Benjamin M. Brink
Assistant Public Printer for Security
and Intelligent Documents
Government Printing Office

Prepared Statement Before the Subcommittee on Government Management, Organization, and Procurement

Committee on Oversight and Government Reform House of Representatives

On Technology For Secure Identity Products

Rayburn House Office Building, Room 2247

Thursday, October 18, 2007
2:00 PM

U.S. GOVERNMENT PRINTING OFFICE | KEEPING AMERICA INFORMED
www.gpo.gov

Mr. Chairman and Members of the Subcommittee, thank you for inviting the Government Printing Office (GPO) to appear here today to discuss technology for secure identity products.

I am Benjamin M. Brink, Assistant Public Printer for Security and Intelligent Documents. Until recently when I was recalled to active duty to mobilize to Afghanistan, I headed GPO's Security and Intelligent Documents business unit, which was created last year as part of our *Strategic Vision for the 21st Century* (December 2004), to perform the functions necessary to produce the e-Passport for the State Department and other Federal products containing both print and electronic security measures.

By both law and tradition, GPO — an agency of the legislative branch – has three essential missions: to provide expert publishing and printing services to all three branches of the Federal Government; to provide, in partnership with Federal depository libraries, permanent public access to the printed and electronic information products of the Government; and to sell copies of authentic printed and electronic documents and other Government information products to the general public.

GPO currently employs about 2,300 staff, more than 75% of whom are represented by 10 unions with 15 bargaining units. For FY 2007, GPO had a total budget of $888 million. Approximately $120 million of that came from direct appropriations for Congressional Printing and Binding and for the Superintendent of Documents. The vast majority of our budget is derived from selling products and services to the Federal Government and the general public.

E-Passports Recently, GPO's fastest growing products and services have been security and intelligent documents. We produce these documents in a trusted, Government-controlled environment, using a secure supply chain, secure technology, and secure personal information. At this date, e-Passports represent the majority of this business, although we project a growing business in Smart Cards and other secure identification documents. We recently received a requisition for Smart Cards from the Department of Homeland Security.

GPO has been producing passports since 1926, when the League of Nations created an international standard for a booklet-style passport specifying the size of the booklet, the position of type, and the method of binding the cover to the pages. Because of GPO's expertise in precision printing and binding, we were selected to produce all passports and we've had the job ever since. Throughout that period, with the State Department and other security agencies, GPO has continuously improved the security of the world's most respected travel document.

Today's e-Passport is the result of a standard issued in 2001 by the International Civil Aviation Organization (ICAO), a bureau in the United Nations that sets standards for many aspects of air travel, including the international standard for interoperable e-Passports. Developmental work was underway at the time of 9/11 and accelerated quickly afterwards. The first U.S. e-Passport was issued to the Secretary of State in 2005.

The principle behind securing the e-Passport is in layered security features. The intricate design of each e-Passport page is in itself a security feature. GPO designers are trained and certified to use secure software to create these designs. Other features are not visible to the naked eye. The security fibers woven into passport paper, and the glue that reinforces the booklet stitching, can only be viewed under ultraviolet light.

Another deterrent to counterfeiting is a sandwich of layered transparent film encasing each data page. On this page, a traveler's identity information and photograph are displayed. Once the layers are fused together, any attempt to separate the layers will destroy all of them. On one of the layers, a kind of super-hologram is embedded. Its appearance changes under fluorescent light from a seal, to a profile of Benjamin Franklin, then to the letters "USA." There are multiple other security features in the pages of the e-Passport booklet.

At the heart of every e-Passport is an integrated circuit, or chip. The chip has been designed, tested, and proven secure under the most challenging conditions. It contains the same personal information that is printed on the data page of the old passport. The only new item is a digital photograph in place of a traditional one. E-Passports are identifiable by the biometric logo stamped on the cover.

Following the issuance of the first e-Passport, there was a dramatic ramp up in e-Passport production during 2006, while production of the non-electronic, or legacy, passport continued. By March 2007, e-Passport production exceeded that of legacy passports, and production of legacy passports ceased altogether in May 2007. Since then, all passports manufactured are e-Passports.

