STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT, OF THE COMMITTEE OF OVERSIGHT AND GOVERNMENT REFORM

April 9, 2008

Good afternoon, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to discuss the Administration's implementation of Homeland Security Presidential Directive 12 (HSPD-12). Protection of our federal facilities and information systems is a priority for the Administration and my remarks today will focus on the progress we have made in improving security through implementation of HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," issued on August 27, 2004.

Prior to HSPD-12, there were wide variations in the quality and security of forms of identification used by Federal employees and contractors to gain access to federal facilities and information systems. The Directive enhances security, increases Government efficiency, reduces identity fraud, and protects personal privacy by establishing a mandatory, Government-wide standard. Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. HSPD-12 is an important component of agencies' information and physical security programs as it improves the basis for making an access control decision. The Directive requires background investigations and standardized identity credentials for employees and contractors. The use of cryptographic credentials will provide a more accurate determination of identity before access is granted. The identity credentials also enable biometric verification when and if the application requires it. The overall goal is to achieve appropriate security assurance for multiple applications, based on an agency risk determination, by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to information systems.

Government-wide Standard

To implement the goals of HSPD-12, the Administration tasked the Department of Commerce to create a government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. In February 2005, Department of Commerce Secretary Gutierrez signed, and the National Institute of Standards and Technology (NIST) published, the Federal Information Processing Standards (FIPS) 201, "Personal Identity Verification of Federal Employees and Contractors." The final version, FIPS 201-1, was issued in March 2006. This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The FIPS 201-1 standard and several associated special publications provide for interoperability of agency credentials and existing Federal Public Key Infrastructure provides the capability to determine the validity of another agency user's credential. To supplement this capability, the General Services Administration (GSA) developed a technical specification for those agencies wanting to exchange additional identity attributes between Identity Management Systems. This draft specification, issued for interagency comment in March 2008, builds upon the technical specifications already issued by the GSA as well as several NIST guidelines available to assist agencies in determining the types of electronic authentication capabilities to implement for addressing requirements of the Federal Information Security Management Act.

With HSPD-12, agencies are also required to adhere to specific business processes for the issuance of Personal Identity Verification (PIV) credentials including a standardized background check, based on existing Office of Personnel Management (OPM) requirements, to verify employees' and contractors' identities. There has been an existing requirement for federal employees to undergo a background investigation based on Executive Order 10450, "Security Requirements for Government Employees," issued on April 27, 1953. HSPD-12 extends these same background investigation requirements to federal contractors with long-term access to federal facilities and information systems.

We have also directed agencies to take full advantage of the capabilities of the new identity credentials and agencies have been requested to prepare plans outlining their implementation strategies. HSPD-12 and the FIPS 201-1 standard provide the technology component that will enable large scale implementation of existing OMB security and privacy directives, such as requirements for two-factor authentication and encryption of personally-identifiable and sensitive information. Use of PIV credentials will also enable secure information sharing across organizational boundaries through the use of cryptography.

By helping agencies evaluate their physical security, information security, and human resources business practices, the Executive Branch is applying a consistent, risk-based approach to physical and information systems security that will improve our security and reduce cost.

Conformance and Interoperability Testing

It is essential for federal agencies to be interoperable if we are to significantly improve the security of our federal systems and facilities. Without interoperability, we will continue to have wide variations in access control implementations which also greatly increases cost. With HSPD-12, this is the first time the President has mandated interoperability of cryptographic credentials across all departments and agencies.

Following the issuance of the FIPS 201-1 standard, the NIST and GSA established a conformance and interoperability program to ensure products are compliant with the standard and interoperable. Currently, there are approximately 350 products and 33 systems' integrators on the Government Certified and Approved Services and Products Listing maintained by GSA. NIST and GSA have also issued various publications and guidance to support interoperability which can be located on the NIST and GSA websites (http://csrc.nist.gov/ and http://www.smart.gov/awg/). The NIST publications primarily focus on security and interoperability requirements for the credentials while the GSA guidance focuses on both the interoperability of products and HSPD-12 system components. Additionally, NIST developed an automated tool which is available for agencies to test their credentials to ensure compliance with the FIPS 201-1 standard. Initial testing of agency credentials was performed by GSA in January 2007.

Reducing Overall Costs to the Federal Government and Streamlining Processes

Agencies have allocated funds for identity management programs and issued credentials for years. In 2003, OMB analyses of executive agency authentication and identity management efforts concluded that agencies were spending in excess of $160 million in FY 2003 and FY 2004 on potentially inconsistent or agency-unique authentication and identity management infrastructure. Beginning last year, OMB is requiring agencies to report current year expenditures for HSPD-12. Analysis of the initial agency submissions indicates inconsistencies in how agencies reported their costs and OMB is working with the agencies to ensure they report complete information and in accordance with the OMB guidance.

To help reduce the overall federal costs of HSPD-12 implementation, the GSA implemented an HSPD-12 Shared Services Offering to agencies in August 2006. Through the GSA service, credentials are offered at a reduced cost due to economies of scale. Currently, 70 federal departments and agencies are participating in the GSA Shared Services program. The service now includes 64 enrollment centers with over 80 enrollment stations available for agency use. Approximately 120 additional enrollment stations are planned for deployment in FY 2008. We anticipate significant cost avoidance across the federal government as a result of the shared infrastructure and services.

