WRITTEN TESTIMONY OF
MICHAEL A. RAPONI
INSPECTOR GENERAL
GOVERNMENT PUBLISHING OFFICE

Before the House Committee on Oversight and Government Reform
October 21, 2015

Good morning, Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee. Thank you for the opportunity to testify on the oversight work of the Office of Inspector General (OIG) as it pertains to "Secure Credentials Issued by the Government Publishing Office." As you are aware, the OIG is an independent entity within the Government Publishing Office (GPO). Therefore, the views expressed in my testimony are based on the findings and recommendations of the OIG and are not intended to reflect GPO's position.

BACKGROUND

GPO produces Federal secure credentials in accordance with its mandate under Title 44 of the U.S. Code to fulfill the printing needs of the Federal Government. According to GPO officials, production of secure credentials falls within the statutory definition of printing. Federal agencies obtain products and services, such as secure credentials, by submitting a Standard Form 1, "Printing and Binding Requisition."

Federal secure credentials include a variety of documents. By agreement with the Department of State (State), GPO produces blank electronic passport books, commonly referred to as ePassports. In approximately 2006, State began issuing ePassports with the addition of a small, contactless Radio Frequency Identification (RFID) computer chip and antenna embedded in the back cover. The computer chip with RFID can store and transmit information to an external card reader.

In December 2007, the Joint Committee on Printing (JCP) authorized expenditures associated with smart card technology for secure identification purposes. GPO subsequently began production in Fiscal Year 2009 for enrollees of the Department of Homeland Security's (DHS) U.S. Customs and Border Protection (CBP) Trusted Traveler Program (TTP) as well as other product lines. Additionally, in 2014, GPO began producing the Border Crossing Card (BCC) for State.

In addition to producing BCCs for State and TTP cards for CBP, GPO produces a variety of secure card credentials for Federal agencies, such as Homeland Security Presidential Directive 12 (HSPD-12)—compliant cards for DHS, driver's licenses for foreign diplomats in the United States, identification cards for U.S. diplomats, and the Transportation Worker Identification Credential (TWIC). GPO's secure card credentials can include electronic security features such as contact or contactless programmable chips, antennas, or a combination of RFID components.

In 2012, JCP authorized expenditures associated with establishment of a continuity-of-operations (COOP) capability for GPO's secure card products and services located at the Stennis Space Center facility in Mississippi.

In 2015, the Government Accountability Office (GAO) reported on its review of activities and processes related to GPO’s production of secure credentials. In its report, GAO states that State and CBP considered a variety of factors for selecting GPO as its source for obtaining secure credentials. Specifically, State and CBP officials believed that after consideration of factors such as interagency coordination and collaboration and pricing, among others, GPO was best able to meet their production needs. State officials noted that factors such as GPO’s experience producing high-performing TTP secure credential cards, its backup production facilities, and the relationship State already had with GPO for producing ePassports led them to choose GPO. For CBP officials, GPO’s experience producing ePassports for State as well as its secure supply chain contributed to selecting GPO.

OIG ASSESSMENTS OF ACTIVITIES AND PROCESSES OF FEDERAL SECURE CREDENTIALS

GPO has established an overall framework of policies and management controls it uses to produce secure credentials. While an established structure is present, opportunities still exist that should help strengthen some activities and processes. OIG has issued 10 reports since 2012 that resulted in 34 recommendations for program improvement relating to secure credentials. Topics for those audits and investigations were: (1) acquisition of U.S. Passport electronic covers (eCovers); (2) supply chain risks associated with U.S. blank ePassports; (3) accountability of ePassports; (4) maturity of the software used to track ePassports through production; (5) the Passport Printing and Production System’s compliance with the Federal Information Security Management Act

(FISMA); (6) system development of a secure credential production system; (7) missing HSPD-12 card stock; (8) verification process when producing law enforcement credentials; (9) employee conduct issues associated with secure credentials; and (10) acquisition of paper used in the production of U.S. ePassports.

For the purpose of this hearing, I will highlight four of the audits.

Acquisition of U.S. Passport eCovers

A key component of each ePassport is its eCover. Each eCover includes manufacturing and inlaying of a contactless computer chip with an antenna assembly. The computer chip contains a central processing unit, operating system software, and various types of memory.

As part of a Hotline complaint, in August 2014 OIG reviewed the key factors used to determine whether a proposal was technically acceptable when GPO procured the most recent U.S. Passport eCovers. In that review, we found that documentation was not sufficient to demonstrate all key evaluation factors were performed, reviewed, and approved by the contracting officer.

One of the issues pertained to inconsistencies with disposition of the test results. In one instance, test results revealed that the eCover submitted by one offeror failed the requirement for the inlay to be smooth, continuous from the edge of the cover to the hinge gap, and to lie flat. In that instance, documents depicted that testing was suspended, and the offeror notified that the proposal was not accepted for award because the product failed to meet specifications. For the remaining proposals, a subsequent test revealed the products failed the specification to read at a rate of less than or equal to 3 seconds. In that instance, the product was accepted.

