both paper and print quality control specifications:

- The Production Manager is responsible for insuring that all printing and binding products manufactured in GPO meet specified quality levels. He will set up process controls, tests, inspections and maintain quality control charts.
- The Printing Procurement Manager is responsible for insuring that all GPO procured printed products meet the specified quality levels. He will conduct on-site inspections to insure that contractors have necessary process controls and procedures to meet quality levels required and arrange for product inspection as necessary to assure that quality levels have been met.

---

<sup>3</sup> Each year, GPO relies on the private-sector to fulfill over 100,000 (or 78 percent) of its print orders.

<sup>4</sup> Relevant standards and specifications that impact the paper and print quality/printing ink that GPO uses or purchases on behalf of its customers include Executive Order 13101, "Greening the Government Through Waste Prevention, Recycling, and Federal Acquisition;" GPO's "Government Paper Specification Standards;" and the Vegetable Ink Printing Act of 1994. For example, the Executive Order states that, when executive branch agencies purchase or cause the purchase of printing and writing paper for a variety of uses, the minimum content standard of the paper shall be no less than 30 percent postconsumer waste materials. Additionally, the Standards establish type, grade, weight, minimum content, and other quality control specification standards for paper used in the Federal Government's public printing, as well as testing methods to measure paper characteristics and ensure that GPO uses, purchases, and receives only conforming paper. Finally, the Act requires that all Federal lithographic printing be performed using ink made from vegetable oil, and prescribes specific vegetable oil content percentages for different types of ink.



## Audit of GPO Quality Control Program (continued)

- The Director of Materials Management Service is responsible for the procurement of printing and binding raw materials which will meet the requirements of the Production Department and standards prepared by the Quality Control and Technical Department.

### Activities to be Reviewed

For this audit, we will evaluate GPO's quality control program and paper and print procurement functions to determine if sufficient controls, including contract clauses, inspections, testing, and remedial action, are in place to ensure that GPO and its vendors are in compliance with all standards and specifications relating to paper and printing services used by the Federal Government.

### Anticipated Benefits

This audit should help strengthen GPO's quality control program, which will (1) ensure that GPO meets its customer's needs and requirements, (2) maximize savings in the Government's paper and print services purchases, and (3) identify and help minimize instances of product substitution and false claims related to GPO vendors' use of nonconforming paper or production of nonconforming printing services.



## • **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 production with 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:

- Review the functionality of the production application, including (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.
- Review technical controls built into the application and determine whether controls meet the requirements of GPO, the Federal Government, and industry best practices.
- 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.



# OIG WorkPlan

## • **GPO Compliance with the Federal Information Security Management Act**

### **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 Executive branch agencies in securing Federal computer systems. FISMA requires that each year Executive branch agencies conduct an independent evaluation of their security programs for compliance with FISMA. 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.

Although it has no specific congressional mandate, GPO has chosen to substantially comply with the principles of the Act. To the extent GPO is a “contractor” for agencies of the Executive branch, those agencies require that GPO comply with FISMA. Compliance with FISMA presents significant challenges for GPO, including protecting critical Agency systems, information, and data.

### **Activities to be Reviewed**

In FY 2007, the OIG conducted a baseline assessment of compliance with FISMA to identify gaps and deficiencies in GPO’s overall information security program. We completed a full FISMA assessment in FY 2009 and will continue to conduct full assessments annually. The assessments will place significant emphasis on systems critical to GPO’s mission as well as those GPO systems that support services to Executive branch agencies. We will perform the assessments using the most recent applicable FISMA requirements and guidelines published by the Office of Management and Budget and the National Institute of Standards and Technology.

### **Anticipated Benefits**

The FISMA assessment will enable GPO to identify weaknesses in its information technology security program and take appropriate corrective measures. The assessment will provide assurance to GPO customers that the Agency complies with established best practices.



