
David Temoshok
Director, Identity Policy and Management
GSA Office of Governmentwide Policy

Information Security and Privacy Advisory Board
September 14, 2006
The HSPD-12 Mandate

Home Security Presidential Directive 12 (HSPD-12):
“Policy for a Common Identification Standard for Federal Employees and Contractors”
-- Signed by President: August 27, 2004

- HSPD-12 has Four Control Objectives:
  - Issue Identification based on sound criteria to verify an individual’s identity.
  - Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation.
  - Personal Identity can be rapidly authenticated electronically.
  - Issued by providers who’s reliability has been established by an official accreditation process.
# Key Milestones

<table>
<thead>
<tr>
<th>Timeline</th>
<th>Agency/Department Requirement/Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 27, 2004</td>
<td>HSPD-12 signed and issued</td>
</tr>
<tr>
<td>Not later than 6 months (February 27, 2005)</td>
<td>NIST Issue standard (FIPS-201)</td>
</tr>
<tr>
<td>Not later than 8 months following issuance of standard (October 27, 2005)</td>
<td>Compliance with FIPS-201 Part One: Identity Proofing and Enrollment. PIV-I</td>
</tr>
<tr>
<td>Not later 20 months following issuance of standard (October 27, 2006)</td>
<td>Commence deployment of FIPS-201 compliant Identity Credentials (FIPS-201 Part Two). PIV-II</td>
</tr>
<tr>
<td>Not later than 32 months following issuance of standard (October 27, 2007)</td>
<td>Compliance with FIPS-201 Part Two: Fully operational Physical and Logical Access</td>
</tr>
</tbody>
</table>
Four Authentication Assurance Levels to meet multiple risk levels

- Low: PIN/User ID
- Medium: Strong Password
- High: PKI/ Digital Signature, Biometrics
- Very High: Multi-Factor Token, PIV Card

Access to Protected Website, Applying for a Loan Online, Obtaining Govt. Benefits, Employee Screening for a High Risk Job

Increased Need for Identity Assurance

Increased $ Cost

E-GOV
Multiple Authentication Technologies

To provide multiple authentication assurance levels, FIPS 201 requires multiple authentication technologies:

- Authentication using PIV Visual Credentials
- Authentication using the CHUID – contact or contactless
- Authentication using PIN
- Authentication using Biometric (match on/off card)
- Authentication using PIV asymmetric Cryptography (PKI)

**Something I have – PIV Card**

**Something I know - PIN**

**Something I am - Biometric**
OMB Guidance – Key Points

OMB Guidance for HSPD-12 - M-05-24:

• To ensure government-wide interoperability, agencies must acquire only products and services that are on the approved products list

• GSA is designated the “executive agent for Government-wide acquisitions of information technology" for the products and services required to implement HSPD-12

• GSA will make approved products and services available for acquisition through SIN 132-62 under IT Schedule 70

• GSA will ensure all approved suppliers provide products and services that meet all applicable federal standards and requirements

GSA’s Role

- Establish interoperability and common performance testing to meet NIST standards, product interoperability testing
- Establish Approved Products Lists for product and services categories requiring FIPS 201 compliance
- Qualify products and services on IT Schedule 70 and SIN 132-62 as FIPS 201 compliant
- Provide full-range of qualified products and services to meet Agency implementation needs
- Approved products and services will be made available on government-wide basis through GSA IT Multi-Award Schedule 70
  ✓ Under E-Gov Act of 2002, State and local Governments can acquire products/services directly from IT Schedule 70.
GSA FIPS 201 Evaluation Program

- NIST FIPS 201— the PIV Standard — established normative requirements for processes and technologies for HSPD-12 security and interoperability

- GSA identified 22 categories of products/services directly impacted by FIPS 201 requirements
  - All 22 categories of products/services are needed for HSPD-12 implementation

- GSA Evaluation Program evaluates all products/services for conformance to FIPS 201 requirements
  - Approved products are posted to the Approved Products List

- Evaluation Program Goal — Ensure products/services used to implement HSPD-12 meet all FIPS 201 security and interoperability requirements.
Relationship of HSPD-12 Evaluation and Acquisition Programs

- NIST NPVIP Testing
  - PIV Applets
  - PIV Middleware

- GSA Evaluation Program
  - 22 categories of products and services
  - Interoperability testing
  - Compliance with FIPS 201

- GSA Approved Products List

- GSA Qualified Integrated Solutions and Services

- GSA HSPD-12 Acquisition Program
  - IT Schedule 70
  - SIN 132-61, 62
  - Approved products
  - Qualified services
HSPD-12 System Components

Enrollment Services
Registration
Data Capture Biometrics
Document Verification

Systems Infrastructure
Identity and Card Management Systems

Card Production Services
Card Printing, Production Inventory, & Distribution

Agency Physical Access Control Systems

Agency Logical Access Control Systems

Finalization Service Provider
Cards issued and Activated

PKI Services
FPKI SSP & FBCA
Cross-certified PKI

Black arrows signify data interfaces
Accessing the Approved Products and Services

