STATEMENT OF

DAVID TEMOSHOK

DIRECTOR, OFFICE OF TECHNOLOGY STRATEGY

OFFICE OF GOVERNMENTWIDE POLICY

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,

ORGANIZATION, AND PROCUREMENT

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

OCTOBER 18, 2007

Congressman Towns, and Members of the Subcommittee, thank you for the opportunity to participate in today's hearing, my name is David Temoshok from the U.S. General Services Administration (GSA).

I am the Director of the Office of Technology Strategy's Identity Management Division in the GSA Office of Governmentwide Policy. The Office of Technology Strategy's Identity Management Division has been responsible for drafting policy standards for compliance assurance and contract turn-key solutions for identity cards for the Federal workforce as required by Homeland Security Presidential Directive #12.

Homeland Security Presidential Directive 12 (HSPD-12), signed by the President in August 2004, established the requirements for a common identification standard and credentials to be issued by Federal agencies to Federal employees and contractors to gain physical access to Federal facilities and logical access to systems and networks. The Directive specified that the technical requirements for the secure credential meet four control objectives. The credential should be

1. issued based on strong criteria for the verification of an individual's identity;
2. strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
3. able to be authenticated electronically; and,
4. issued only by providers whose reliability has been established by an official accreditation process.

Significant strides have been made to deploy a very complex set of technologies for HSPD-12 cards and credentials in an effective and cost efficient manner that is sustainable into the future. The National Institute of Standards and Technology (NIST) of the Department of Commerce was directed by the Presidential Directive to create standards and requirements for the security and interoperability of the cards and processes required for the government-wide implementation of HSPD-12. Accordingly, NIST issued Federal Information Processing Standard (FIPS) 201, The Personal Identity Verification Standard, in February 2005. NIST has issued additional technical specifications to ensure that the cards, data stored on the cards, and data interfaces are standardized across government implementations. GSA established the FIPS 201 Evaluation Program in May 2006 to evaluate commercial products and services for conformance to the normative requirements of FIPS 201. With NIST, we have established 23 categories of products and services (e.g., smart cards, card readers, fingerprint scanners, facial image capture equipment, card printing equipment, etc.) that require evaluation and testing for conformance to FIPS 201 requirements. Commercial industry has responded to the FIPS 201 requirements quickly and effectively; there now are more than 300 compliant products approved for government-wide use for the implementation of HSPD-12. We publicly post all approved products on the FIPS 201 Approved Products List at our website: www.idmanagement.gov.

To meet the mandates of the Presidential Directive, NIST published requirements for HSPD-12 identification credentials in FIPS 201. Compliant credentials are referred to as Personal Identity Verification (PIV) cards and are tested and approved to meet the following FIPS 201 requirements:

- PIV cards are "smart" cards that contain at least one integrated circuit chip for data storage and computational functions;
- Physical printing of PIV cards provide for standard appearance and mandatory printed information, which includes: color picture, name, employee, organizational affiliation, card expiration date, card serial number, and issuer identification (any other data fields are optional);
- PIV card integrated circuit chips possess the capability to perform data exchange interfaces in both contact and contactless modes;
- PIV cards must contain the following digital credentials: Personal Identification Number (PIN), cardholder unique identifier (CHUID -- a unique number assigned to the specific card, similar to a credit or debit card number), two fingerprint biometric templates, and PIV cryptographic authentication credential (asymmetric key pair and corresponding PIV authentication certificate).
- For security and privacy protection, all PIV data stored on the integrated circuit chip may be accessed by contact interface only following card activation through successful PIN entry; the only PIV data permitted for contactless interface is the cardholder unique identifier (CHUID).

Thus, PIV cards provide multiple digital credentials to accomplish the electronic authentication mandated by the third HSPD-12 control objective. NIST published Special Publication 800-63, Recommendations for Electronic Authentication to provide identity authentication requirements for the four authentication assurance levels established by the Office of Management and Budget in Policy Memo M-04-04. Depending on the level of authentication assurance required for the physical or logical access controls, PIV card credentials (PIN, CHUID, biometric templates, cryptographic credentials) may by used singly or as multiple form factors to accomplish the highest levels of authentication assurance under NIST Special Publication 800-63.

To accomplish the second control objective of the Presidential Directive, FIPS 201 requires both physically printed and electronic security controls for the PIV card. All PIV cards are required to contain security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. Examples of such physical printing controls are: laser etching and engraving, optically variable ink, micro printing, holograms, holographic images, and watermarks. PIV cards are also required to possess the capability of electronic security controls using the cards' cryptographic functions. These controls include:

- Validation of the PIV authentication certificate;
- Validation of the digitally signed objects on the PIV card (i.e., CHUID, biometric template);

- Cryptographic challenge-response using the PIV authenticate key to perform cryptographic functions.

These cryptographic security functions are extremely sophisticated and make the PIV digital credentials virtually impossible to counterfeit. GSA tests the commercial and agency-specific PIV cards to ensure that these security functions are uniformly implemented.

GSA also spearheaded the development of standard government interfaces that will be needed to ensure that the Agency systems can exchange data and work together over the long term. This work defined a common system architecture for components and defined interface specifications for the exchange of data across HSPD-12 system components.

The GSA Managed Service Offering (MSO) was established in the fall of 2006 to provide compliant credential and identity services to Federal agencies meeting the requirements of HSPD-12 and the Federal Information Processing Standard (FIPS) 201.

GSA pursued the managed services strategy to save money but also to improve service quality, and decrease implementation risk. Explicit benefits include:

- Reduced setup cost and risk from the use of a common solution with strong configuration management to ensure that all mandatory requirements are met now and in the future;
- Improved internal controls and accountability for role assignments;
- Improved economies of scale associated with sharing a common hardware and software environment; and
- Increased transparency of services through Service Level Agreements, performance measures, and predictable upgrades.

The MSO is currently serving 67 agencies and commissions with the responsibility to provision and manage over 800,000 electronic identity accounts. This is approximately 50 percent of the civilian Federal population. The MSO allows agencies to offload the difficulty of meeting the FIPS credentialing standards and managing the electronic identity while agencies have continued accountability for providing accurate employee identity data and managing the status of their employees. GSA succeeded in aggregating the needs of multiple agencies to produce volume and cost efficiencies in delivery of credentials as well as providing enrollment infrastructure across the US to efficiently serve both the federal employee and contractor populations who fall under FIPS rules. The service provides a sophisticated identity infrastructure needed to meet FIPS requirements as well as logistics support such as enrollment stations, labor, training, and help desk support needed for high availability, both in normal and emergency situations. Information on the GSA MSO service is available at www.FedIDCard.gov. The GSA Team continues to work closely with all customers to ensure compliance with HSPD-12 requirements.

GSA offers the approved products and services for HSPD-12 implementation on GSA Multi-Award Schedule 70 for government-wide acquisition. GSA has created Special Item Numbers 132-61 and 132-62 for HSPD-12 approved products and services. An amendment to the Federal Acquisition Regulations requires that only approved products be incorporated in agency implementations. The approved products and services on Information Technology Schedule 70 are also available to state and local governments for cooperative purchasing.

In summary, HSPD-12 has had significant participation from industry and Federal agencies. Significant progress has been made in a relatively short amount of time without compromising on the goals of the program and with serious consideration on how to achieve cost-effective implementation. I am happy to take any questions you may have.