U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

AUDIT REPORT
10-06

# Security of GPO's e-Passport Supply Chain

## March 31, 2010

MEMORANDUM

U.S. GOVERNMENT PRINTING OFFICE

OFFICE OF INSPECTOR GENERAL

**Date**

March 31, 2010

**To**

Deputy Public Printer

Chief Management Officer

Managing Director, Security and Intelligent Documents

Chief Acquisition Officer

**From**

Assistant Inspector General for Audits and Inspections

**Subject**

**Final Report on Audit of Security of GPO's e-Passport Supply Chain Report Number 10-06**

Enclosed please find the subject final report. Please refer to the Executive Summary for the overall audit results. Our evaluation of your response has been incorporated into the body of the report and the response is included in its entirety at Appendix C. We consider management's proposed actions responsive to each of the report's seven recommendations. Recommendation five will be closed upon issuance of this report. Recommendations one, two, three, four, six, and seven will remain open pending completion of the agreed upon corrective actions. Please notify us when those actions are complete. The status of each recommendation upon issuance of this report is included in Appendix D. The final report distribution is in Appendix E.

We appreciate the courtesies extended to the audit staff. If you need additional information or would like to arrange a meeting to discuss this final report, please contact Mr. Karl Allen, Supervisory Auditor at (202) 512-0277, or me at (202) 512-2009.

Kevin J. Carson

Kevin J. Carson
Assistant Inspector General for Audits and Inspections

Enclosure

cc:
Chief Technology Officer
Managing Director, Operations Support
Managing Director, Plant Operations
Acting General Counsel

## *Contents*

**Executive Summary** ..... i

**Introduction** ..... 1

**Findings and Recommendations** ..... 4

Finding A. No Formal e-Passport Supply Chain Security Process ..... 4

Finding B. Improvement Needed with Documentation for the e-Passport Supplier Assessment Process ..... 7

Finding C. No Direct Contractual Control of Significant e-Passport Supply Chain Processes ..... 12

Finding D. Lack of Contract Security Requirements ..... 15

Finding E. Incomplete Contract File Documentation ..... 17

Finding F. e-Passport Storage Issues ..... 19

**Appendix A – Objectives, Scope, and Methodology** ..... 21

**Appendix B - Acronyms Used in the Report** ..... 24

**Appendix C - Management's Response** ..... 25

**Appendix D - Status of Recommendations** ..... 30

**Appendix E - Report Distribution** ..... 31

**Major Contributors** ..... 32

# Office of Inspector General

**Report Number 10-06** **March 31, 2010**

# Security of GPO's e-Passport Supply Chain

## Executive Summary

**Background.** The Government Printing Office (GPO) Office of Inspector General (OIG) has completed an audit of the GPO's Electronic Passport (e-Passport) supply chain.[1] GPO is the sole source for producing U.S. passports for the U.S. 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. This report is the latest product resulting from the OIG's continuing oversight of GPO's passport production process. See Appendix A for a complete list of other reports issued.

Due to the sensitive nature of the audit subject matter and its impact on national security, the names of passport suppliers and specific products supplied have been omitted from this report.

**Objective.** The objective of the audit was to assess the adequacy of GPO's security over its e-Passport components and supply chain.

**Results of Audit.** GPO's e-Passport supply chain is vast, consisting of approximately 60 commercial suppliers located throughout the United States and overseas. GPO's Office of Security and Intelligent Documents (SID) has dedicated staff to ensure the security and integrity of the e-Passport supply chain. This staff maintains contact with the key e-Passport suppliers, reviewing those supplier's security policies and inspecting their manufacturing facilities.

GPO should ensure the continued security of the e-Passport supply chain by establishing a formal security oversight process. That formal process should consist of formulating and publishing a directive that assigns specific responsibilities to the various GPO organizations, ensuring that appropriate GPO personnel review all proposed e-Passport contracting actions, and establishing a formal assessment process for e-Passport suppliers.

---

[1]Supply chain, as used in the context of this audit, refers to the network of GPO product suppliers used to produce, store, and transport the e-Passport.

The audit identified that GPO's e-Passport supply chain security process was largely informal. In addition, different GPO Offices that should have been working in a coordinated manner to ensure supply chain security, such as SID, Acquisitions, Operations Support, Plant Operations, and Security Services, were instead working autonomously of each other.

Through discussions with SID's Managing Director, the Director of Product Security, the Secure Supply Chain Manager, and the Office of Acquisition's Chief of Specialized Procurements, we developed a list of 16 suppliers that provided either significant components or operations in the e-Passport supply chain. In analyzing security assessments and contract documentation for each of those 16 suppliers, we identified the following:

- GPO had a total of 16 security assessment reports on only 11 of the 16 suppliers.

- GPO had no direct contractual relationship with 6 of the 16 suppliers because they were subcontractors to a prime GPO contractor. Four of those six subcontractors were critical to e-Passport operations. Because GPO contracts did not have specific language reserving GPO's right to authorize and review the operations of these subcontractors, GPO had less control over critical e-Passport operations, such as providing passport covers or inserting computer chips into the passport covers at an overseas location – both noted single points of failure[2] in the e-Passport supply chain.

- Six of the 10 e-Passport supplier contracts reviewed did not contain security plans or security-related requirements, including contracts with a high-risk supplier and several overseas suppliers.

- GPO contract files lacked required documentation for 5 of the 10 e-Passport supplier contracts reviewed. In addition, the files did not contain evidence that GPO properly vetted the suppliers to ensure that they could meet GPO requirements in the most secure and economical manner.

The audit also identified that GPO's security process for storing some finished blank e-Passports and supplies, including the passport book covers containing the inlayed computer chips, could be strengthened.

**Recommendations.** We made 7 recommendations to GPO management to help GPO further improve the security of its e-Passport supply chain. Specifically, we recommended that GPO:

---

[2]A single point of failure is a part of a production process which, if it fails, will stop the entire production process from working. One strategy to prevent a single point of failure is to provide redundancy for such critical components in the production process.

- Develop a formal security process for the e-Passport supply chain, including a process that ensures appropriate GPO personnel review proposed contracting actions;

- Formalize the e-Passport supplier security assessment process;

- Insert appropriate clauses into new e-Passport contracts to ensure adequate security requirements and GPO rights to oversee subcontractors;

- Document e-Passport contract files in accordance with the GPO Materials Management Acquisition Regulation (MMAR); and

- Reassess e-Passport storage policies.

**Management's Response.** GPO management concurred with each of the report's recommendations and has either already implemented or planned corrective actions that we consider responsive to the recommendations.

