HSPD-12 and Open Identity Initiative

Information Security and Privacy Advisory Board

Carol Bales

Office of Management and Budget

October 27, 2011

HSPD-12 Key Activities FY05-11

2005

- NIST issued FIPS 201 (Feb 2005)
- HSPD-12 implementing guidance issued by OMB (M-05-24) (Aug 2005)
- Agencies submitted HSPD-12 Implementation Plans (2005)

2006

- NIST issued FIPS 201-1 (Mar 2006) and associated publications (e.g. 800-96, 800-53 etc)
- Privacy Models released by OMB (M-06-06) (Feb 2006)
- NIST established Conformance Testing Program (Mar 2006)
- GSA established Interoperability Testing Program & Certified and Approved Products and Services List (June 2006)
- Acquisition guidance issued by OMB (M-06-18) (Aug 2006)
- GSA established HSPD-12 Shared Services Program (Aug 2006)
- Final FAR Rule Issued (Sept 2006)
- Agencies submitted updated implementation plans (Sept 2006)
- Agencies began issuing credentials (Oct 2006)

2007

- OMB issued M-07-06 requiring agency validation and monitoring of compliant identity credentials (Jan 2007)
- NIST issued additional special publications (800-76-1 and 800-104) to support HSPD-12 implementation (2007)

2008

- OPM issued guidance on issuing HSPD12 credentials to non-U.S. citizens (July 2008)
- OMB issued guidelines on using HSPD-12 credentials for physical and logical access (May 2008)
- Information Security and Identity Management Committee chartered by the CIO Council (Sept 2008)
- NIST issued 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems" (November 2008) along with additional publications (800-78-2, 800-79-1, 800-73-2, 800-87) in 2008

2009

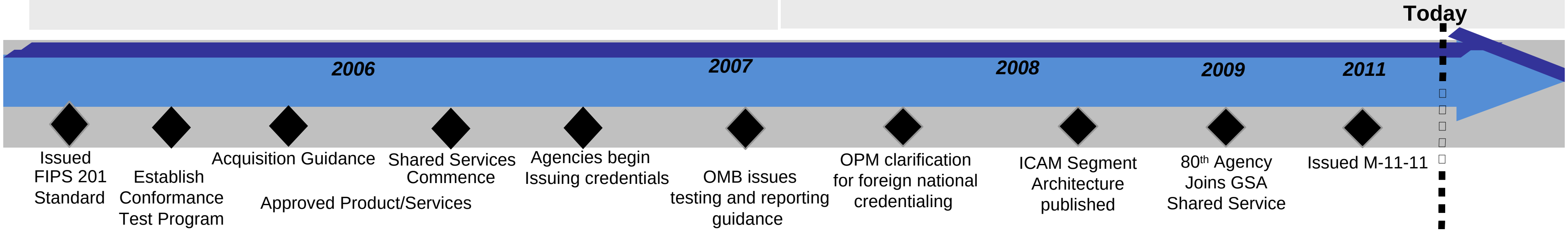
- Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance and Segment Architecture issued (Nov 2009)

2010

- Developed FISMA reporting metrics focused on usage of PIV credentials
- CIO Council issues PIV-Interoperability guidance for non-federal issuers (Jul 2010)

2011

- Issued M-11-11, Continued Implementation of Homeland Security Presidential Directive 12 (Feb 2011)