HSPD-12 has also been the impetus to streamline the business process of capturing and transmitting electronic fingerprint files used for screening and adjudication of background investigations for new employees and contractors. The new enrollment stations provide for the electronic transmission of fingerprints to OPM and, for those agencies previously submitting hard copy fingerprints, this will speed the screening and adjudication time required for the hiring process.

Privacy Requirements

HSPD-12 implementation is grounded in the longstanding policy framework overseen by OMB. The intent of HSPD-12 is to allow agencies to grant access based on risk-based access control decisions; however, we must also protect the personal information of federal employees and contractors. Agencies must follow existing privacy and security law and policies to ensure employee and contractor information is protected and appropriately used.

In February 2006, OMB issued Memorandum M-06-06, "Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12," which provides agencies with sample privacy documents to use as models in implementing HSPD-12 in their agencies. The sample documents include:

- System of Records Notice of Personnel Security Files
- System of Records Notice for Identity Management System(s)
- ID Proofing and Registration Privacy Act Statement
- Card Usage Privacy Act Statement
- Privacy Impact Assessment for Personal Identity Verification

Subsequently, in May 2007, OMB issued Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." This memorandum re-enforces requirements to protect personally identifiable information.

How Do We Oversee Agency Performance?

To ensure agencies are on track, OMB has taken steps to closely monitor agency implementation progress and the completion of key activities. In September 2006, OMB asked agencies to submit updated HSPD-12 implementation plans. As part of their HSPD-12 implementation plans, we requested agencies document their plans for integrating physical and logical access control systems with the use of PIV credentials. We requested agencies indicate how they intend to use the capabilities of the credentials to the fullest extent possible to address cybersecurity weaknesses and improve physical access control. Additionally, we issued OMB Memorandum M-08-01, "HSPD-12 Implementation Status," on October 23, 2007 directing agencies to either confirm their HSPD-12 implementation plan was still on target or update their plan with a revised schedule by which the agency will meet as soon as possible the requirements of HSPD-12.

In January 2007, OMB issued guidance requiring quarterly reporting on the status of background investigations and number of PIV credentials issued. Beginning March 1, 2007 and each quarter thereafter, agencies were directed to post to their federal agency public website a report on the number of credentials issued. The guidance also requires testing of agency credentials to ensure compliance with the FIPS 201-1 standard published by NIST. Additionally, we asked the President's Council on Integrity and Efficiency to conduct a review of agency processes to ensure they are consistent with HSPD-12 and FIPS 201-1. As a result, several agencies' Inspectors General completed reviews of agency HSPD-12 implementations and provided recommendations to the agencies. On October 26, 2007, OMB also issued a memorandum providing updated instructions for public reporting of HSPD-12 implementation status and we requested additional information on background investigation status and major milestones as outlined in agency HSPD-12 plans. We are ensuring that agency status is transparent and accessible to the public.

Status of Agency Implementations

In accordance with their HSPD-12 implementation plans, by October 27, 2008, agencies are expected to complete background investigations for all existing employees and contractors and ensure their infrastructure and capabilities are in place so they are issuing credentials as standard business practice. Agencies must also continue to complete all additional milestones as indicated in their agency/OMB mutually agreed-upon implementation plans. The current status of agency implementation is as follows:

- On December 31, 2007, OMB released the first aggregate review of agencies' public posting of HSPD-12 implementation status reports. OMB's review and the details of the agency HSPD-12 Implementation Plan reports can be found on the E-gov website (http://www.whitehouse.gov/omb/egov/b-1-information.html.)
- As of March 1, 2008, agencies reported:
    - over 2.5 million or 59% of their employees (which includes military personnel) have completed background investigations
    - over 500,000 or 42% of contractors have completed background investigations
    - over 143,000 or 3% of employees have received PIV credentials
    - over 36,000 or 3% of contractors have received PIV credentials
    - over 900 or 0.8% of other individuals that agencies have identified as requiring credentials based on their long-term access to federal facilities or information systems have received PIV credentials
- In addition to the approximately 180,000 individuals that have received credentials, as of March 31, 141,000 have completed the enrollment process to receive their identity credentials.

Next Steps

As part of our oversight role, OMB will continue to use quarterly reporting mechanisms along with agency information technology budget planning documents to track key performance metrics for HSPD-12 compliance.

Additionally, in anticipation of agencies' plans to integrate the use of PIV credentials with physical access systems, NIST, in consultation with the Interagency Security Committee and several federal agencies, developed Special Publication 800-116, "A Recommendation for the Use of PIV Credentials with Physical Access Control Systems." The publication provides guidelines for securely and cost effectively integrating PIV credentials and readers with physical access control systems. The purpose is to describe a strategy for agencies to enable their physical access control systems to use PIV credentials. The draft publication was released for a 42-day public comment period on April 1, 2008.

Conclusion

Over the past three and a half years, the Executive branch has made steady progress in achieving the goals of the Presidential Directive. HSPD-12 and the FIPS 201-1 standard, when implemented, provide the foundation for identity trust and the ability to streamline business processes to improve authentication processes. The government's implementation and use of PIV credentials will result in a standardized environment for launching a number of new applications and improving the security of federal information systems and facilities.

HSPD-12 is part of the Administration's overall plans to enhance security and is closely aligned with other ongoing security initiatives and plans for improving physical security to implement recommendations of the 9-11 Commission. Once fully implemented, we expect HSPD-12 to significantly improve the federal government's security posture and reduce costs through implementation of standard processes and federated identity management. We continue to build upon our existing efforts to improve security and enhance privacy.

We look forward to working with the members of this Committee and appreciate your continued support in improving the security posture of the federal government.