Accountability of U.S. Blank ePassports

At any stage of the production process, something can go wrong. There may be rejects, operator errors, machine jams, or counting problems. During the production process, computer chips in damaged and nonconforming blank ePassports are electronically destroyed and the books and eCovers containing the computer chips are physically destroyed after production.

In September 2014, OIG reported on the steps GPO took for ensuring accountability of blank ePassports throughout various stages of the production process. By way of computer chips, we traced and analyzed more than 2.4 million eCovers through the production process to final destination at State.

In part, we found a lack of sufficient documentation to support physical destruction of 4,292 eCovers and blank ePassports.

While destruction records did not exist, GPO stated that risks were reduced because of the presence of security cameras, an operational protocol requiring two people be present to enter the physical destruction area, and a requirement for background checks of employees. Our review did not identify any direct evidence indicating that eCovers or blank ePassports were removed from GPO premises.

Supply Chain Risk: U.S. Blank ePassports

GPO produces blank ePassports by integrating and assembling materials and components procured from the private sector using a variety of processes, both internal and external, to test the quality of its products.

Since March 2010, when OIG performed its first audit of the supply chain, GPO has made significant improvements. GPO established a framework and took steps addressing risks related to its highly complex global supply chain for blank ePassports. In August 2010, GPO implemented policies requiring that the Office of Security Services perform a risk assessment of the supply chain for the purpose of identifying threats to the integrity of the secure credentials. Since that time, the Office of Security Services has performed 42 assessments of ePassport suppliers and made 94 recommendations for improvement.

In December 2014, OIG reported on whether GPO identified and addressed risks necessary to protect itself in the event a key component of blank ePassports were either compromised or had its supply chain threatened.

While GPO process improvements are significant, OIG found that procedures for ensuring the security of the supply chain were not always followed. We found that: (1) risk assessments were not conducted for five components within the supply chain, (2) risk assessments did not always include all required components needed for determining risk, (3) prescribed monitoring frequencies were not always adhered to when conducting risk assessments, and (4) risk assessment recommendations were not always tracked.

OIG also identified risks associated with sole-source providers for key components of the supply chain. We found that while business continuity risks associated with sole-source providers were noted, plans for mitigating those risks were not documented.

Development of a Secure Credential Production System

In May 2014, GPO reported that the secure credential production system developed to produce the TWIC failed to process data as expected. The system did not process data at an acceptable rate, and the secure communication connection between GPO and another Government agency failed. Temporary card production delays were reported for June 2014. GPO reported that as of July 2014 the secure credential production system was operating in accordance with the Interagency Agreement. In March 2015, OIG analyzed the steps taken to develop the secure credential production system, focusing on whether risks were adequately mitigated during the System Development Life Cycle (SDLC).

In that audit, we found that GPO has taken numerous steps to establish an overall SDLC policy to follow when introducing a new product, system, or service. Furthermore, GPO has integrated its SDLC policy into its Information Technology (IT) Configuration Management, Enterprise Architecture, and IT security policies. However, in examining the activities associated with development of the secure credential production system, we found project formulation policies were not followed, detailed SDLC procedures were not always developed, and the SDLC framework for managing projects was not followed for approximately 60 percent of the tasks.

RECOMMENDATIONS

Since 2012, OIG has made a total of 34 recommendations, of which 22 are closed and the remaining 12 are open pending further verification. We continue to work collaboratively with GPO to improve operations and maintain a long-standing record in delivering a world-class service to our Nation. We note that Senior Managers are actively engaged in working with OIG to enhance awareness of and involvement in addressing OIG recommendations.

CONCLUSION

In conclusion, OIG is not aware of any current security breaches or supply chain disruptions affecting GPO’s production of secure credentials. Thank you for the opportunity to testify today. I would be pleased to answer any questions that you or any Members of the committee may have.

GPO

MICHAEL A. RAPONI
Inspector General

Mr. Raponi was appointed as Inspector General (IG) for the Government Publishing Office (GPO) in November 2011. As IG, Mr. Raponi oversees the agency's Office of Inspector General (OIG), which provides an independent and objective means of keeping the Director and Congress informed about problems and deficiencies relating to the administration and operations of GPO.

Prior to GPO, Mr. Raponi served 4 years as the Deputy Assistant Inspector General for Audit at the Department of Labor (Labor). While in that position, he oversaw the Department of Labor's audit program, including regional and national audit offices. Before working for Labor, Mr. Raponi held various leadership positions with the Offices of Inspectors General at both the Department of Veteran's Affairs and Department of Housing and Urban Development.

Mr. Raponi served in the U.S. Army as a Patriot Missile System Mechanic during Operation Desert Shield and Operation Desert Storm.

Mr. Raponi holds a Master's Degree in Business Administration from Webster University in St. Louis, Missouri, and a Bachelor of Science Degree in Business Administration from the University of Northern Colorado. Mr. Raponi has earned credentials as a Certified Fraud Examiner, Certified Government Financial Manager, and a Certified Internal Controls Auditor.