## • **Passport Transportation Audit 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 eCovers Contract Administration**

### **Background and Objectives**

The current U.S. electronically enabled Passport program has been in effect since 2004. To ensure continuity in the supply of passports for issuance to U.S. citizens/nationals, GPO, in cooperation with the Department of State's Bureau of Consular Affairs issued an RFP in Fiscal Year 2010 for the second procurement of eCovers used in the manufacturing of U.S. Passports. eCovers consist of the passport cover material containing a contactless Integrated Circuit (IC) with an antenna assembly. The eCovers are the backbone of the ePassport and are a single-point-of-failure in the ePassport manufacturing process. As part of the planned contract, the Government intends to make an initial security assessment and periodic announced and unannounced follow up assessments of all manufacturing facilities. All assessments will focus on physical security, information technology security, supply chain security, business continuity, and other areas as appropriate. Inspectors will follow a structured methodology to assess the facility's compliance with current applicable standards. Contractors are to provide full access to their facilities in a timely manner. Furthermore, this same requirement shall be set forth from the prime contractor to each of its subcontractors.

### **Activities to be Reviewed**

We will evaluate policies, procedures and practices utilized by GPO to award the contract, monitor contract performance, including manufacturing security, modify the contract, and close the contract.

### **Anticipated Benefits**

This audit may identify contract administration weaknesses that can be improved in order to better protect GPO interests and insure the uninterrupted flow of the ePassport supply chain.



## • **Audit of GPO Safety Program**

### **Background and Objectives**

GPO is the largest industrial manufacturer in the District of Columbia. GPO employees routinely operate heavy equipment and machinery; engage in welding and cutting operations; and encounter, handle, and store solvents, compressed gases, combustible and flammable liquids, and hazardous materials and waste. Even those employees who are not directly involved in the Agency's printing processes encounter workplace hazards, since plant operations in GPO's facility take place on multiple floors occupied by both plant and non-plant employees. Between 2008 and 2009, GPO employees reported 170 job related injuries and illnesses, which does not include mishaps or close calls from hazardous or unsafe conditions that did not result in a worker's compensation claim.

According to GPO Directive 670.10A, "Government Printing Office Safety Program," GPO's policy is to provide a safe and healthful workplace for its employees, consistent with applicable Federal, state, and local laws, standards, and guidelines. However, as a Legislative Branch agency, GPO is not subject to the regulations or oversight of the Occupational Safety and Health Administration, making an effective safety program even more critical.

### **Activities to be Reviewed**

For this audit, we will evaluate GPO's safety program, including industrial safety and hygiene, to determine if it is sufficient to minimize and prevent injuries, mishaps, and close calls and ensure the welfare of GPO employees and other resources. As necessary, we will review GPO's various union contracts and agreements.

### **Anticipated Benefits**

This audit should help strengthen GPO's safety program and provide opportunities for improving the Agency's working conditions. Improved safety practices should result in a reduction in accidents, worker's compensation claims, and missed time resulting from job related injuries and illnesses.



# OIG WorkPlan

## • **Audit of the GPO Travel Card Program**

### **Background and Objectives**

In FY 2008 GPO contracted with Citibank (having contracted with Bank of America previously) for GPO employees to be issued Visa travel cards at no charge or interest fees. The employee is billed directly and is personally liable for all charges incurred with the card. In accordance with GPO Instruction(s), travel cards issued to GPO employees shall be used for expenses incurred in conjunction with official travel.

There have been no audits conducted by GPO OIG since the changeover in banks. Program management has stated that it is still becoming accustomed to a different system, without the same kind of rules or training as was instituted by the previous bank.

The overall objective of the audit will be to evaluate the effectiveness of GPO's Travel Card Program to determine (a) whether adequate controls exist over the issuance of travel cards; (b) whether travel cards are being used for official need only; and (c) that payments are timely and travel claims are processed timely and accurately.

### **Activities to be Reviewed**

These activities should include:

- Travel card SOPs, as prescribed by both GPO and Citibank
- Blanket and single trip travel orders
- Training programs for card usage, and training documentation
- Testing and monitoring for unauthorized or unallowable use
- Monitoring of card activity, including delinquent accounts

### **Anticipated Benefits**

The audit will determine whether the revised system of controls and bank interaction are adequate and effective and meet the needs of GPO. Our audit will identify better opportunities to manage the travel card program at GPO.