## Introduction

e-Passport History. The International Civil Aviation Organization (ICAO), a Secretariat of the United Nations governing many aspects of international air travel, establishes standards for international passports. As early as 1996, ICAO began discussing the use of biometrics and advanced technology for improving the security of passports and facilitating international air travel. In November 2000, after considering several technologies, ICAO decided in favor of using contactless chip technology in passports that could be inserted into the passport covers to enable the storing of biometric and other information about the passport holder. By September 2001, ICAO had made considerable progress toward the introduction of the first generation e-Passports.[3]

In response to the September 11, 2001 terrorist attacks, the United States enacted the 2002 Enhanced Border Security and Visa Entry Reform Act. The Act required Visa Waiver Program (VWP) countries to produce e-Passports as a condition of keeping their designation under the VWP.[4] The United States, while not legislatively mandated to do so, committed to incorporating the embedded technology into U.S. passports because of security and identity advantages. In FY 2007, GPO printed its last legacy passport and began producing only e-Passports. In FY 2008, the first year that GPO produced only e-Passports, the Agency produced 23.6 million e-Passports for the DOS.

e-Passport Materials and Suppliers. 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. 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.

Other GPO e-Passport Responsibilities. The GPO Office of Acquisitions is responsible for e-Passport supply acquisition activities in accordance with the MMAR. The Office of Plant Operations stores e-Passport supplies at GPO's Washington, DC and Stennis, Mississippi, production facilities. The Office of Operations is responsible for ensuring that storage access devices are adequate and

---

[3]Keesing Journal of Documents & Identity, Annual Report e-Passports 2008-2009.

[4]The VWP enables nationals of 35 participating countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. The program was established in 1986 with the objective of eliminating unnecessary barriers to travel, stimulating the tourism industry, and permitting the DOS to focus consular resources in other areas.

functioning properly. Finally, the Office of Security Services ensures that only authorized personnel gain entrance to GPO printing facilities and respond to security-related incidents.

e-Passport Risks. The risks associated with counterfeited passports are well documented. The National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission) in its July 22, 2004 report states, "For terrorists, travel documents are as important as weapons….in their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas …" [5]

U.S. Senator Susan Collins, in a June 29, 2005 hearing to examine vulnerabilities in the U.S. passport system, stated:

> Fraudulent travel documents are essential to terrorists, and the U.S. passport is the gold card of travel documents. 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.

DOS officials have also referred to the risks of counterfeited passports. In a June 22, 2005 statement before the U.S. House of Representatives Homeland Security Committee, Subcommittee on Economic Security, Infrastructure Protection and Cyber Security, the DOS Deputy Assistant Secretary for Consular Affairs stated:

> Our objective in designing the new passport is to raise further the bar against counterfeiting or the fraudulent use of lost or stolen passports. Advances including color shifting ink, micro printing, latent image lettering and a security laminate over the biographic data page that includes optical variations, all serve to deter counterfeiters and forgers.

Acting upon those risks, GPO senior management has cited on several occasions the need for strong security over the e-Passport supply chain. On October 18, 2007, the former Assistant Public Printer for SID testified before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on Government Management, Organization, and Procurement, and stated:

> The security of the e-Passport would be useless without securing the manufacturing process and supply chain. GPO has implemented and continues to improve the security of its supply chain . . . . Vendors are regularly audited and reviewed and requirements are continually being improved as procurements expire and are rebid to bring the extended supply chain under even closer Government control.

---

[5]Page 384 of the 9-11 Commission Report. See http://www.gpoaccess.gov/911/Index.html.

GPO also responded to questions from the U.S. House of Representatives Committee on Energy and Commerce regarding passport security. In its April 9, 2008 response, the Agency stated that "GPO has taken all reasonable steps to assure that the production of and the supply chain for e-Passports is secure;" and that "high security is the norm for any security component supplier in the e-Passport supply chain."[6]

[6]See http://www.gpo.gov:80/pdfs/news-media/press/h_engcom_epassport_04-09-08.pdf.

## Findings and Recommendations

## Finding A. No Formal e-Passport Supply Chain Security Process

GPO did not have a formal, Agency-wide policy and related processes that would ensure security for the e-Passport supply chain as required by GPO internal control standards and as dictated by the well-documented need for supply chain security. This occurred because of a lack of sufficient management attention to ensure that a properly organized e-Passport supply chain security process was implemented. Without a formal process, the Offices of SID, Acquisitions, Operations Support, Plant Operations, and Security Services were each operating autonomously in their actions, performing their respective functions related to passport suppliers with little interaction or coordination and with no formal guidelines. The lack of a formal process was also a contributing factor to the other conditions identified in this report.

***Process Requirements***

GPO Instruction 825.18A, "Internal Control Program," May 28, 1997, provides guidance to GPO managers for improving the effectiveness of GPO operations, such as security for the supply chain. The instruction defines internal controls as the organization, policies, and procedures used to ensure that GPO (1) achieves intended program results, (2) uses its resources consistent with the Agency mission, (3) protects its programs and resources from waste, fraud, and mismanagement, and (4) follows all laws and regulations. The instruction defines internal control documentation as written policies, organization charts, procedural write-ups, manuals, memoranda, flowcharts, software, and related written materials.

In following GPO internal control criteria, and considering GPO's well-documented need for security of the e-Passport supply chain, GPO should have a comprehensive security policy for its e-Passport supply chain. That policy should include the following criteria:

- Processes that identify necessary supplies and suppliers, vet potential suppliers for their ability to meet specific security requirements, implement contractor security procedures and standards, properly document resultant contract files, specify proper storage of materials, assess the risks associated with all supplies and suppliers, and mandate security assessments of the suppliers on a regular basis based on that risk.

- A clear outline of the responsibilities of personnel who participate in the process, including the Public Printer, Deputy Public Printer, SID Managing Director, SID Director of Product Security, Chief Acquisition Officer, Managing Director of Plant Operations, Managing Director of Operations

Support, General Counsel, Director of Security Services, and applicable subordinate staff.

- A clear line of authority for the entire product security process through the Public Printer.

- A requirement to maintain adequate, qualified staff members to perform the documented security assessment process for the e-Passport supply chain.

***No Documented e-Passport Supply Chain Security Process***

GPO did not have a formal, Agency-wide process that ensured security of the e-Passport supply chain and did not adequately staff the existing supply chain oversight process. In addition, there were no existing documented policies, procedures, techniques, or mechanisms in place that implemented a security process for the e-Passport supply chain. Although the Office of Plant Operations provided us with revised, unsigned, Standard Operating Procedures (SOPs) for the receiving, storing, and issuing of e-Passport raw materials, no other standardized procedures existed for any other e-Passport supply chain processes within SID or Acquisitions.

