Frequently Asked Questions About the Standard for Personal Identity Verification (PIV) of Federal Employees and Contractors

Background
On Aug. 27, 2004, the President issued a Homeland Security Presidential Directive calling for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors.

According to the directive, “secure and reliable forms of identification” means identification that is based on sound criteria for verifying an individual employee's identity; is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; uses electronic methods of rapid authentication; and is issued only by providers whose reliability has been established by an official accreditation process.

The directive called for the Secretary of Commerce to promulgate the federal standard by the end of February 2005 in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget, and the Director of the Office of Science and Technology Policy. To help fulfill the Commerce Secretary’s mandate under the directive, DoC’s National Institute of Standards and Technology (NIST), in conjunction with other organizations, developed the standard as Federal Information Processing Standard (FIPS) 201, Personal Identity Verification for Federal Employees and Contractors. Commerce Secretary Carlos Gutierrez approved FIPS 201 on Feb. 25, 2005. (FIPS are issued by DoC’s NIST after approval by the Secretary of Commerce pursuant to the Federal Information Security Act of 2002.)

The directive is available at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, and other information is available at http://csrc.nist.gov/piv-project/index.html.

1. Which agencies are responsible for implementing the directive?
Four federal agencies have specific responsibilities for implementing this directive: Department of Commerce, Office of Management and Budget (OMB), General Services Administration (GSA), and Office of Personnel Management (OPM). DoC’s NIST is establishing standards, recommendations, guidelines, and conformance tests for components of the PIV system. OMB is responsible for overseeing agency implementation of the directive and will develop implementation guidance for federal agencies. GSA is responsible for assisting agencies in procuring and operating PIV sub-systems such as card and biometric readers. OPM is responsible for assisting agencies in authenticating and vetting applicants for the PIV card.

2. Were comments on the standard sought from the public and other federal agencies?
DoC/NIST and OMB held several public meetings to discuss the technical and policy issues related to the standard. DoC/NIST released the draft standard on November 8, 2004, and on Dec. 20, 2004, released two drafts of supporting technical documents. Public meetings were held on Oct. 7 and 8, 2004; Nov. 18, 2004; and Jan. 19, 2005. DOC/NIST worked closely with other federal agencies, including OMB, the Office of Science and Technology Policy, and the Departments of Defense, State, Justice, and Homeland Security, as well as private industry. As a result, comments were received from more than 80 organizations and individuals. These comments were carefully considered and led to many changes in the standard. (Comments are available at http://csrc.nist.gov/piv-project/FIPS201-Public-Comments.html)

3. What must agencies do and when in order to meet HSPD-12 and FIPS 201 requirements?
Key activities that each agency must perform include—

- establish a program to ensure that the identification issued by their organization meets the PIV standard (within four months of the issuance of the standard);
- identify any additional applications (beyond the scope of the standard) for which the standard also should be used and report them to the Assistant to the President for Homeland Security and the Director of the Office of Management and Budget (within six months of the issuance of the standard);
- comply with the first phase of the PIV standard within eight months of the issuance of the standard; and
- comply with the second phase of the PIV standard on a timetable to be established by OMB.

4. How is security being improved?

The standard was designed so that compliant components and systems will provide improved security over many existing practices and systems for federal facilities and information systems—both the “identity proofing” process and technical security mechanisms.

In the PIV “identity proofing” process, government agencies must obtain and review for each applicant at least two identity documents issued by approved government entities. At least one of the documents must be a government-issued photo ID. The standard also mandates that agencies vet an applicant through an OPM background investigation process, the National Agency Check with Written Inquiries (NACI). This is not a new requirement for employees; it is new for some contractors. Government policy has required this check for all employees since the 1950s. The initial phase of that check, known as the “National Agency Check,” must be completed before the new ID card is issued. When the written inquiries part of the NACI is completed, the agency must review the results (as is required now) and take appropriate action if negative results are received.

The technical security mechanisms include the use of smart card, cryptography, and biometrics technologies to achieve graduated levels of security for agency applications. Identity credentials are securely stored and protected on the Integrated Circuit Chip (ICC). Cryptographic key material and a Personal Identification Number (PIN) on the card provide for the protection of sensitive stored and communicated data using NIST approved algorithms. When used with the card—“something you have,” biometrics provide an additional layer of security in the form of “something you are.” The standard includes requirements to protect the privacy of PIV cardholders.

The PIV standard enhances the overall security of the system by supporting the following objectives:

- A credential is issued only to an individual whose true identity has been ascertained by the issuer.
- Only an individual with a background investigation on record is issued a credential.
- An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid federal or state government issued picture ID.
- Fraudulent identity source documents are not accepted as genuine and unaltered;
- A person suspected or known to the government as being a terrorist is not issued a credential.
- No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued.
- No credential is issued unless requested by proper authority.
- A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked.
- 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.
- An issued credential is not modified, duplicated, or forged.

