

HSPD-12 FAQs – October 1, 2009

IMPLEMENTATION

1. What documents/programs are currently available to help agencies implement FIPS 201?

- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems
- NIST Special Publication 800-73 specifies PIV card interface characteristics
- NIST Special Publication 800-76 specifies PIV card biometric characteristics
- NIST Special Publication 800-78 specifies cryptographic algorithm requirements and characteristics
- NIST Special Publication 800-79 provides guidance for PIV issuer accreditation
- OMB M-05-24 provides implementation guidance on HSPD-12
- GSA memorandum of August 10, 2005 specifies the procedures for ordering goods and services in compliance with the Presidential Directive
- NIST Special Publication 800-85 provides conformance tests for validating PIV components as complying with SP 800-73
- NIST Special Publication 800-87 contains codes for the identification of Federal and federally-assisted organizations, needed in PIV identifiers
- NIST Special Publication 800-100 Information Security Handbook: A Guide for Managers
- NIST IR 7329: Information Security Guide For Government Executives
- OMB M-05-24 provides policy guidance and deadlines supplementary to HSPD-12
- OMB M-06-18 provides updated acquisition guidance to Federal agencies
- Federal Identity Management Handbook
- Smart Card Handbook

2. Is there a list of "approved" identity proofing and registration processes?

There is not a list of "approved" identity proofing and registration processes, per se. "Approved" means that the process has met the control objectives, and the head of the agency has approved in writing that the process does meet the objectives. SP 800-79 provides further guidance on the certification and accreditation of PIV card issuing organizations. (See FIPS-201, Section 2)

3. Is Personal Identity Verification different from access authorization such that having a PIV card or achieving identity verification does not automatically entitle the cardholder to physical or logical access?

Yes. Access control remains the purview of the local facility or IT system security policy.

4. Will agencies maintain records of access to facilities by individuals?

This is outside the scope of the standard. It can be anticipated that agencies will continue to maintain records, in accordance with the Privacy Act, of access to and unsuccessful attempts to access their facilities and systems as required for their security and audit needs.

5. Does compliance to FIPS 201 mean that every door in every federal building must have a PIV card reader?

No. Generally, agencies will implement FIPS-201 access controls on facility access points (i.e. entry doors) first. Further deployment within the facility is at the discretion of the agency facility security manager. As agencies develop their plans in accordance with HSPD 12, they should focus on the highest-risk facilities for initial deployment of readers. Over time, this could expand to lower-risk facilities.

6. Is a 2.5mm border where printing is not permitted required for the topology of the card?

Yes. Compliance with the dimensions specified in FIPS 201 is required.

7. Does the PIV Sponsor, Registrar, PIV Card Approval and the PIV issuer have to be all different people or can one person have multiple roles?

A two-way separation of roles is the absolute minimum that could possibly meet the FIPS 201 test. In practice, however, it would be challenging to define two roles such that each provides a reliable cross-check on all critical actions of the other. Special Publication 800-79 recommends "the roles of Applicant, Sponsor, Registrar, and PCI [PIV Card Issuer] must be played by different people when issuing a PIV Card." Such a three-way separation of roles can generally be sufficient to insure that the test of FIPS 201 is met, namely, "a single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential." However, the requirement for a particular separation of roles depends on the implementation of the PIV issuance system.

8. What format is required for the enrollment record (which encapsulates biometric records, document scans, demographic information, etc.)?

The standards permit individual departments and agencies to select the format most appropriate to their operations.

9. Does Registrar record signing only apply to pen-and-paper records, or does it also apply to electronic enrollment records?

The requirement applies to both paper and electronic storage. The method is left to individual departments and agencies. If cryptographic signature processes are employed, they must conform to the requirements of NIST standards and guidelines.

10. During reissuance, if an attribute has changed, who is responsible for verifying the change and recording the change and the reason for it?

This function is best performed by the Registrar since this is the individual rechecking the records during card re-issuance. However, this is open to individual agency discretion which may choose to utilize an alternative process.

11. Is support for PIV card logical access mandatory on enrollment systems and/or issuance systems? If so, is PIV card verification required for all operator logins?

Credential-based identification support is specified in FIPS 201. Use of the identity credentials for specific access control applications is not. However use of a PIV card to verify Registrar, Sponsor, Approval, or Issuer roles for card issuance activities as an on-going activity would be an effective mechanism for maintaining the security of the process.

12. Do PIV enrollment systems need to communicate directly with PIV Digital Signatories, PIV issuance systems or any other satellite systems, or is it expected that all of this will be conducted via the IDMS?

This will vary based on individual agency implementations.

13. Will PIV enrollment systems be expected to send Electronic Fingerprint Transmission Specification (EFTS) records directly to the FBI Integrated Automated Fingerprint Identification System (IAFIS), or is that a function that will be handled by the IDMS?

This will vary based on individual agency implementations.

14. For the facial image, is there a specific color backdrop that should be used?

There is no backdrop color requirement; however, per the recommendation of the International Committee for Information Technology Standards (INCITS) 385, the background should be uniform.

15. Can identity proofing be conducted by federal employees and also "trusted agents," where trusted agents might include contractors?

FIPS 201 does not prohibit contractors from being employed to conduct identity proofing activities

under the supervision of government employees in accordance with departmental or agency security and contracts management policies.

16. How can agencies receive an advance report of the fingerprint check results?

Agencies who receive their investigations from OPM, may obtain advance reports of fingerprint check results by putting the code "R" in the Codes block of the Agency Use section of any of the standard investigative forms (SF-86, SF-85P, or SF-85).

17. Is guidance available on how to implement PIV cards with physical access control systems?

18. Is there a plan for agency IDMS and CMS systems to be linked?

Linkage of any backend identity infrastructure is not envisioned at this time due to proprietary data formats as well as security and privacy concerns. However, because PIV cards are standardized, a PIV card issued to an employee at one agency may be used at a different agency if the agency grants access.