Today

2006

2007

2008

2009

2011

Issued FIPS 201 Standard

Establish Conformance Test Program

Acquisition Guidance

Approved Product/Services

Shared Services Commence

Agencies begin Issuing credentials

OMB issues testing and reporting guidance

OPM clarification for foreign national credentialing

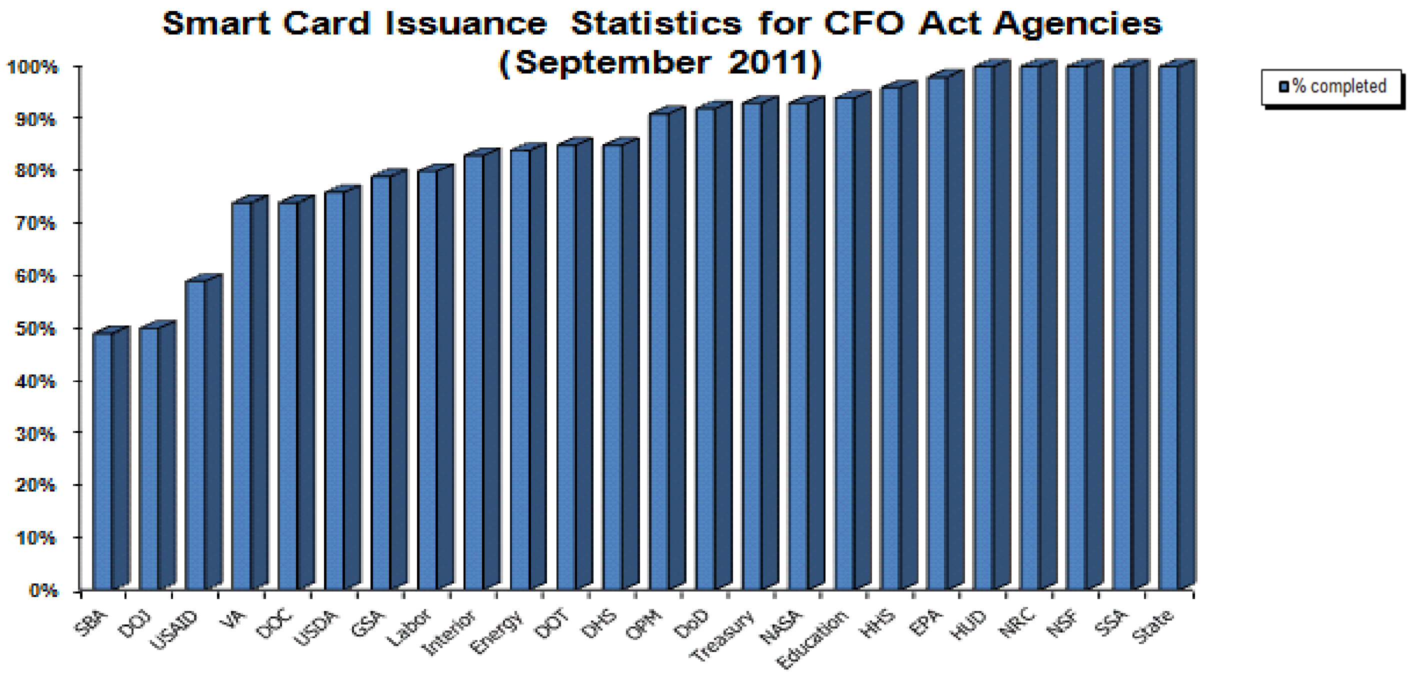
ICAM Segment Architecture published

80th Agency Joins GSA Shared Service

Issued M-11-11

HSPD-12 PIV Card Issuance Status

HSPD-12 Objective: Improve the security of our federal facilities and information systems by implementing common processes for identity proofing and ensuring interoperability through use of standardized credentials for physical and logical access.



PIV Cards Issued as of September 1, 2011: 5,116,925 (89%)
(Includes military personnel)

Agency specific status may be located at:
http://www.whitehouse.gov/omb/e-gov/hspd12_reports/

OMB Memorandum M-11-11

M-11-11, "Continued Implementation of HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors": *Required each agency to issue an implementation policy, by March 31, 2011, requiring use of Personal Identity Verification (PIV) credentials as the common means of authentication for access to that agency's facilities, networks, and information systems.*

Requirements to be included in each agency's policy:

- Effective immediately, all new physical and logical access control systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.

- 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.

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

- 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).

October 2011 OMB Memorandum

October 6, 2011 OMB Memo: Requirements for Accepting Externally Issued Identity Credentials

Effective 90 days following final approval of at least one Trust Framework Provider agencies are to begin implementing the new requirement that will result in full implementation over the next three years by taking the following actions:

- All new development of assurance Level 1 web sites that allow members of the public and business partners to register or log on must be enabled to accept externally-issued credentials in accordance with government-wide requirements.
- Existing assurance Level 1 web sites that allow members of the public and business partners to register or log on must include the requirement to accept externally-issued credentials in accordance with government-wide requirements when those sites are enhanced or upgraded.

Additionally, where appropriate and as resources permit, Levels 2, 3 and 4 websites that allow members of the public and business partners to register or log on should be enabled to accept externally-issued credentials at higher levels of identity assurance in accordance with government-wide requirements.

FICAM Performance Metrics

Key end-state targets include:

- 100% of employees and contractors have PIV credentials (for authentication, digital signature, and to facilitate encryption)
- 100% of government applications accessible to federal employees and contractors using PIV credentials for authentication
  - ***CyberScope was first government-wide application to be PIV-enabled***
- 100% of physical access control systems implemented in accordance with NIST SP 800-116
- 1 digital identity per federal user (when assurance of identity is required) for everyday use and for use during times of disaster response (F/ERO)
- 100% of external agency applications enabled to accept third party credentials for authentication and authorization

For complete list of end state targets see Section 5.3 of ICAM Roadmap

Upcoming Activities/Next Steps

- Federal CIO Council and OMB to issue FICAM Roadmap 2.0
- NIST to issue updated HSPD-12 standard (FIPS 201-2)
- NIST to evaluate options for alternative credential form factors for mobile devices
- Federal CIO Council ICAM subcommittee and Interagency Security Committee to establish joint PIV interoperability working group
  - Work group to consist of representatives from the 18 PIV issuance infrastructures and will focus on facilitating cross-agency use of PIV cards for physical access
- DHS to continue hosting CyberStat accountability sessions
- OMB to host meetings with agencies to discuss requirements outlined in Oct 6 CIO memorandum on accepting externally-issued credentials

Resources

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

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

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

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

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

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

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

Federal Identity, Credential and Access Management Roadmap and Implementation Guidance

http://www.idmanagement.gov

OMB Memorandum 11-11, Continued *Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,* February 2011

http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

October 6, 2010 Memorandum: Requirements for Accepting Externally Issued Identity Credentials

http://www.cio.gov/Documents/OMBReqforAcceptingExternally_IssuedIdCred10-6-2011.pdf

Contact Information

Carol Bales
Policy Analyst
Office of Management and Budget
EOP
Carol_Bales@omb.eop.gov
202-395-9915

Deb Gallagher
Co-chair, ICAM Subcommittee
Office of Government-wide Policy
GSA
Deborah.Gallagher@gsa.gov
202-219-1627

Paul Grant
Co-chair, ICAM Subcommittee &
Special Assistant, Federated IDM and
External Partnering, Office of the CIO
DoD
Paul.Grant@osd.mil

www.idmanagement.gov