A total of 25 countries currently issue e-Passports that are compatible with the ICAO standard. With more than 15 million e-Passports issued to date, the U.S. has issued more e-Passports than all other nations combined and is currently producing more than 550,000 per week to meet unprecedented citizen demand. GPO manufactures three kinds of e-Passports: Tourist, Diplomatic, and Official. Official Passports are used by Government employees traveling on official business. We also make secure travel documents for other Federal agencies, including a travel booklet for the Immigration Service and another booklet for the Coast Guard.

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. All e-Passports are manufactured under serial number control. By assigning a serial number to the chip each credential is tracked throughout the assembly process. The same serial number is used when the finished credential is personalized. Vendors are regularly audited and reviewed and requirements are continually being improved as procurements expire and are re-bid to bring the extended supply chain under even closer Government control.

Smart Cards The success and experience of our e-Passport program has enabled us to create an expanded family of e-credentials, incorporating proven e-Passport electronics, to assist Federal agencies in meeting the requirements of Homeland Security Presidential Directive 12 (HSPD-12), requiring all Federal agencies to provide employees and contractors with a Smart Card ID by the fall of 2008. These services can also be brought to bear in the compliance with the security and intelligent document standards mandated by the Intelligence Reform Act of 2004.

Based on electronics similar to those used in the e-Passport, Smart Cards grant access to Government facilities, networks, information, and other resources. Utilizing the same principle of layered security adapted for application to polycarbonate and other plastic materials, Smart Cards are composed of layers of printed and non-printed material and contain a programmable chip and antenna. An RFID (Radio Frequency Identification Device) card, a close relative of the Smart Card, contains a small, usually non-programmable chip along with an antenna. In addition to designing and manufacturing Smart Cards, GPO is in the process of procuring the capability to provide card personalization. In the personalization process, the Smart Card chip is loaded with the bearer's identity information, biometric data, and permissions.

To date, GPO has designed the security printing for two card-based identification systems. The most recent, the Trusted Traveler, SENTRI, and NEXUS Cards for the Department of Homeland Security, confirm identity and speed border crossing for regular, pre-registered, low-risk travelers between the United States, Canada, and Mexico. GPO has also designed the artwork and non-electronic security features for the new Department of Defense (DOD) Common Access Card (CAC). This is the identification card for all U.S. armed forces personnel and is currently being phased into the DOD system to provide additional visual security features and to comply with new HSPD-12 standards. This card provides both visual and electronic identification as well as physical and logical access to buildings and systems using its electronics. GPO also assisted the Social Security Administration (SSA) in designing the new security features of the Social Security Card.

When a Smart Card is brought close to or contacts a reader, the transmission of the identity information is often protected by Public Key Infrastructure (PKI) encryption, ensuring the highest level of protection for electronic information that travels over ordinary, non-secure networks. At GPO, PKI is used three ways: to protect personal information on an e-Passport or Smart Card from electronic eavesdropping; to issue certificates of authenticity for electronic documents provided through our Library Services Program; and to enable our customers to issue their own certificates of authenticity. This speeds the process by which official Government documents are submitted to the *Federal Register* and other journals of Government. The GPO has recently been designated as a Shared Services Provider for PKI, one of two Federal civilian agencies with that designation.

GPO Security and Intelligent Document Consulting and Design Services Our security and intelligent documents consulting and design services have been sought by the State Department, Department of Defense, Department of Homeland Security, FBI, Coast Guard, and the Social Security Administration. We have also made recommendations to the Real ID Standards Committee, participating through the Document Security Alliance (DSA), where our security documents expert sits on the board. We have worked closely with agencies like these to propose, develop, test, and improve comprehensive security credential solutions. The services we provide include fraud detection, threat assessment, and supply chain analysis, based on the secure supply chain that protects our e-credentials. We also help our customers identify the weak links in their supply chains and recommend methods by which new links can be forged.

GPO adds value to our consulting services by guiding policy formulation in organizations focused on security document policy. We participate as members of:

- the DSA
- the Federal Identity Credentialing Committee (FICC)
- the Inter-Agency Board for Equipment Standardization and Interoperability (IAB)
- the North American Security Products Association (NASPO)
- the ICAO

By integrating GPO expertise in security credential design, security printing, e-credentials, Smart Cards, and PKI, GPO stands ready to provide Federal e-credential expertise whenever and wherever we can help strengthen our national security.

Mr. Chairman and Members of the Subcommittee, this concludes my prepared statement, and I would be happy to answer any questions you may have.