Approved Products for PKI, systems integrators, and FIPS 201 products are accessed at http:idmanagement.gov
Where are we today? 43 days to go (counting weekends)

• 9 agencies committed to their own infrastructure:
  ✓ DHS, DoD, NASA, DoS, SSA, EPA, NSF, HHS, Treasury

• 100+ Agencies want to share infrastructure
  ✓ All small agencies
  ✓ DOC, HUD, USDA, DOI, GSA, DOE, OPM, Federal Reserve, NARA, FCC committed
  ✓ Several undecided

• Shared Service Providers
  ✓ DoD – for branches of military
  ✓ 8 agencies serviced by State Dept
  ✓ DOI RFP issued July 24 for agencies serviced by DOI HR
  ✓ GSA

• GSA Government-wide Shared Service
  ✓ SSP RFP award 8/18
  ✓ Intended for government-wide use
  ✓ Agencies to sign up through MOU and Interagency Agreement by September 30
  ✓ GSA Managed Service Office established 7/06
  ✓ Will meet 10/27/06 implementation requirements for all participating agencies
**HSPD-12 Shared Services Architecture**

**First**, the issuing agency provides affiliation (sponsorship) feeds, adjudication results, and revocation requests to the SIP. The SIP provides reports back to the agency.

**Second**, the ESP retrieves applicant data from the SIP, enrolls the applicant, and sends enrollment data back to the SIP.

**Third**, the SIP sends fingerprint data collected from the ESP to OPM for suitability checks, and results are sent to the agency.

**Fourth**, after agency adjudication the PSP accepts cardholder information from the SIP needed to print the card. When card printing is completed card data is returned to the SIP, including which chip ID was used for this applicant. The card is then locked with a transport key and shipped to the designated FSP.

**Sixth**, the certificate could be requested and loaded at the FSP, if desired.

**Scope of shared services are HSPD-12 system components inside the red border. These are core HSPD-12 services to meet PIV 1 & 2 compliance. LACS/PACS, FBI and OPM interfaces are outside scope.**
Shared Services Initial Operating Capability

GSA Shared Services will issue PIV cards NLT 10/27/06 for all participating agencies in 4 multi-tenant locations.

**New York, NY**
Jacob K Javits
Federal Bldg
26 Federal Plaza

**Seattle, WA**
Jackson Federal
Bldg
915 Second Ave

**Washington, DC**
GSA-ROB
7th and D St SW

**Atlanta, GA**
Richard B Russell
Federal Bldg
75 Spring St

*** These are the expected locations
Agencies Touched by Initial Rollout

Initial Operating Capability in New York, Seattle, Atlanta, Washington DC provides local access to shared enrollment stations for 133 federal agencies.

New York, NY: Javits Federal Bldg

Seattle, WA: Jackson Federal Bldg

Atlanta, GA: Richard B Russell Federal Bldg

Washington, DC: GSA-ROB
The Shared Enrollment Service will provide an “Enrollment Broker” to handle standard enrollment data from hundreds of enrollment stations into the shared PIV system.
Sharing Opportunities

1. Enrollment Stations – largest single cost; largest opportunity for savings

2. Centralized Components – “fixed cost” item whether 10,000 card holders or 1 million card holders

3. Standard Interfaces
   -- AWG developing standard interfaces for enrollment/SIP, SIP/OPM, SIP/FBI, SIP/PACS, backend authentication
   -- Potential for standard API

4. Other Opportunities - TBD
FAR Amendments for Implementation of HSPD-12

• FAR Interim Rule: Common Identification Standard for Contractors
  ✓ Published as Interim Rule January 3, 2006; final rule approved for issuance 9/06.
  ✓ Contractors must comply with PIV requirements for personnel needing routine access to Federal facilities and/or information systems
  ✓ Coordinated and issued by Civilian Acquisition Council (CAC) and Defense Acquisition Regulations (DAR) Council.

• FAR Case 2005-017: Requirement to Purchase Approved Authentication Products and Services
  ✓ Issued as Proposed Rule, 8/23/06.
  ✓ Requires agencies to use only FIPS 201 approved products and services for the implementation of HSPD-12.
Conclusion

Where we are today.....

It ain’t pretty ..... 

Gotta move forward ...

Lots and lots of moving parts...

I believe we’ll achieve the goal.
For More Information

- Visit our Websites:
  - http://www.idmanagement.gov
  - http://www.cio.gov/ficc
  - http://www.cio.gov/fpkipa
  - http://www.csrc.nist.gov/piv-project

- Or contact:

  David Temoshok
  Director, Identity Policy and Management
  202-208-7655
  david.temoshok@gsa.gov