In addition, GPO did not have a documented organizational structure clearly defining key areas of authority, responsibility, or appropriate lines of reporting for e-Passport supply chain security as GPO internal control standards require. The existing Agency oversight process consisted of only one employee responsible for the security of the e-Passport supply chain, the SID Director of Product Security.[7]

***Lack of Coordination among GPO Offices***

The GPO Offices of SID, Acquisitions, General Counsel, Operations Support, Plant Operations, and Security Services each performed their functions related to e-Passport supplies and suppliers (security assessment, procurement, procurement review, and storage/plant security, respectively) autonomously and with little evidence of interaction among the various organizations, and with no written guidelines.

For example, no process existed to ensure that SID and the GPO General Counsel review all contracting actions related to e-Passport suppliers prior to award. Both the SID Product Security Manager and an Associate General Counsel stated that such a process was needed and agreed that having this type of review in place would improve the process. Likewise, the GPO Director of Security Services stated that

---

[7]The GPO Office of Inspector General, in its inspection report AI0502, "Blank Passport Product Integrity and Security", March 31, 2005, recommended that GPO management create and fill a Director of Product Security position.

GPO needed better communication between his office and SID regarding movement of e-Passport blank books and chips within GPO facilities.

The lack of an established, overall e-Passport supply process contributed to each of the issues identified in this report.

## Recommendation

1. GPO Management should develop and publish a formal directive for the security process of the e-Passport supply chain that clearly documents the responsibilities of all personnel involved in the process, including the Public Printer, Deputy Public Printer, Chief Management Officer, Managing Director of SID, SID Director of Product Security, Chief Acquisition Officer, Managing Director of Plant Operations, Managing Director of Operations Support, General Counsel, Director of Security Services, and all applicable subordinate staff. That directive should include the establishment of clear lines of authority for the entire process through the Public Printer.

**Management's Response.** Concur. GPO Management plans to create a new GPO agency directive to address the lines of authority; roles and responsibilities; and security policies, procedures and processes for the multiple secure supply chains that support e-Passports, e-Credentials and other product lines. The complete text of management's response is in Appendix C.

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. The recommendation is resolved but undispositioned, and will remain open for reporting purposes pending the formal publishing of the proposed directive.

## Finding B. Improvement Needed with Documentation for the e-Passport Supplier Security Assessment Process

Improvements are needed to document GPO's internal security assessment process of its various e-Passport suppliers. We identified that GPO did not have:

> (1) documentation supporting the risk levels associated with significant suppliers,
>
> (2) a risk-based schedule listing the frequency of when each supplier/operation should be assessed and the next planned security assessment, and
>
> (3) documentation supporting several assessments of major e-Passport suppliers.

These conditions occurred because GPO lacked sufficient staff to effectively oversee the security assessment process for the e-Passport supply chain. The SID Director of Product Security is the sole GPO official responsible for conducting assessments of e-Passport suppliers. Without adequate documentation supporting the security assessment process, GPO could potentially have difficulty with the continuation of this function should SID experience office attrition.[8]

### *Benchmark Process at the Bureau of Engraving and Printing*

To provide a benchmark for evaluating the supply chain security assessment process, we met with the Bureau of Engraving and Printing's (BEP) Director of Security, Director of Product Security, and several staff members. The BEP, which prints billions of Federal Reserve Notes each year for delivery to the Federal Reserve System, has 10 major suppliers, all located in the United States. BEP requires both personnel and facility clearances for all of its suppliers and has the Defense Security Service handle all facility clearance issuance and monitoring.

BEP's Product Security Branch, which is independent of the organization with responsibility for the BEP production process, is responsible for the security of the supply chain and maintains separate product security files for each supplier. BEP requires that all of its supply chain vendors sign security agreements detailing security and transportation requirements. Personnel from BEP's Product

---

[8]The SID Director of Product Security retired from Federal service at the end of 2009. At this time, the OIG is unaware of how the position will be filled or replaced.

Security Branch and its Office of Compliance[9] evaluate each supplier's conformity with security agreements through surveys and occasional inspections. BEP personnel then use established guidelines and a security checklist for conducting the inspections. The Product Security Branch issues a formal, signed report after every inspection. The BEP Product Security Branch has a staff of seven employees and the Office of Compliance has 25 employees.

Finally, BEP's Emergency Management Division is responsible for evaluating business continuity and Continuity of Operations planning with regards to the printing of Federal Reserve Notes. Part of the Division's mission is to identify sole source suppliers and mitigate any single points of failure.

Based on our review of BEP's process as well as our own audit experience, we believe a formal security assessment process of the supply chain should consist of the following:

- a clearly documented risk analysis for each supplier;
- a schedule of the required frequency of security assessments for each supplier/operation, appropriately designed based upon risk;
- a documented report for each assessment that contains the date of the assessment, recommendations to appropriate officials, and an authorized signature by an appropriate level of management; and
- a follow-up process that shows recommendations are implemented in a timely manner.

***Lack of Documentation of Reported Formal Supply Chain Security Assessment Process***

As indicated above, on April 8, 2008, GPO provided responses to the U.S. House of Representatives Committee on Energy and Commerce on questions regarding passport security. In its response, the Agency stated that:

> GPO and the Department of State [DOS] have a formal audit process to provide security assurance for the electronic component production and assembly facilities. All other suppliers are audited in a formal process by the GPO Director of Product Security using

[9]BEP's Product Security branch works with BEP's manufacturing division to establish criteria for currency production and storage. This branch also handles supply chain security and maintains separate product security files for each supplier and contractor. The Compliance branch is responsible for ensuring its suppliers' compliance with signed security plans and agreements.

> the American National Standards Institute/North American Security Products Organization [ANSI/NASPO] Security Assurance Standards as criteria. GPO is satisfied with the scope and veracity of the audits.

However, we were unable to find any documented evidence of the formal e-Passport supply chain audit (security assessment) process noted by the Agency. Through inquiries of GPO officials, we developed a list of 16 suppliers that provide the most significant components or operations in the e-Passport supply chain and requested contractual and security assessment documentation for each of those suppliers.

Our review of the available documentation indicated that GPO:

(1) identified risk levels for 11 of the 16 suppliers but had no documentation supporting how those risk levels were determined,

(2) had no risk-based schedule of the next planned security assessment for each supplier/operation, and

(3) had 16 security assessment reports on only 11 of the 16 suppliers.

