EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

February 3, 2011

M-11-11

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
Director

SUBJECT: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors

The *Cyberspace Policy Review*, adopted by the President, and the President's Budget for Fiscal Year 2011 highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials including a standardized background investigation to verify employees' and contractors' identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities.[1] Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry.[2]

As discussed in OMB Memorandum 10-28, *"Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),"* DHS is exercising primary responsibility within the Executive Branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543.

In the attached memorandum, DHS outlines a plan of action for agencies that will expedite the Executive Branch's full use of the PIV credentials for access to federal facilities and information systems. I ask for your help in overseeing your agency's implementation of this plan of action and your agency's completion of its adoption of the PIV credentials.

---

[1] HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be due to extenuating circumstances (e.g. system is in the process of being decommissioned.)

[2] Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed (i.e. E-Authentication Assurance Level 1), such as low risk public-facing websites, blogs, etc. For additional information, refer to NIST Special Publication 800-63 at www.nist.gov.

As the DHS memorandum explains, the majority of the federal workforce is now in possession of the credentials, and therefore agencies are in a position to aggressively step up their efforts to use the electronic capabilities of the credentials. To that end, and as the DHS memorandum further explains, each agency is to develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. Moreover, the DHS memorandum outlines a set of requirements that needs to be included in an agency's implementation policy, in order for that policy to be effective in achieving the goals of HSPD-12 and realizing the full benefits of PIV credentials.

Agency progress on HSPD-12 implementation will be monitored by the National Security Staff, and OMB will continue to provide guidance and oversight for agency Information Technology investments.

Questions for OMB may be directed to Carol Bales at 202-395-9915 or eauth@omb.eop.gov.

Attachment

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 3, 2011

MEMORANDUM FOR THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Gregory Schaffer, Assistant Secretary for Cyber Security and Communications,
Department of Homeland Security

SUBJECT: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12
Policy for a Common Identification Standard for Federal Employees and Contractors

The *Cyberspace Policy Review*, adopted by the President, and the President's Budget for Fiscal Year 2011 highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal Personal Identity Verification (PIV) smartcard credentials including a standardized background investigation to verify employees' and contractors' identities. Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities and disaster response sites, as well as multi-factor authentication and digital signature and encryption capabilities.[1] Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry.[2]

This memorandum outlines a plan of action for agencies that will expedite the Executive Branch's full use of the credentials for access to federal facilities and information systems.[3] As of December 2010, agencies reported that approximately 5 of 5.7 million federal employees and contractors have completed background investigations, and 4.5 million have PIV credentials. With the majority of the federal workforce now in possession of the credentials, agencies are in a position to aggressively step up their efforts to use the electronic capabilities of the credentials.

To that end, each agency should develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the agency's policy needs to include the following requirements:

---

[1] HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be justified by extenuating circumstances (e.g. system is in the process of being decommissioned.)

[2] Use of PIV credentials is not required for access to Federal applications where identity assurance is not needed (i.e. E-Authentication Assurance Level 1), such as low risk public-facing websites, blogs, etc. For additional information, refer to NIST Special Publication 800-63 at www.nist.gov.

[3] HSPD-12 applies to federal employees and contractors and requires: (1) completion of background investigations; (2) issuance of standardized identity credentials; (3) use of the credentials for access to federal facilities; and (4) use of the credentials for access to federal information systems.

- Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.[4]

- Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.

- Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order to ensure government-wide interoperability, OMB Memorandum 06-18, "*Acquisition of Products and Services for Implementation of HSPD-12*" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.

- Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.[5]

- The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (available at www.idmanagement.gov).

As an initial step, I request you designate an agency lead official for ensuring the issuance of the agency's HSPD-12 implementation policy. Please send the name, title and contact information for your agency's lead official to HSPD12.FNS@dhs.gov and icam@gsa.gov by February 25, 2011.

The CIO Council guidance referenced above provides agencies with additional guidance to support their HSPD-12 and other identity management implementations. Additional information on HSPD-12 is available in the attached reference materials.

To further support HSPD-12 implementation, the DHS is partnering with the General Services Administration (GSA) on implementation activities. GSA will continue to administer the Interoperability Test Program and Approved Products and Services List for HSPD-12, serve as the Public Key Infrastructure Policy Authority, and manage the HSPD-12 Managed Services Office. The DHS and GSA will work together to provide agencies with guidance for implementing the government-wide architecture defined in the "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance." This includes a DHS partnership with the GSA Public Building Service (PBS) to ensure that implementation of physical access requirements for Federal buildings, under PBS' purview, are implemented in accordance with the

[4] The Federal Information Security Management Act of 2002 requires agencies to ensure that information security is addressed throughout the life cycle of each agency information system.
[5] As indicated in paragraph 4 of HSPD-12, agencies were to begin using the common identification standard in November 2006 to gain physical access to federally controlled facilities and logical access to federally controlled information systems.

"Federal Security Level Determinations for Federal Facilities – An Interagency Security Committee Standard" and NIST guidelines.

We welcome any questions your agency might have regarding this guidance. Questions may be directed to HSPD12.FNS@dhs.gov, icam@gsa.gov, or (202) 219-1627. Please share this memorandum with your Chief Information Officers, Chief Information Security Officers, Chief Financial Officers, Chief Human Capital Officers, Chief Privacy Officers, Chief Security Officers, senior agency officials for privacy, senior agency officials for facilities and physical security, budget officers, and any other relevant offices and individuals within your agency.

cc: Howard Schmidt, Special Assistant to the President and Cybersecurity Coordinator, National Security Staff
Vivek Kundra, Administrator, E-Government and Information Technology, Office of Management and Budget
Martha N. Johnson, Administrator, General Services Administration

Attachment

References

Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004

HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the Federal Government to its employees and employees of federal contractors for access to federally-controlled facilities and networks.

http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

NIST FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for "national security systems" as defined by 44 U.S.C. 3542(b)(2).

http://csrc.nist.gov/publications/PubsFIPS.html

OMB Memorandum 05-24, *Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005

This memorandum provides implementing instructions for HSPD-12 and the Standard (NIST FIPS 201.)

http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2005/m05-24.pdf

Federal Identity, Credential and Access Management Roadmap and Implementation Guidance

The Federal Identity, Credential, and Access Management (ICAM) Roadmap addresses unclassified federal identity, credential and access management and how the Executive Branch of the Federal Government will interact with external organizations and individuals. It provides a government-wide architecture for ICAM.

http://www.idmanagement.gov

NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*

The purpose of this publication is to describe a strategy for agencies to enable their physical access control systems to leverage HSPD-12 Personal Identity Verification (PIV) Credentials. The document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to Federal government facilities and assets.

http://csrc.nist.gov/publications/nistpubs/800-116/sp800-116.pdf