



**Interagency Advisory Board**  
***HSPD-12 Insights: Past, Present and Future***

**Carol Bales**  
**Office of Management and Budget**  
**December 2, 2008**



# Importance of Identity, Credential and Access Management within the Federal Government

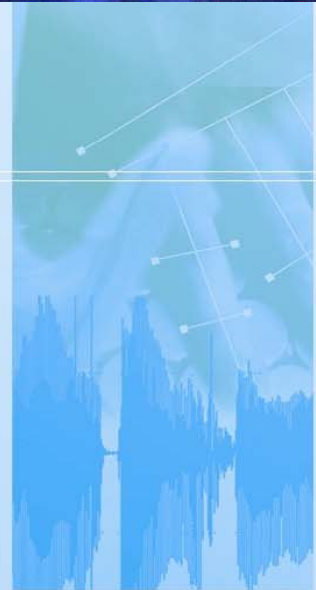
"Trusted Identity" is a key enabler for ensuring the safety and security of our national assets

A growing need to authenticate identity

- Determining access rights on a moment's notice is essential
- Denying access to those who would cause us harm

The following are among our objectives:

- Improve our security by implementing recommendations of the 9-11 Commission, etc
- Achieve appropriate identity assurance for
  - physical access
  - electronic access
- Implement common vetting processes, to extent practicable
- Increase use of cryptographic and biometric identity credentials



# Implementing Secure Authentication and Ensuring Interoperability

## **E-Authentication Policy Framework (M-04-04 and NIST SP 800-63)**

- Established a government-wide framework
- Describes four levels of identity assurance
  - ❖ 1- Little Assurance, 2- Some Assurance, 3- High Assurance, 4- Very High Assurance
- Requires agencies to review new and existing electronic transactions and implement appropriate identity proofing and technical solutions

## **General Services Administration works with private sector to:**

- Ensure Products and Services offered to the federal government meet specific technical and policy requirements and facilitate interoperability
- Enable reuse of identity credentials through trust relationships between different government programs and external entities

**Enablers of the E-authentication policy include HSPD-12 and Federal PKI**



# HSPD-12 & Federal PKI

## Homeland Security Presidential Directive 12

- Issued August 27, 2004 to 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.
- Applies to employees and contractors with long-term access to Federally Controlled Facilities and Federally Controlled Information Systems
- Applicability to other categories based on agency risk (e.g. guest researchers, volunteers, temporary employees under 6 months)

## Federal Public Key Infrastructure Policy Authority

- An interagency body set up under the Federal CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.

*HSPD-12 and FPKI support E-authentication up to Level 4.*



# Benefits of HSPD-12 Credentials

- Provide for digital signature, encryption, and archiving of documents to improve security and facilitate information sharing.
- Attain very high trust in identity credentials during disaster response, disaster recovery, and reconstitution of government scenarios.
- Attain a very high confidence in an asserted identity when logging onto government networks from remote locations.
- Protect PII on government laptops by enabling full disk encryption using the HSPD-12 credential as the encryption key.
- Use a single, interoperable authentication token for physical and logical access to all applications within and across domains.



# Opportunities for Cost Savings/Avoidance

- Agencies are to report identity, credential, and access management (E-authentication) cost savings/avoidance in accordance with OMB M-06-22
- Opportunities for savings/cost avoidance include:
  - Consolidation or elimination of legacy credential systems
  - Use of third-party credentialing or identity proofing services
  - Adoption of an enterprise-wide single (or reduced) sign-on approach
  - Use of HSPD-12 PIV cards for physical and/or logical access
    - For logical access, use of PIV cards could be leveraged for ALL E-authentication identity assurance levels (1-4)
  - Use of federated identity services
- Cost savings could be associated with a number of areas related to electronic authentication and identity management, including:
  - *Help desk calls, user account maintenance, new user identity proofing, PKI software licenses, PKI software maintenance fees, integration, software, hardware, IT operations services, IT operations staff, training, certification and accreditation, privacy/security reporting, and policy compliance.*



# HSPD-12 Key Accomplishments to Date

- NIST technical standard (FIPS 201-1) and several publications have been issued: 800-53A, 800-53B, 800-73, 800-76, 800-78, 800-79-1, 800-87, 800-96, 800-104 & 800-116
- Several OMB policy memos issued – to include acquisition guidance and privacy models
- NIST established Conformance Testing Program in March 2006
- GSA established Interoperability Testing Program & Government Certified and Approved Products and Services List in June 2006
- 390 products and 34 systems integrators on GSA approved products and services list
- GSA Managed Service Office established in August 2006 now serving 70 agencies nationwide
- Final FAR Rule Issued in Sept 2006
- Specification for exchanging IDMS information issued by GSA in 2007
- 20 credential issuance infrastructures are in operation (*issuance stats on next slide*)
- Business process improvements implemented (e.g. fingerprints being transmitted electronically to OPM)
- OPM issued final guidance addressing credentialing of non-US citizens (July 2008)
- Technical standard is being leveraged by other federal programs (e.g. TWIC and FRAC) and external organizations to facilitate interoperability across domains.
- Successful interoperability testing between credentialing programs: Exercises include “Winter Storm” and “Summer Breeze” led by the Department of Homeland Security.

# HSPD-12 Implementation Status

## ***As of October 27, 2008:***

HSPD-12 credentials issued to Employees: **1,249,685 (28%)**

HSPD-12 credentials issued to Contractors: **338,427 (30%)**

## ***As of September 1, 2008:***

Background investigations completed for Employees: **2.5M (52%)**

Background investigations completed for Contractors: **600K (42%)**

Remaining Employees Requiring PIV credentials: **3.1M**

Remaining Contractors Requiring PIV credentials: **800k**

Remaining Background Investigations to be completed for Employees: **2.4M**

Remaining Background Investigations to be completed for Contractors: **800k**

\* "US Military Personnel are included in Employee Numbers.

\* Some Numbers are approximate.



# Expectations for Coming Year

*To achieve the goals of HSPD-12, agencies are to:*

- Complete background investigations for all existing employees and contractors, and continue initiating investigations for all new employees and contractors
- Issue PIV credentials to all new employees and contractors as part of their regular business process
- Issue credentials to existing employees and contractors in accordance with the schedule in their Agency/OMB mutually agreed-upon implementations plans
  - Prioritize issuance of credentials to first responders and ensure compliance with H.R. 1, Section 1615
- Implement plans for integrating logical and physical access control systems with the use of PIV credentials
- Reaccredit HSPD-12 systems in accordance with 800-79-1 (systems must be reaccredited within one year of revised NIST guideline)



# Moving Forward

- The incoming Administration, which will be provided the recommendations of the NSTC IdM Task Force etc, will determine whether to expand the program
- GSA and Federal CIO Council groups to focus on:
  - Completing realignment of key identity, credential and access management functions and services (E-auth/FPKI/HSPD-12)
  - Reducing authentication system development & acquisition costs
  - Facilitating more cost effective solutions for providing credentials to business partners or, through trust relationships, leverage credentials issued by external entities
  - Ensuring interoperability
    - CIO Council to issue “PIV Interoperability for Non-Federal Issuers”
- GSA and Federal CIO Council groups, in coordination with other IdM program representatives and industry, to develop the *Federal Identity, Credential and Access Management Handbook*
  - Handbook to incorporate guidance from E-authentication document suite as appropriate





<http://www.whitehouse.gov/omb>

<http://www.idmanagement.gov>

<http://www.biometrics.gov>

<http://www.fedidcard.gov>

<http://csrc.nist.gov/publications/>

**Carol Bales**

**Carol\_Bales@omb.eop.gov**

**202-395-9915**