Although there were reports documenting the 16 security assessments performed, the format of the reports were not conducive to ensuring that GPO took proper corrective actions. For example, the reports were not signed by any GPO official; recommendations, if applicable, were not directed to a specific senior GPO manager for action; and the reports contained no specific corrective action timeframes to ensure the timely implementation of recommendations to correct any noted deficiencies. In addition, two reports were not dated. The SID Director of Product Security stated that he uses ANSI/NASPO standards as a baseline criteria in conducting the assessments; however, the assessment methodology and criteria was not documented in the reports.

***Supply Chain Security Assessment Process Performed by One Person***

Although BEP has more than 30 employees to oversee its supply chain process, GPO, which has more major suppliers, including several located in foreign countries, has a product security staff of just one individual (the SID Director of Product Security) to carry out the same oversight activities that BEP performs. Furthermore, while the Office of Security at BEP reports independently of BEP currency printing operations, at GPO, the SID Director of Product Security reports to the Operations Manager within SID, the same organization responsible for producing e-Passports.

The SID Director of Product Security (the Director) stated that he has visited all of the identified major suppliers and is aware of the risks associated with each (OIG staff accompanied him on a review of a foreign e-Passport chip supplier). Because of the time and resource constraints inherent with being a one-person operation, performing more assessments and fully documenting all oversight activities has

been a challenge for the Director. The Director further stated that most GPO e-Passport suppliers are subject to frequent audit and review by other parties of interest, which makes scheduling regular reviews even more difficult. As a result, the Director performs many of GPO's security assessments on an ad-hoc basis.

Although we found no evidence of past issues involving the independence of the Director, conflicts of interest could arise within SID between expending resources to improve the security of the e-Passport supply chain and maximizing revenue generated from e-Passport production. Having the individual who performs the security assessments residing within SID but reporting to an organization outside of SID would mitigate any potential conflicts of interest.

Finally, without adequate documentation of the oversight process for the e-Passport supply chain, GPO may not be able to effectively continue this important oversight function since it is a one-person operation.

## Recommendations

2. The SID Managing Director should:

a. Develop a formal, fully documented security assessment program for the e-Passport supply chain consisting of (1) a documented analysis of the risks associated with each of the e-Passport suppliers, (2) a schedule for performing security assessments on suppliers on a regular basis based on the risks identified in the analysis, including dates of all prior assessments, (3) a standard reporting process containing the results of all security assessments with dates, appropriate signatures, and formal recommendations, and (4) a process for monitoring and following up on recommendations.

**Management's Response.** Concur. The SID Managing Director formed a task force in October 2009 to establish a formal supply chain vendor security assessment program called the "Vendor Security Audit Program" for the e-Passport and e-Credential product lines. Implementation of this new Vendor Security Audit Program will be integrated with the hiring of a new SID Director of Product Security and the roll out of the new supply chains associated with the on-going e-Passport cover Request for Proposal (RFP) during 2010. (see Appendix C).

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. The recommendation is resolved but undispositioned, and will remain open for reporting purposes pending completion and implementation of the new Vendor Security Audit Program.

b. Develop an analysis of the staffing level needed to carry out an effective security assessment process for the e-Passport supply chain based on risk as well as an associated staffing plan.

**Management's Response.** Management stated that the data gained from the implementation of the Vendor Security Audit Program will reveal and drive the resources needed to carry out the process (see Appendix C).

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. The recommendation is resolved but undispositioned, and will remain open for reporting purposes pending completion and implementation of the new Vendor Security Audit Program.

3. The Deputy Public Printer, in coordination with the SID Managing Director, should evaluate the feasibility of having the Agency's security assessment function for the e-Passport supply chain report to a GPO organization independent of SID.

**Management's Response.** Concur. Management is performing a study to formally document the critical phases and components of the supply chains supporting the e-Passport and e-Credential SID product lines. The results of this study will assist GPO Management with decisions as to the appropriate lines of communication and accountability. In addition, the SID Managing Director is planning formal organizational chart changes to incorporate a formal "dotted line" to the Deputy Public Printer to ensure that the Director of Product Security always has a senior executive outside of SID to bring controversial or sensitive observations and reports (see Appendix C).

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. The recommendation is resolved but undispositioned, and will remain open for reporting purposes pending completion of management's study.

## Finding C. No Direct Contractual Control of Significant e-Passport Supply Chain Processes

GPO had no direct contractual relationship with 6 of the 16 key suppliers in the e-Passport supply chain. This condition occurred because of a lack of coordination between SID and the Office of Acquisitions to ensure that GPO had sufficient rights for subcontractor oversight. As a result, GPO has no specific legal rights to review, authorize the subcontracting of, and inspect the operations of companies that provide critical components for the e-Passport, including two companies considered to be single points of failure in the supply chain.

A critical process in e-Passport production is the embedding of computer chips into the passport covers. GPO contracts with two suppliers to provide passport covers with embedded computer chips. Those two suppliers subcontract with one single supplier that embeds the chips into the covers. That subcontractor further subcontracts with two other suppliers that provide the passport covers and the inlay material that covers the chips. Figure 1 shows the contractual relationships between the parties involved in the process of embedding chips into the passport covers:

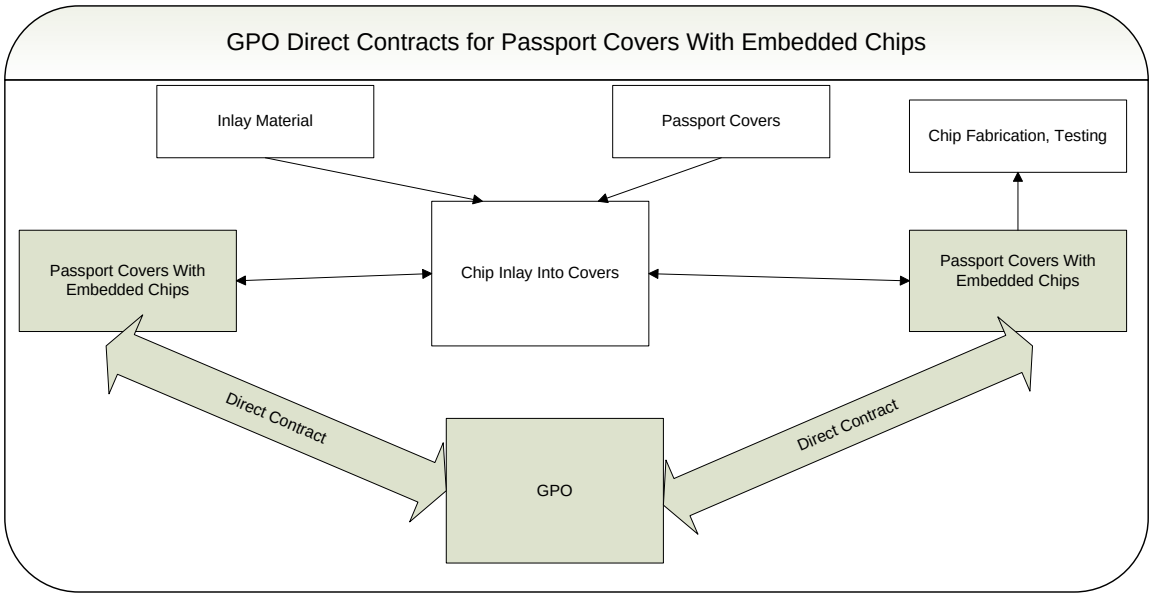


Figure1. Flow of contractual relationships between parties involved in the process of embedding chips into the passport covers. Shaded areas show the only direct contractual relationships with GPO.

GPO did not have a direct contractual relationship with suppliers that provided the following key components within the e-Passport electronic production and assembly facilities: insertion of the computer chips into the passport covers; provision of passport cover stock; provision of chip inlay material; and chip testing

and fabrication. In addition, GPO did not have a direct contractual relationship with two other suppliers responsible for supplying key components of a shielding material used in the passport.

GPO also did not have specific contractual rights to review, authorize the subcontracting of, and inspect these companies' operations with respect to e-Passport supply chain security. GPO identified two of the subcontractors as single points of failure in the e-Passport production process. Despite the challenges presented by the lack of specific contractual rights, the SID Managing Director has developed a working relationship with each of the six subcontractors and has been able to conduct periodic assessments of their operations. However, the lack of contractual agreements does not guarantee similar access in the future.

Through discussions with BEP security officials, we found that BEP requires specific subcontractor approval and oversight requirements in all of its supply contracts. SID is working with the GPO Office of Acquisitions to revise the language of supply contracts for e-Passports to require stronger oversight. GPO currently has a contract with a supplier for work on the new Trusted Traveler Program card.[10] That contract specifically states:

> GPO shall evaluate the supply chain and facility of the prime contractor and any subcontractors for security in handling, storing, and assessing raw or finished product prior to award of contract and reserves the right and authority to perform unannounced evaluations at any time once a contract award is made.

Similar language should be inserted into all contracts for the supply of important components of the e-Passport

## Recommendation

4. The SID Managing Director should coordinate with the Chief Acquisition Officer to ensure that any new contracting action related to e-Passports contains language requiring that GPO maintain the right to oversee subcontractor activities.

**Management's Response.** Concur. The SID Managing Director worked with the Chief Acquisition Officer and his staff to incorporate language in the contract of the upcoming e-Passport cover RFP, as well as all future applicable contracts, that will allow the GPO and DOS' Diplomatic Security Organization to visit, audit and inspect the prime contractors and associated subcontractors (see Appendix C).

---

[10]The Trusted Traveler Program, created under the United States, Canada, and Mexico trilateral Security and Prosperity Partnership, will allow enrolled participants access to all established trusted travel lanes at land crossings, airports, and marine ports of entry.

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. As a result, the recommendation is considered dispositioned, and will be closed upon issuance of this final report.

## Finding D. Lack of Contract Security Requirements

Of the 10 significant e-Passport supply contract files reviewed, 6 did not contain requirements for security, the development of security plans, or appropriate industry-standard accreditation such as NASPO certification.[11] The files did not contain the information because SID, the Office of Acquisitions, and the Office of the General Counsel did not coordinate a review of all proposed e-Passport contracts to ensure that the contracts contained adequate security requirements. As a result, suppliers of key e-Passport components, some of which GPO has designated as high risk, are not contractually bound to provide adequate and appropriate controls over the security of their facilities and employees.

SID officials have expressed a desire to have sound security requirements and appropriate certification requirements written into all e-Passport supplier contracts. However, of the 10 e-Passport supplier contracts examined, only 4 contracts (two for the passport covers with computer chips, one for the passport paper stock, and one for the transportation of the passports from GPO to DOS) contain specific security requirements. Further, of those four, only the contract for the paper stock contains a reference to ANSI/NASPO certification. Some of the suppliers with no contracted security requirements were of concern because those suppliers:

- provided security and forensic features such as security ink, security foil, and security laminate;
- were designated by GPO as high risk;
- were the only known source of a certain supply; and
- were located overseas.

An Associate General Counsel stated that the Office of General Counsel only reviews passport supply contracts when a problem arises. He also recommended that the Office of General Counsel should make it a standard practice to be more proactive with regard to e-Passport supplier contract oversight.

---

[11]NASPO is a tax-exempt 501(c)(6) nonprofit organization created to certify security products organizations through the identification of best practices in the security field. To obtain NASPO certification, organizations must fulfill NASPO accreditation criteria—identified best practices pertinent to high security (NASPO Class I), medium security (NASPO Class II), and basic security (NASPO Class III). Certification by NASPO indicates the recipient company has met the specific requirements of its accreditation process.

## Recommendation

5. The Deputy Public Printer and the Chief Management Officer should direct the SID Managing Director, the Chief Acquisition Officer, and the General Counsel to coordinate efforts to review all new contracting actions related to e-Passports to ensure that they contain appropriate requirements for maintaining adequate security and for attaining appropriate certification.

**Management's Response.** Concur. The new GPO agency directive will include language that specifically directs the SID Managing Director, Chief Acquisition Officer and General Counsel's Office to formally review future contracting actions related to security products and services (see Appendix C).

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. The recommendation is resolved but undispositioned, and will remain open for reporting purposes pending the formal publishing of the proposed directive.

## Finding E. Incomplete Contract File Documentation

GPO did not have sufficient contract file documentation for 5 of the 10 significant e-Passport supplier contracts reviewed. The lack of sufficient documentation occurred because the GPO Office of Acquisitions did not effectively coordinate with SID to ensure that e-Passport contract files are maintained in accordance with the MMAR. As a result, no assurance exists that GPO properly vetted e-Passport suppliers.

The GPO MMAR, Section 4.8, "Government Contract Files", states:

> The head of each division performing contracting, contract administration, or paying functions shall establish files containing the records of all contractual actions. (b) The documentation in the files (see 4.803) shall be sufficient to constitute a complete history of the transaction for the purpose of—(1) providing a complete background as a basis for informed decisions at each step in the acquisition process; (2) supporting actions taken; (3) providing information for reviews and investigations; and (4) furnishing essential facts in the event of litigation or congressional inquiries. (Emphasis added.)

