STATEMENT OF

MICHAEL SADE

ACTING DEPUTY ASSISTANT COMMISSIONER

INTEGTRATED TECHNOLOGY SERVICE

FEDERAL ACQUISITION SERVICE

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT

U.S. HOUSE OF REPRESENTATIVES

APRIL 9, 2008

Good afternoon Chairman Towns and Ranking Member Bilbray. I am Michael Sade, Acting Deputy Assistant Commissioner for Integrated Technology Service within the Federal Acquisition Service within the General Services Administration (GSA). Thank you for the opportunity to participate on today's panel to discuss the current implementation status of Homeland Security Presidential Directive 12 (HSPD-12).

As part of the implementation strategy for HSPD-12, the Office of Management and Budget (OMB) designated GSA to serve three key roles to facilitate the Government-wide implementation of HSPD-12:

1. "Executive Agent for Acquisition of Information Technology" for the implementation of HSPD-12;
2. "HSPD-12 Shared Service Provider" to provide shared HSPD-12 services and infrastructure to Federal agencies; and,
3. Leadership of the Federal Identity Credentialing Committee.

I will describe these three roles and their status in my testimony today.

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 Presidential Directive required four control objectives be met; specifically, that the new identification standard and credentials must 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. Capable of being 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 credentials in an effective and cost efficient manner that is sustainable into the future. The Department of Commerce was directed by the Presidential Directive to create standards and requirements for the security and interoperability of the credentials 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.

Compliant credentials are referred to as Personal Identity Verification (PIV) cards and must meet the following FIPS 201 requirements:

- PIV cards are "smart" cards that will contain at least one integrated circuit chip for data storage and computational functions;
- Physical printing of PIV cards will provide for standard appearance, mandatory printed information includes: color picture, name, employee and organizational affiliation, card expiration date, card serial number and issuer identification, other data fields are optional;
- PIV card integrated circuit chips will 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); and,
- For security and privacy protection, all PIV data stored on the integrated circuit chip will 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).

Executive Agent for the Acquisition of Information Technology

To facilitate Government-wide implementation of the Presidential Directive and the requirement that all HSPD-12 implementations be interoperable, GSA was designated as the "Executive Agent for Acquisition of Information Technology" for the Government-wide implementation of HSPD-12. 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, GSA has established 23 categories of products (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 are now more than 350 compliant products approved for Government-wide use for the implementation of HSPD-12. GSA established an amendment to the Federal Acquisition Regulation to require Federal agencies to acquire only approved products from the FIPS 201 Approved Product List for the implementation of HSPD-12. In this way GSA ensures that the products used for implementation meet FIPS 201 requirements and can, in fact, be interoperable across Government. GSA publicly posts all approved products on the FIPS 201 Approved Products List at our website: www.idmanagement.gov.

HSPD-12 Shared Service Provider

Federal agencies have been faced with very real challenges – technical, logistic and funding – in order to meet all HSPD-12 requirements and aggressive implementation milestones. GSA established the USAccess Program to offer Federal agencies a compelling solution to this challenge. Through the USAccess

Program, GSA offers participating agencies a managed, shared service solution that simplifies the process of procuring and maintaining PIV compliant credentials, while at the same time, meeting HSPD-12 milestones for issuing the credentials. GSA's Managed Service Offering (MSO) is responsible for administering and coordinating the USAccess Program. The USAccess Program provides shared infrastructure and end-to-end services for all participating agencies and allows the Federal Government to leverage the costs to build and manage complex infrastructure, rather than each agency attempting to build separate redundant systems on their own. It provides the project, acquisition, and financial management necessary to help participating agencies receive the USAccess service.

Since the launch of the program in 2006, the USAccess Program has enrolled approximately 70 Federal agencies into the program, representing the potential to issue between 850,000 to 1 million cards to Government employees. The program also serves as one of the Federal Government's best examples of a cross-Government service (i.e. "shared service") where cost, infrastructure and program management expenses are shared across program participants to produce overall cost savings for the Government.

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

- Centralized program management: Participation in the program alleviates Federal agencies from having to manage the complexities of building and maintaining their own in-house HSPD-12 compliant products. GSA's MSO will manage the acquisition of services, coordinate integration with Government systems, as well as manage contractors for the USAccess program.
- Built-in HSPD-12 Policy Compliance: As the executive agent for the program, GSA has evaluated the technology powering the USAccess system to ensure it meets HSPD-12 requirements. Participating agencies gain immediate access to an end-to-end service that enables them to begin issuing PIV-compliant credentials according to Government milestones.
- Reduced capital expenditures: Using a shared services model, the USAccess program has adopted a simplified, per-credential fee system that eliminates the large upfront costs typically encountered with implementing new IT infrastructures. By leveraging the collective buying power of the Federal Government, the USAccess program spreads infrastructure costs among all USAccess program participants, which in turn reduces the overall price for each individual agency.
- Enhanced Security: Federal agencies can trust the credentials issued under the USAccess program as each credential is registered and verified

according to the requirements outlined by NIST and GSA. By utilizing a standard credentialing system such as the USAccess program, agencies will enhance security and reduce identity fraud. Participating agencies can easily use the USAccess service to procure credentials for their employees and contractors across the United States.

By issuing a common, standard credential to every Federal employee and contractor, the USAccess Program improves Government security and the safety of its citizens. USAccess cardholders can easily identify themselves to other Federal Government workers, while also trusting the identity of other USAccess card holders. At the same time, these card holders will also use their cards to access Government systems and facilities that are critical to performing their jobs. In turn, the Federal Government is able to protect its enterprise infrastructure by validating the identity of people accessing it.

There are currently more than 64 USAccess Program enrollment centers located in more than a dozen states with the majority in the Washington, DC area. Ultimately there will be more than 225 enrollment stations deployed across the country. These are often shared by multiple agencies.

Leadership of the Federal Identity Credentialing Committee

GSA also provides the Government-wide forum for coordination of implementation activities, common issue resolution, and direction through the Federal Identity Credentialing Committee (FICC). All agencies are represented on the FICC to provide a focal point for implementation of the Government-wide identity credentialing capability as required by HSPD-12 and defined in FIPS 201. Members of the FICC are expected to both participate in the implementation of FIPS 201 and champion these activities at the agencies they represent. FICC working groups are tasked with specific work activities to assist in building key aspects of the Government-wide infrastructure for HSPD-12 implementation. A key aspect of this work has been through the FICC Architecture Work Group that has issued the HSPD-12 architecture and technical interface specifications in order to accomplish the long-term objective of Government-wide interoperability of all HSPD-12 solutions.

In summary, the implementation of HSPD-12 has seen major efforts and contributions from industry and Federal agencies and has produced notable accomplishments for Government and industry. The infrastructure that GSA has established for HSPD-12 is critical to meet the requirements of the Presidential Directive and critical implementation milestones. 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.