5. What are the primary requirements for an agency to implement FIPS 201?

The FIPS 201 requires issuance of identity credentials that consist of public key infrastructure (PKI) and biometrics technology on a smart card. The high-level requirements as specified in FIPS 201, in accordance with HSPD 12, are as follows:

- identify the facilities, systems, and other applications that will use the PIV standard;
- obtain the services of an accredited PIV card issuer;
- review and revise procedures for PIV card applicants to provide acceptable identity source documents (i.e., OPM I-9) and complete PIV card application;
- obtain services for capturing biometric information as specified in the FIPS 201;
- obtain PIV card readers with biometric readers as needed;
- procure cards, readers, and PKI services conforming to FIPS 201;
- enable applications to use the PIV card; and
- operate and maintain a PIV card authentication and personal identity verification system.

6. How does FIPS 201 protect privacy?

Protecting personal privacy is a core requirement of the presidential directive. Many of the requirements in the standard for hiring federal employees are based on longstanding privacy law and policy. For example, agencies are required to appoint a PIV privacy official, assess their PIV systems to ensure privacy is protected, identify information to be collected about individuals and how the information will be used, assure that systems containing personal information adhere to fair information practices, and audit systems for compliance with privacy policies and practices. Also, the Office of Management and Budget will provide additional implementation guidance for federal agencies concerning privacy.

The government will not establish a central database to track movement of employees and contractors or the systems they access. Personally identifiable information stored on the card is minimal. Personally Identifiable information such as electronic fingerprints will be cardholder protected (e.g. requires a PIN to unlock) while stored on a PIV card.

The technology on the card does not allow for tracking movement of contractors and employees while moving throughout a building. Because of the wireless capability of the PIV card, concern has been expressed that data can be inadvertently or maliciously captured. To alleviate this concern, employees will be required to keep the card in an electronically opaque sleeve when not in use to minimize the risk of unauthorized reading of data from the card without the consent of the cardholder.

7. What is the rationale behind the selection of smart card, fingerprint, and PKI technologies?

The presidential directive required a standard for secure and effective identification and authentication of federal employees and contractors but did not specify how to achieve it. DoC/NIST proposed using a single form factor (credit-card-sized printable badge) containing one or more integrated circuit chips in order to create a portable means to store and process data in a secure manner. Many organizations already have adopted smart card standards and technology for identity verification. Cryptography can be used to provide data integrity and confidentiality protection for data communications and storage. A Public Key Infrastructure can provide the support system needed to deploy and protect the cryptographic keys.

Of the several potential means of personal biometric marker verification (e.g., DNA, iris scans, hand geometry, handwritten signatures, facial images, or fingerprints), fingerprints were chosen as being the least invasive and most cost-effective, reliable, repeatable, and accurate means of verification available using publicly available technology. While the best fingerprint capture, storage, and matching algorithms are still a matter of debate, NIST fingerprint experts recommended the use of two fingerprints for storage on the card as the most acceptable for inclusion in the standard. To minimize storage requirements, storage of an electronic facial image is not required but is optional. A facial image is required to be printed on the card for visual verification.

Agencies may choose to augment the minimum requirements of the standard.

8. Does FIPS 201 apply to all agencies including the smaller agencies (e.g. micro-agencies)?

All federal departments and agencies and all their contractors requiring access to federal facilities and systems must comply with this standard and the specifications in the supporting documents, except that the standard shall not apply to identification associated with national security systems as defined by law. Small agencies may join with other agencies (and are encouraged to do so when cost effective) to implement and use FIPS 201 complying components and systems.

9. Are waivers to the standard allowed?

There is no provision for waivers to standards issued by the Secretary of Commerce under the Federal Information Security Management Act of 2002. HSPD #12 also does not provide a waiver provision.

10. Can federal agencies use the standard for other purposes beyond the scope of the standard to include national security applications?

The HSPD envisions potential other uses of the new standard and specifically tasks agencies to identify additional applications important to security for which the standard might be employed. Such wider use must conform to OMB policy (including the relevant privacy provisions) and, if national security systems are involved, the applicable requirements to protect national security information and systems.

11. How is agency compliance monitored and what happens if an agency does not comply?

Like many other agency activities, oversight is the responsibility of each agency's Inspector General, the Office of Management and Budget, the Government Accountability Office, and oversight committees of Congress. NIST is responsible for providing a conformance test program to help agencies comply with FIPS 201. Information on the conformance program is available at http://csrc.nist.gov/piv-project/index.html. Non-compliance may include a range of consequences from negative audit reports to budgetary impacts. More importantly, agencies that do not comply will not meet the President's HSPD 12 goals of secure and reliable identification for federal employees and contractors.

12. What are the funding sources for agency implementation of FIPS 201?

All federal agencies have existing background check, access control, and identification credential activities. It is anticipated that these activities, and the funding used to support them will be used in support of activities compliant with FIPS 201. Any additional funding needs for implementing FIPS 201 should be requested by agencies through the normal federal budget process.