Personnel in the Office of Acquisitions stated that the acquisitions in question were for simple, commercial, over-the-counter products such as ink, papers, glue, or labels; and that using purchase orders was the most economical way to purchase such items. However, although the actual individual products could be viewed as simple commercial products, when taken in context they should be considered significant items because of their intended use as components for e-Passports.

In addition, the contract files for these purchase orders generally consisted of just the purchase order document. Therefore, the files contained none of the information detailed in MMAR Section 4.8(b) above. As such, no documentation existed to support how GPO chose the supplier, how the supplier met the needs of GPO, or if the supplier was secure and financially stable. SID officials stated that such information probably existed somewhere in SID.

Each of the suppliers for the contracts in question provided GPO with sensitive e-Passport materials such as secure ink, secure foil, or secure laminate. Two of the suppliers were foreign companies operating overseas. GPO further noted that two of the suppliers were the only available source for a particular product and designated one supplier as high-risk. Therefore, all transactions concerning these suppliers and their selection process should have been fully documented.

## Recommendation

6. The Deputy Public Printer and the Chief Management Officer should direct the SID Managing Director and the Chief Acquisition Officer to coordinate efforts to ensure that all e-Passport contract actions are documented in accordance with the requirements of the GPO MMAR.

**Management's Response.** Concur. The new GPO agency directive will include language that specifically directs the SID Managing Director and the Chief Acquisition Officer to ensure that all e-Passport contract actions are documented in accordance with the requirements of the GPO MMAR (see Appendix C).

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. The recommendation is resolved but undispositioned, and will remain open for reporting purposes pending the formal publishing of the proposed directive.

## Finding F. e-Passport Storage Issues

We identified several security weaknesses related to the storage of e-Passport components at GPO's Central Office in Washington, DC.

**Security of Passport Book Covers.** A significant supply of passport covers with embedded computer chips are kept in a locked cage in a designated location at GPO headquarters. The cage has two sliding doors. Although one of the doors was protected with a biometric security device requiring fingerprint scans and an access card, the other door was padlocked. Both doors lead to the same storage area.

Having one of the doors padlocked defeats the purpose of having the biometric device on the other door. Personnel in Operations Support stated that GPO did not plan to replace the padlock with another biometric device. Officials in Operations Support stated that a "two-person rule" exists for the storage area, meaning that no one is allowed to enter the area unless they are authorized and accompanied by another authorized employee. However, GPO has no formal documentation or explanation of the two-person rule, nor was there any indication of markings in storage areas requiring any such rule.

**Access to Finished Passport Books.** GPO stored some finished passport books in the same location as the supply of passport covers with embedded computer chips. Storing passport covers and finished passports in the same space provides access to both items by individuals who would not otherwise be permitted access. SID maintained a list of 26 individuals with access to the storage area. That list did not differentiate between individuals authorized to access finished books versus passport covers. In addition, that list contained one individual who no longer worked for GPO and one individual who worked at the Agency's alternate passport production facility in Stennis, Mississippi.

**Storage of Other Passport Materials.** GPO stored some e-Passport adhesive, plastic film, sealing tape, gummed tape, sewing thread, labels, and foil in a room in the basement with double doors padlocked together. Because the doors were not flush with surrounding walls, there was enough space above them through which a person could gain access to the room with enough time and persistence.

## Recommendation

7. The Deputy Public Printer and Chief Management Officer should direct that SID, Plant Operations, Operations Support, and Security Services jointly develop a formal e-Passport supply storage policy addressing (a) physical security and locking specifications for e-Passport supplies, (b) an up-to-date list of personnel authorized to access storage areas for both passport covers and finished books, and (c) procedures for entering storage areas.

**Management's Response**. Concur. GPO's offices of SID, Physical Security and Materials Management have developed SOPs for the movement of e-Passport raw material chips from truck delivery to secure storage as well as to the production spaces. SOPs were also written for the handling and movement of finished goods to secure storage. These modifications will include the physical security requirements for the storage areas, access policies and procedures and directions for the maintenance and control of access lists (see Appendix C).

**Evaluation of Management's Response.** Management's planned action is responsive to the recommendation. The recommendation is resolved but undispositioned, and will remain open for reporting purposes pending the finalization of the SOPs.

# Appendix A. Objectives, Scope, and Methodology

We performed the audit from February through December 2009 at the GPO Central Office in Washington, DC, at BEP's Washington, DC facility, and at several e-Passport suppliers' manufacturing facilities. We performed the audit in accordance with generally accepted government auditing standards.

**Objective**

The objective of the audit was to assess the adequacy of GPO's security over its e-Passport components and supply chain.

**Scope and Methodology**

To accomplish our objective, we performed the following:

- Interviewed GPO officials from the Offices of SID; Acquisitions; Plant Operations; Operations Support; General Counsel; Security Services; and Finance and Administration. Specifically, we interviewed the SID Managing Director; Director of Product Security; Director of Complex Acquisitions and Special Projects; Chief of General and Paper Procurement; Chief of Specialized Procurements; Chief Financial Officer; Associate General Counsel; Director of Security Services; Chief of Physical Security Branch; Chief of GPO Uniformed Police; Chief of Supply Management Office; Supervisory Inventory Management Specialist; and Industrial Security Specialist.

- Interviewed officials from other Federal agencies, including BEP, the Government Accountability Office, and the Defense Security Service.

- Developed a list of 16 significant e-Passport suppliers through input provided by staff from the offices of SID and Acquisitions. Requested contract files and records of all reviews, and security assessments of each of those suppliers performed by GPO, and examined all records obtained.

- Accompanied and observed the Director of Product Security and two security specialists from DOS as they inspected security controls at several e-Passport suppliers' foreign manufacturing facilities.

- Toured and inspected all e-Passport component storage facilities at GPO's Washington, DC central office.

- Toured and observed BEP's Washington, DC Federal Reserve Note printing and supply storage facilities.

- Toured and inspected an e-Passport supplier's United States' manufacturing facility.

**Management Controls Reviewed**

We reviewed and evaluated the management controls associated with the security process for GPO's e-Passport supply chain. Specifically, we determined whether GPO had formal documented policies, procedures, techniques, or mechanisms in place to implement a security process for its e-Passport supply chain; and whether an organizational structure was in place that clearly defined key areas of authority, responsibility, and appropriate lines of reporting for e-Passport supply chain security.