# OIG WorkPlan

## • Network Vulnerability Assessment

### 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. Inadequate network security controls potentially expose the Agency to network instability and unauthorized compromise of systems and data from both internal and external threats.

### Activities to be Reviewed

Annually, we will assess the adequacy of security controls from both an internal and external perspective on selected networks and public facing Web servers supporting various critical GPO operations. Our assessment will leverage the benchmarks published by the Center for Internet Security (CIS)<sup>5</sup> as well as network security requirements by the National Institute of Standards and Technology. 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.

---

<sup>5</sup> 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.



# OIG WorkPlan

## • **Audit of Software Quality Assurance**

### **Background and Objectives**

Software Quality Assurance (SQA) is the process of monitoring software development and maintenance processes and methods used to ensure quality. SQA encompasses the entire software development and maintenance process and is used by organizations to help ensure the success of software. Without adequate SQA, GPO is at increased risk of both software and data problems in its systems supporting the Agency's various business units, including the implementation of software with incomplete or erroneous decision-making criteria and the occurrence of inaccurate or incomplete data used in the automated process. Past OIG audits and inspection activities identified weaknesses in various components of GPO's SQA program.

The objective of this audit is to determine whether GPO's Office of the Chief Information Officer has an effective SQA program to reduce the risk of software and data problems in GPO systems.

### **Activities to be Reviewed**

The OIG will evaluate GPO's SQA program using various benchmark sources such as the National Institute of Standards and Technology (NIST), the Institute of Electrical and Electronics Engineers (IEEE), and Carnegie Mellon's Capability Maturity Model Integration (CMMI). Specifically we will review the effectiveness of the following SQA components at GPO:

- Software design
- System Software Testing Strategies (requirements phase, design phase, program phase, installation phase testing, testing evaluation, acceptance testing, regression testing etc)
- Source code control
- Change management
- Configuration management

### **Anticipated Benefits**

This audit should help GPO improve the software and data quality of its automated systems.



## • **Security Controls At GPO Contracted Security Printers**

### **Background and Objectives**

“In the post 9/11 era, documents such as U.S. Passports, Social Security Cards, travel documents, and immigration forms require new levels of security from their creation to their ultimate disposition.” (A Strategic Vision for the 21st Century, U.S. Government Printing Office, December 1, 2004). To meet this demand, GPO established a Security and Intelligent Document business unit (SID) whose mission is to “work with Federal agencies to assist in the safe and secure design, production and distribution of security and intelligent documents”. SID accomplishes its mission in two ways: by ensuring that the sensitive documents it supplies to Federal customers are manufactured in government space with secure government personnel and a government controlled supply chain, or by contracting such work out to private security printers. GPO’s Print Procurement business unit handles all planning and administration associated with procuring sensitive documents from private vendors.

The types of sensitive documents procured by GPO vary. Some, such as Lincoln visas, are security documents in the strict sense; i.e., they are designed to accurately identify holders using secure design features and biometric data. Others, such as social security cards, contain Personally Identifiable Information (PII) that if lost or compromised could lead to identity theft or other fraudulent use resulting in substantial harm to individuals. A third category consists of negotiable instruments and enabling documents that entitle holders to public grants or benefits and that could lead to widespread economic fraud if compromised. Examples of these types of documents that are procured by GPO include Veterans Identification Cards and blank U.S. Treasury checks. Any failure by GPO to exercise due diligence in requiring that the companies that manufacture and print these types of documents maintain adequate security controls and submit to external audits poses a threat to individuals, taxpayers, and the national security.

The overall objective of the audit will be to evaluate GPO’s process for ensuring adequate security over the design, manufacture and distribution of sensitive documents procured from security printers. Specifically, we will identify whether appropriate controls are in place to ensure that contracted security printers meet



## **Security Controls at GPO Contracted Security Printers (continued)**

applicable security standards and allow on-site risk analysis and review by GPO personnel. We will also evaluate whether a sufficient level of expertise exists in GPO's Print Procurement business unit to identify competent security printers, and to insert security clauses into contracts where applicable.