13. What documents/programs are currently available or under development to help agencies implement FIPS 201?

- NIST Special Publication 800-73 specifies PIV card interface characteristics.
- Draft 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 will provide implementation guidance on HSPD-12.
- NIST will provide conformance tests for validating PIV components as complying with FIPS 201.
- Subject to funding support, NIST will provide technical assistance to support implementing and operating a PIV system that complies with FIPS 201.

14. Can a PIV card be used by other organizations for other purposes (e.g., access to private facilities, identification for airline travel)?

A PIV card could be accepted for other ID purposes by visual verification of the picture on the card with the cardholder. Restrictions on such uses are difficult to enforce and are impossible in many cases.

15. If a large corporation were to meet the requirements of the specification, would their corporate badges be acceptable for access to federal facilities and information resources?

The technical contents of a PIV card are just one part of an agency's PIV system. The initial validation of identity source documents, vetting of a PIV applicant, cryptographic sealing of data elements on the card by an accredited issuer, and interfacing with the access authorization and control systems are other parts. No existing corporate badge system is expected to meet all the provisions of FIPS 201, including the federal background checks, and hence would not be acceptable without augmentation. Agencies receiving such requests may wish to address this on a case-by-case basis.

16. How many times can an applicant reapply before a permanent denial is issued?

An applicant does not apply directly for a card but provides information so an agency can support a card issuance request. Individuals may apply for federal or contractor employment as often as they choose. However, since OPM centrally conducts background checks, their records could be used to identify any attempts to abuse the system or "shop around" among agencies for a valid credential.

17. Will PIV documents stress that Personal Identity Verification is different than access authorization and just having a PIV card or achieving identity verification should not entitle the cardholder to physical or logical access?

Identification/authentication and access control are very distinct processes.

The PIV card provides a means for the cardholder to verify his or her identity by authentication of a cardholder's PIV card, credentials, and comparison of biometric markers stored on the card with those captured from the current card holder.

The decision of who will have access to which facility or computer system is outside the scope of the standard. Each agency will continue to decide who is allowed access to their specific resources and facilities. More specifically, all cardholders will not have access to all federal buildings or information systems.

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

The standard does not address this. We anticipate 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.

19. How much will it cost agencies to implement FIPS 201?

This will vary by agency depending upon how well its current identification credential program already meets the requirements of the new standard and the level of difficulty or complexity to migrate to the new standard. Some costs (e.g., understanding requirements, initiating projects) are fixed; some (e.g., PIV card readers, PIV card issuer facilities) are proportional to the number of facilities and systems involved; some (PIV cards, PIV card issuance) are proportional to the number of employees involved.

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

Clearly this is not practical. As agencies develop their plans in accordance with HSPD 12, they should focus on the highest-risk facilities and systems for initial deployment of readers. Over time, this could expand to lower-risk systems and facilities.

21. What is a concise security policy statement that can be used for implementing and operating a PIV system?

One sample might be: "It is the policy of this organization to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by adopting and using procedures, components, and systems for secure and reliable identification and authentication of federal government employees and contractors (including contractor employees) as specified in FIPS 201 and its supporting documents.”

22. Why is the standard divided into 2 parts?

The standard is divided into two parts so agencies can make an orderly migration—in terms of both technology and "identity proofing"—from their current systems to the requirements established by the standard and meet the ambitious deadlines established by the President in HSPD #12. We first focus on the most important goal: improved security. The first part, to be implemented within eight months of the standard's issuance, focuses on security objectives, to include "identity proofing." With all agencies meeting the same security objectives, there will be a basis for trust among agencies with regard to the mutual recognition of their employee and contractor credentials. The second part of the standard, which will take longer to implement because of the many varying electronic credential systems now in place, focuses on the common technical interoperability requirements of HSPD #12. When fully implemented, a card from one agency can be electronically recognized by any other agency so that a decision of whether to grant the cardholder access can be made.

23. What information is required to be stored on the card?

Only a minimal amount of information is required to be electronically stored on the card. The PIV Card must contain only the following data:

1. Personal Identification Number (PIN)—this data is used to authenticate the cardholder to the card--in the same way a PIN is used with an ATM card. The PIN never leaves the card, and it cannot be read from the card.
2. A Cardholder Unique Identifier (CHUID)—this number uniquely identifies the individual within the PIV system.
3. Two fingerprint biometrics that are PIN protected.
4. One asymmetric cryptographic key pair used to authenticate the card to the PIV system.

The standard does not require any other personal information such as the cardholder's SSN, address, or phone number to be stored on the card. Release of biometric information and use of the private key can take place only AFTER the cardholder provides the correct PIN number. Only the Cardholder Unique Identifier is required by the standard to be available through the wireless interface.

24. What will the card look like?

Various possible configurations of the card topology are included in the standard. Each card will contain a required set of items (e.g., a printed picture of the cardholder, name, expiration date, etc.) However, the appearance of the cards will vary a bit among agencies as each agency will decide which of the optional fields (e.g., signature, agency seal, issue date, etc.) they choose to use—or even define their own, within the flexibility provided by the new standard.