In conducting our review of management controls, we followed Federal Government internal control guidelines in Office of Management and Budget Circular A-123, "Management Accountability and Control," June 21, 1995; GPO Instruction 825.18A; and the Government Accountability Office's, November 1999, "Standards for Internal Control in the Federal Government." The audit identified a management control deficiency in that GPO did not have a formal, Agency-wide process for ensuring security for the e-Passport supply chain as required by basic Federal Government internal control standards. This issue is detailed in Finding A in the body of the report. Implementing the recommendations in this report should improve this management control deficiency.

**Computer-Generated Data**

We did not rely on any computer-processed data for this audit.

**Other Related Reports Issued by the GPO Office of Inspector General**

- GPO Passport Printing Costs, Report 09-02, December 22, 2008

- Protection of E-Passport Production System, Report 08-07, May 30, 2008

- Planning for GPO's Secure Production Facility, Report 08-05, January 28, 2008

## Appendix A

- Operating System Security for GPO's Passport Printing and Production System, Report 08-06, March 31, 2007

- Blank Passport Product Integrity and Security, Report AI-05-02, March 31, 2005

- Passport Security (FORTUNA) System, Report AI-05-01, October 22, 2004

- Passport Product Cost Recovery, Report AI-04-03, September 2004

- Blank Passport Transportation Security, Report AI-04-04, September 2004

## Appendix B. Acronyms Used in the Report

| | |
|---|---|
| ANSI/NASPO | American National Standards Institute's North American Security Products Organization |
| BEP | Bureau of Engraving and Printing |
| DOS | U.S. Department of State |
| FY | Fiscal Year |
| GAO | Government Accountability Office |
| GPO | Government Printing Office |
| ICAO | International Civil Aviation Organization |
| MMAR | Materials Management Acquisition Regulation |
| OMB | Office of Management and Budget |
| SID | Security and Intelligent Documents |
| SOP | Standard Operating Procedures |
| VWP | Visa Waiver Program |

# Appendix C. Management's Response

GPO

**Memorandum**

*Security and Intelligent Documents*

January 29th, 2010

From: Stephen LeBlanc, Managing Director, Security and Intelligent Documents

To: (1) Tony Ogden, Inspector General, Office of the Inspector General
(2) Kevin Carson, Assistant Inspector General for Audits and Inspections, Office of the Inspector General

**Subj: Management's Response to the Draft IG Audit Report #10-XX dated November 24 2009 titled Security of GPO's e-Passport Supply Chain**

Thank you for the opportunity to respond to the draft IG Audit Report #10-XX dated November 24, 2009 and titled "Security of GPO's e-Passport Supply Chain".

The following response is provided for your reference and addresses the seven recommendations contained in Findings A through F.

**Draft IG Audit Recommendation in Finding A: No Formal e-Passport Supply Chain Security Process**

**Recommendation 1: GPO Management should develop and publish a formal directive for the security process of the e-Passport supply chain that clearly documents the responsibilities of all personnel involved in the process, including the Public Printer, Deputy Public Printer, Chief Management Officer, Managing Director of SID, SID Director of Product Security, Chief Acquisition Officer, Managing Director of Plant Operations, Managing Director of Operations Support, General Counsel, Director of Security Services, and all applicable subordinate staff. That directive should include the establishment of clear lines of authority for the entire process through the Public Printer.**

GPO Management concurs with this recommendation. A new GPO agency directive will be created to address the lines of authority, roles and responsibilities, security policies, procedures and processes for the multiple secure supply chains that support e-Passports, e-Credentials and other product lines using proprietary and sensitive components. The scope of this directive will include assuring security and continuity of operations in the various supply chain vendors and contractors as well as the movement, handling, storage and accounting for secure production components within GPO facilities.

An analysis and study is presently underway to document the critical components of each product line supply chain with the intent to record and assess both the "as-is" and "to-be" conditions.

GPO expects to publish a formal directive by April 2010.

1

**Draft IG Audit Recommendations in Finding B: Improvement Needed with Documentation for the e-Passport Supplier Assessment Process**

**Recommendation 2: The SID Managing Director should:**

**a. Develop a formal, fully documented security assessment program for the e-Passport supply chain consisting of a (1) documented analysis of the risks associated with each of the e-Passport suppliers, (2) schedule for performing security assessments on suppliers on a regular basis based on the risks identified in the analysis, including dates of all prior assessments, (3) standard reporting process containing the results of all security assessments with dates, appropriate signatures, and formal recommendations, and (4) process for monitoring and following up on recommendations.**

GPO Management concurs with this recommendation. The SID Managing Director formed a task force in October 2009 to establish a formal supply chain vendor security assessment program called the "Vendor Security Audit Program" for the e-Passport and e-Credential product lines.

This Vendor Security Audit Program includes:

- Formal Vendor Security Audit Authorization Forms signed off by the SID Managing Director to initiate all audits.
- Pre-audit vendor research resulting in a standard Vendor Information Report.
- Audit criteria based on The American National Standards Institute (ANSI), the North American Security Products Organization (NASPO) and applicable International Organization for Standardization (ISO). The key audit criteria will be based on these standards and vendor visits and evaluations will be crafted to employ the NASPO methodology.
- Vendors will be evaluated on their overall risk in the areas of financial health, IT security, secure storage, waste disposal, continuity of operations, physical security systems, personnel security issues, incident history and compliance.
- Documented Vendor Risk Assessment Matrix utilizing a point based analysis and documented risk level for the major criteria resulting in an overall risk score that will drive future audit trip frequencies, corrective actions and resources needed.
- Formal post-audit Security Audit Reports that will be signed off by the SID Managing Director and filed in a systematic manner.

Implementation of this new Vendor Security Audit Program will be integrated with the hiring of a new SID Director of Product Security and the roll out of the new supply chains associated with the on-going e-Passport cover RFP during 2010.

**b. Develop an analysis of the staffing level needed to carry out an effective security assessment process for the e-Passport supply chain based on risk as well as an associated staffing plan.**

The data gained from the implementation of the Vendor Security Audit Program will reveal and drive the assets and resources needed to carry out the associated vendor visits, audits and record keeping tasks. The eventual results of the documented Risk Assessment Matrix and associated risk levels and vendor audit frequencies will dictate the resources required to conduct these processes and programs. Presently SID has one Director of Product Security position dedicated full time to these tasks. The SID Managing Director has worked with GPO Human Capital to create a second position description titled Chief of Product Security to assist the Director in their responsibilities. Additionally, GPO Management's formal analysis of the "as-is" and "to-be"

## Appendix C

aspects of the secure supply chain management practices will aid in decisions as to whether additional human resources are required for these processes and programs. Service Level Agreements (SLA) that define personnel resources, areas of responsibility and roles between SID and other agency business units such as Physical Security and IT Security can be established to formally augment the resources needed to properly execute the Vendor Security Audit Program.