### **Activities to be Reviewed**

We plan to examine contract files in Print Procurement that document sensitive procurements and determine whether each contains appropriate security clauses or attachments. We would then conduct discussions with applicable GPO officials to identify roles and responsibilities with regard to ensuring adequate security of procured sensitive documents. Finally, we will travel to contractor facilities as appropriate to assess security of operations.

### **Anticipated Benefits**

This audit should identify opportunities to reduce the risk that GPO-procured security documents will be lost or compromised prior to reaching the GPO customer.



## • 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 consumption, costs, and develop preliminary costs and energy savings associated with implementing the recommended ECMs.

The preliminary report that PEPCO provided GPO identified 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.



# OIG WorkPlan

## Energy Use at GPO (continued)

### 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 an effective program of energy audits, ECMs and targeted projects.



# OIG WorkPlan

## • Audit of GPO use of Overtime

### Background and Objectives

As of March 2010, GPO had 2,286 employees. The agency also paid for 104,778 overtime hours for the first six months of FY10. For the same time period in FY 09, GPO had 2,351 employees and paid 97,196 hours of overtime. The 7,582 hours represents an increase of almost 8%. The major business units which show significant increases in overtime hours include: Security and Intelligence Documents, Security Services, and Administration. Plant Operations also had an increase in FY 10, however, it was not as significant as the other business units.

According to GPO Directive 640.7D, "General Pay Administration," GPO's policy recognizes several types of overtime (authorized, non-authorized, irregular, regular, call-back, etc.). GPO is subject to the requirements of the Fair Labor Standards found in Title 29 which requires the payment of overtime at "not less than one and one-half times the regular rate at which he is employed". There are additional requirements/limitations provided in Title 29, particularly in regard to those employed under a collective bargaining agreement.

The policy also includes a limitation of the amount of overtime that can be paid that mirrors the limitations found in Title 5, Chapter 55 even though the Agency is not required to the pay administration requirements in this Title.

### Activities to be Reviewed

For this audit, we will evaluate GPO's overtime payments to determine if they have been paid according to the agencies' policy. We will also attempt to determine the basis for the significant increases in overtime payments during the first half of FY10. As necessary, we will review GPO's various union contracts and agreements.

### Anticipated Benefits

The audit should identify the reasons for the increased requirements for overtime and possible steps that could be taken to reduce these costs. It should also provide opportunities to enhance controls and provide assurance that the overtime being paid is necessary and accurate.



# OIG WorkPlan

## • Implementation of Windows Active Directory and Group Policy Technology

### **Background and Objectives**

As part of enhancements to its information technology infrastructure, GPO is implementing Windows Active Directory and related Group Policy technology. Active Directory is a Microsoft Corporation technology that provides a variety of services, including:

- Kerberos-based authentication
- DNS-based naming and other network information
- Central location for network administration and delegation of authority
- Information security and single sign-on for user access to network based resources
- Central storage location for application data
- Synchronization of directory updates among servers.

Active Directory allows administrators to assign policies, deploy software, and apply critical updates to GPO's network infrastructure. Therefore, the Active Directory infrastructure and Group Policy objects must be adequately secured in order to maintain continuity of operations and stability of GPO's network. Properly implemented, Active Directory can greatly enhance network performance and management. The objective of this audit will be to determine whether GPO is implementing Active Directory and Group Policy objects in a secure and stable manner.

### **Activities to be Reviewed**

We will review all critical security configurations associated with the implementation against Center for Internet Security and other industry best practices.

### **Anticipated Benefits**

This audit should help ensure that GPO's network infrastructure is secure and stable.



# OIG WorkPlan

## • **Audit of GPO Property Management Program**

### **Background and Objectives**

Each year, GPO invests substantial public funds in thousands of Government property items, including accountable property<sup>6</sup> and stock items<sup>7</sup>. An effective and well-documented property management program is necessary to adequately control this property throughout its lifecycle. According to GPO Directive 810.11B, “GPO Property Management Program,” the primary objective of the Agency’s property management program is to ensure that the necessary equipment, machinery, materials, supplies, and other property are readily available to support GPO’s mission and provide a continuous stream of benefits to GPO’s customers. Additionally, without adequate controls, GPO’s property is at risk for loss, theft, and misuse, and GPO lacks assurance that its assets are properly accounted for in accordance with the Federal Accounting Standards Advisory Board statements relevant to property accounting and reporting.

