Requirements of Personal Identity Verification

Standards and HSPD#12

Presentation by NIST June 27, 2005

HSPD-12 Presidential Policy Driver

Home Security Presidential Directive 12 (HSPD-12):

"Policy for a Common Identification Standard for Federal Employees and Contractors"

Dated: **August 27, 2004**

HSPD 12 Requirements

Secure and reliable forms of personal identification that is:

- ❑ Based on sound criteria to verify an individual employee's identity

- ❑ Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation

- ❑ Rapidly verified *electronically*

- ❑ Issued only by providers whose reliability has been established by an official accreditation process

NIST
National Institute of
Standards and Technology

HSPD 12: Requirements (cont.)

❑ Applicable to *all* government organizations and contractors except identification associated with National Security Systems

❑ Used for access to Federally-controlled facilities and logical access to Federally-controlled information systems

❑ Flexible in selecting appropriate security level – includes graduated criteria from *least* secure to *most* secure

❑ Implemented in a manner that protects citizens' privacy

National Institute of
Standards and Technology

HSPD-12 Milestones

Timeline	Agency/Department Requirement/Milestone
August 27, 2004	**Directive signed and issued**
Not later than 6 months (February 25, 2005)	**Issued standard**
Not later than 4 months following issuance of standard (June 25, 2005)	**Program in place to ensure that identification issued by organizations meet the PIV Standard (Part-1)**
Not later than 6 months following issuance of standard. (August 25, 2005)	**Identify additional applications that could benefit from conformance to the standard**
Not later than 8 months following issuance of standard (October 27, 2005)	**Compliance with standard (Part-1)**

NIST
National Institute of Standards and Technology

FIPS 201 Development Process

- ❑ Preliminary thinking posted on PIV web site in late September 2004

- ❑ Held 4 workshops on draft standards (1 workshop for government only)

- ❑ Published preliminary draft and draft for public review

- ❑ Independent coordination with the Government Smart Card Interagency Advisory Board and Federal Identity Credentialing Committee

- ❑ Final consultations with Defense, State, Homeland Security, Justice, OSTP, and OMB

- ❑ Processed ~1900 comments from over 90 organizations.

NIST
National Institute of
Standards and Technology

Nature of Comments on the Draft

❑ Differences from current systems and systems development programs in which substantial resources have been invested

❑ Resource and time required to implement changes to existing systems

❑ Privacy concerns held by unions and public

❑ Time required to conduct background checks

❑ Differences among agencies regarding best mechanisms for:

  ❑ Physical and logical security
  ❑ Technology
  ❑ Performance
  ❑ Business issues

Comment Evaluation - Considerations

Key balancing interests include:

- Increased security
- Enhanced interoperability
- Cost
- Time
- Privacy
- Employee/union interests
- Usability
- Industry concerns

- Training
- Agency flexibility vs. consistency
- Simplicity
- Installed base technology
- Emerging standards and technology
- Technology neutrality

All within the context of meeting the President's HSPD 12 mandate for change

NIST
National Institute of
Standards and Technology

Supporting Documentation

- Supporting Publications
  - SP 800-73 – *Interfaces for Personal Identity Verification* (card interface commands and responses)
  - SP 800-76 – *Biometric Data Specification for Personal Identity Verification*
  - SP 800-78 – *Recommendation for Cryptographic Algorithms and Key Sizes*
  - SP 800-79 – *Issuing Organization Accreditation Guideline*
- NIST PIV Website (http://csrc.nist.gov/piv-project/)
  - Draft and Completed Documents
  - Frequently Asked Questions (FAQs)
  - Comments Received (In Original Format)
- Additional Guidance
  - OMB Guidance (Policy) {http://www.whitehouse.gov/omb/inforeg/hspd-12_guidance_040105.pdf}
  - FICC Guidance (Implementation – *Identity Management Handbook*) {http://www.cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf}
  - NIST Guidance on Certification and Accreditation

NIST
National Institute of
Standards and Technology

Current Fiscal Year 2005 FIPS 201 Schedule

Scheduled Deliveries

Homeland Security Presidential Directive Signed	August 27, 2004
DoC Promulgation of FIPS 201	February 25, 2005
[GSA Federal Identity Management Handbook v0.2	March 8, 2005]
NIST SP 800-73, Interfaces for Personal Identity Verification	April 8, 2005
NIST SP 800-78, Crypto Algorithms for Personal Identity Verification	April 8, 2005
<u>Draft SP 800-79, PIV Card Issuing Organization Accreditation Guidelines</u>	<u>June 17, 2005</u>
NIST SP 800-76, Biometric Data Specification for Personal Identity Verification	June 24, 2005*
Publish FIPS 201 Reference Implementation	June 25, 2005
[FIPS 201 Implementation Plans Due to OMB	June 27, 2005]
Draft SP 800-79 Comments Due	July 15, 2005
Final SP 800-79, PIV Card Issuing Organization Accreditation Guidelines	July 25, 2005

Other FY 2005 Activities

- FIPS 201/FIPS 140-2 Derived Test Requirements
- FIPS 201 Conformance Test Suite
- FIPS 201 Compliance Test Facility Accreditation Guideline
- FIPS 201 Test Implementation Guidelines
- FIPS 201 Pre-Issuance Specification
- [Standard Common Software Platform – Facilitation of FIPS 140-2 Validation]
- [FIPS 201 Component and System Developer's Handbooks]
- Training Documentation [Testing, Developer, Issuer, User]

* Dependent on Homeland Security Council Action

NIST
National Institute of
Standards and Technology