**Recommendation 3: The Deputy Public Printer, in coordination with the SID Managing Director, should evaluate the feasibility of having the Agency's security assessment function for the e-Passport supply chain report to a GPO organization independent of SID**

GPO Management concurs with this recommendation to evaluate the Agency's organizational placement of the security assessment functions. Presently, an analysis and study is underway to formally document the critical phases and components of the product line supply chains supporting the e-Passport and e-Credential SID product lines. With the intent to record and assess both the "as-is" and "to-be" conditions, the results of this study will assist GPO Management with decisions as to the appropriate manning levels needed, reporting relationships, roles and responsibilities to be defined and lines of communication and accountability.

Due to the unique and specific knowledge required of the SID business, products and processes, it is essential that the functions of the supply chain security assessments be conducted by individuals thoroughly in tune with SID operations, processes and future strategies. The draft IG audit recommendation suggested that a possible conflict of interest exists in the current organizational structure where the Director of Product Security reports to the SID Operations Manager and a need for greater independence. To mitigate this situation, the SID Managing Director has already taken action to rewrite the position description for the Director of Product Security and revise the SID organizational chart to show that the position reports directly to the SID Managing Director. Additionally, formal organizational chart changes to incorporate a formal "dotted line" to the Deputy Public Printer will ensure that the Director of Product Security always has a senior executive outside of SID to bring controversial or sensitive observations and reports.

**Draft IG Audit Recommendation in Finding C: No Direct Contractual Control of Significant e-Passport Supply Chain Processes**

**Recommendation 4: The SID Managing Director should coordinate with the Chief Acquisition Officer to ensure that any new contracting action related to e-Passports contains language requiring that GPO maintain the right to oversee subcontractor activities.**

GPO Management concurs with this recommendation. The SID Managing Director worked with the Chief Acquisition Officer and his staff to incorporate language in the contract of the upcoming e-Passport cover RFP that will allow the GPO and Department of State's Diplomatic Security organization to visit, audit and inspect the prime contractors and associated sub-contractors. In addition to this specific case, the SID Managing Director has worked with the Chief Acquisition Officer and his staff to ensure all future contracts for raw materials, services and components that support SID's secure federal credential product lines contain similar standard language that allows GPO personnel to oversee contractor and subcontractor activities.

3

**Draft IG Audit Recommendation in Finding D: Lack of Contract Security Requirements**

**Recommendation 5: The Deputy Public Printer and the Chief Management Officer should direct the SID Managing Director, the Chief Acquisition Officer, and the Office of General Counsel to coordinate efforts to review all new contracting actions related to e-Passports to ensure that they contain appropriate requirements for maintaining adequate security and for attaining appropriate certification.**

GPO Management concurs with this recommendation. The new GPO agency directive (see management's response to the draft Recommendation 1 found in Finding A) will be written with language that specifically directs the SID Managing Director, Chief Acquisition Officer and General Counsel's Office to formally review future contracting actions related to security products and services. This coordination will ensure that the contracting actions contain appropriate requirements for maintaining adequate security.

**Draft IG Audit Recommendation in Finding E: Incomplete Contract File Documentation**

**Recommendation 6: The Deputy Public Printer and the Chief Management Officer should direct the SID Managing Director and the Chief Acquisition Officer to coordinate efforts to ensure that all e-Passport contract actions are documented in accordance with the requirements of the GPO MMAR.**

GPO Management concurs with this recommendation. The new GPO agency directive (see management's response to the draft Recommendation 1 found in Finding A) will be written with language that specifically directs the SID Managing Director and the Chief Acquisition Officer to ensure that all e-Passport contract actions are documented in accordance with the requirements of the GPO MMAR. This coordination will ensure that the contracting actions will be documented, recorded and maintained in a special file designated for contracts dealing with security products and services. Additionally, the Acquisitions organization will investigate the efficacy of scanning these security related contract files into digital format for secondary storage.

**Draft IG Audit Recommendation in Finding F: e-Passport Storage Issues**

**Recommendation 7: The Deputy Public Printer and Chief Management Officer should direct that the SID Directors, Plant Operations, Operations Support, and Security Services jointly develop a formal e-Passport supply storage policy addressing (a) physical security and locking specifications for e-Passport supplies, (b) an up-to-date list of personnel authorized to access storage areas for both passport covers and finished books, and (c) procedures for entering storage areas.**

GPO Management concurs with this recommendation. An existing Directive, titled "Rules and Regulations Governing Buildings and Grounds", will be the core document that will be modified and updated to reflect these secure supply storage policies. Over the past several months, SID, Physical Security and Quality Control and Inventory Management Department have worked closely to consolidate the storage of all secure product raw materials and finished products into specific secure storage spaces. Additionally and to support the ISO 9000 certification processes, SID, Physical Security and Materials Management have constructed Standard Operating Procedures (SOP) for the movement of e-Passport raw material chips from truck delivery to secure storage as well as to the production spaces. SOPs were also written for the handling and for the movement of finished goods to secure storage. These modifications will include the physical security requirements for the storage areas, access policies and procedures and directions

4

## Appendix C

for the maintenance and control of access lists. This cross-functional effort should be completed by April 2010.

Sincerely

Stephen LeBlanc
Managing Director, SID

5

## Appendix D. Status of Recommendations

| Recommendation No. | Resolved | Unresolved | Open/ECD* | Closed |
|---|---|---|---|---|
| 1 | x | | 04/31/10 | |
| 2(a) | x | | 12/31/10 | |
| 2(b) | x | | 12/31/10 | |
| 3 | x | | 04/31/10 | |
| 4 | x | | 04/31/10 | |
| 5 | x | | | 03/31/10 |
| 6 | x | | 04/31/10 | |
| 7 | x | | 04/31/10 | |

*Estimated Completion Date.

# Appendix E. Report Distribution

**Government Printing Office**

Public Printer
Deputy Public Printer
Acting General Counsel
Chief Financial Officer
Chief Human Capital Officer
Chief Information Officer
Chief Technology Officer
Director, Congressional Relations
Director, Security Services
Managing Director, Plant Operations
Managing Director, Security and Intelligent Documents

## Major Contributors to the Report

Karl Allen, Supervisory Auditor
Joel Weiss, Management Analyst