### **Activities to be Reviewed**

The audit will (1) review the Agency’s compliance with property management policies, procedures, and standards, and (2) evaluate the adequacy and effectiveness of GPO’s internal controls for the property management lifecycle, including the following processes:

- acquisition and receipt of property
- control and safeguarding of property
- physical inventory of property
- reconciliation to and adjust of property records
- return of property to the Stores Division
- transfer, reutilization, disposal and/or sale of property

---

<sup>6</sup> Accountable property includes personal property that is (1) valuable (e.g., having an acquisition cost or value of \$1,000 or greater), (2) sensitive (such as weapons or other restricted-use equipment), (3) pilferable (such as cameras, televisions, and power tools), or (4) so important that it must be safeguarded and individually accounted for during its useful life. Accountable property generally excludes furniture and consumable items such as inventories of operating materials and supplies (e.g., printing inks and papers).

<sup>7</sup> Stock items are those maintained in inventory by the Materials Management Service due to frequency and volume of use by GPO operating and administrative areas. These include office supplies, machine parts, and raw materials.



## **Audit of GPO Property Management Program (continued)**

### **Anticipated Benefits**

This audit should help strengthen GPO's property management system, which will (1) reduce the risk of loss, theft, or misuse of GPO property, (2) help identify assets that are in unusable condition or in excess of current and anticipated needs, and (3) provide assurance to management, external auditors, and other interested parties that reported assets exist and exist in the quantities recorded in inventory or property management systems.



# OIG WorkPlan

## • Domain Name System Security

### Background and Objectives

Domain Name System (DNS) is used by every modern computer to translate names (e.g. www.gpo.gov) to Internet Protocol addresses (e.g. 162.140.239.10). GPO's DNS infrastructure plays an integral role in the overall security posture of the network environment. Not only should DNS be configured securely, but it should also be designed to provide a very high level of availability and redundancy. An update to DNS, DNS Security (DNSSEC) for the root zone is currently being developed with support from the U.S. Department of Commerce. DNSSEC will have security implications for GPO's IT infrastructure. The objective of our audit will be to determine whether GPO is tracking and appropriately implementing DNSSEC within its DNS infrastructure.

### Activities to be Reviewed

We will ensure that GPO follows National Institute of Standards and Technology guidance for securing DNS. Specifically, we will evaluate GPO controls over

- Data integrity, to ensure that the authenticity of domain name information served by GPO is correct.
- Authenticity, to maintain the integrity of domain name information set in transit from GPO.
- Availability to ensure GPO's DNS servers are configured to prevent/minimize denial of service attacks against it.

### Anticipated Benefits

The audit should enhance security assurance by GPO to its digital customers relying on GPO DNS.



## • **GPO Compliance with Federal Standards for HSPD-12: Personal Identity Verification**

### **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.

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



## • List of Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CIS	Center for Internet Security
CMMI	Capability Maturity Model Integration
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf Software
CP	Certificate Policy
CPS	Certificate Practice Statement
DNS	Domain Name Service
DNSSEC	Domain Name Service Security
ECM	Energy Conservation Measures
FASAB	Financial Accounting Standards Advisory Board
FBCA	Federal Bridge Certificate Authority
FDsys	Federal Digital System
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
HSPD	Homeland Security Presidential Directive
IEEE	Institute of Electrical and Electronic Engineers
IT	Information Technology
IT&S	Information Technology and Systems
ITS	Inventory Tracking System
IV&V	Independent Verification and Validation
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PPPS	Passport Printing and Production System



# OIG WorkPlan

## List of Acronyms (continued)

PURL	Persistent Uniform Resource Locator
RPPO	Regional Printing Procurement Office
SECAPS	Secure Card Personalization System
SID	Security and Intelligent Documents
SQA	Software Quality Assurance

