F.A.Q. - FIPS 201

NASA SEWP Security Center

Erika McCallister
Dennis Taylor
Adam Schuchart

May 6, 2005

DISCLAIMER

This FAQ is intended for informational purposes only. It represents the NASA SEWP Security Center's interpretation of FIPS 201. There are no express or implied warranties regarding the veracity of the information provided. Please contact NIST directly for further information or questions about FIPS 201.

Table of Contents:

FIPS 201 Background:

1. What is the history of FIPS 201?

   Federal Information Processing Standard (FIPS) 201 is the result of President George W. Bush's desire to have interoperable federal identity management systems (IDMS) for access to federal facilities and systems. The idea began as part of the President's Management Agenda during Bush's first term. In July, 2003, the Office of Management and Budget (OMB) initiated the process by sending a memo to each federal Chief Information Officer (CIO) outlining a standard for federal authentication and identity management systems. On August 27, 2004, the president issued his twelfth Homeland Security Presidential Directive (HSPD-12), which was entitled, *Policy for Common Identification Standard for Federal Employees and Contractors*. HSPD-12 presented several objectives for requiring a uniform identity management process, and it established the timeframe for implementation of the new IDMS standard. Additionally, HSPD-12 granted the National Institute of Standards and Technology (NIST), acting under the authority of the Department of Commerce, the power to create Federal Information Processing Standard 201 (FIPS 201), which is the mandatory IDMS standard for all federal departments and agencies.

2. What is HSPD-12?

   HSPD-12 is the presidential directive that ordered federal agencies to implement a mandatory common identity management system for their employees and contractors. The directive has four primary goals:
   A. Enhance security
   B. Increase government efficiency
   C. Reduce identity fraud
   D. Protect personal privacy

   The directive specifically required that the agencies issue "secure and reliable forms of identification," which means that identification:
   A. is issued based on sound criteria for verifying an individual employee's identity
   B. is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
   C. can be rapidly authenticated electronically; and
   D. is issued only by providers whose reliability has been established by an official accreditation process

   HSPD-12 specifically delegated the power to promulgate a standard for uniform federal identity management systems to the Secretary of Commerce, who directs NIST. Additionally, the promulgation of the standard required consultation with

the Secretary of State, the Director of the OMB, the Attorney General, the Secretary of Homeland Security, and the Director of the Office of Science and Technology Policy.

3. What is FIPS 201?

FIPS 201 is a mandatory Federal Information Processing Standard. NIST composed FIPS 201 as directed by the Secretary of Commerce who was empowered by HSPD-12. The purpose of FIPS 201 was to create a federal standard for identity management systems, which will authenticate federal employees and contractors for physical access to federal facilities and for logical access to federal systems.

4. To whom does FIPS 201 apply?

FIPS 201 applies to all employees and contractors of federal departments and agencies requiring physical access to federal facilities and logical access to federal systems, except logical and physical access to national security systems as defined in 44 USC 3542(b)(2), which is part of the Federal Information Security Management Act (FISMA).

FISMA defines "national security system" as:

Any information system (including telecommunication system) used by an agency or contractor, or any other organization on behalf of any agency which:

A. the function, operation, or use:
   i. involves intelligence activities
   ii. involves cryptologic activities related to national security
   iii. involves command or control of military forces
   iv. involves equipment that is an integral part of a weapon or weapons system; or
   v. is a routine administrative system (see C below), and it is critical to the direct fulfillment of military or intelligence missions
B. or is protected at all times by procedures established for information that have been specifically authorized by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
C. This does not include a system that is used for routine administrative and business applications, including payroll, finance, logistics, and personal management applications.

For additional information in determining whether a system qualifies as a national security system, see NIST SP 800-59, entitled *Guideline for Identifying an Information System as a National Security System*.

5. Are there any waivers to the requirements of FIPS 201?

   No, there are no waivers to FIPS 201. All federal departments and agencies are required to comply with FIPS 201. The only exception to FIPS 201 is logical and physical access to national security systems as defined by FISMA.

6. What are the deadlines for program creation and implementation?

   FIPS 201 requirements were phased in based on the original date of HSPD-12, which was August 27, 2004:

   - 6 months after issuance of HSPD-12 (Feb 27, 2005) – Secretary of Commerce shall promulgate the standard
   - 4 months after promulgation of the standard (June 27, 2005) – Departments and agencies shall have a program in place for meeting the standard for identification issuance
   - 6 months after promulgation of the standard (August 27, 2005) – Departments and agencies shall identify relevant facilities and other unnamed applications to be covered by the standard to the Assistant to President for Homeland Security
   - 7 months after promulgation of the standard (September 27, 2005) – Assistant for Homeland Security and the Director of OMB shall make recommendations to the president about use for applications not originally listed
   - 8 months after promulgation of the standard (October 27, 2005) – Departments and agencies must have implemented and must be using the standard for access control

General Personal Identity Verification Information:

7. What is PIV?

   PIV is the abbreviation for Personal Identity Verification.

8. What is the difference between authentication and authorization?

   Authentication is the process of confirming a person's identity based on the reliability of the person's credential. In contrast, authorization deals with identifying a user's permissions.

9. What is a credential?

A credential is an object that is verified when presented to the verifier in an authentication transaction.

10. What is a smart card and how does it work?

A smart card is a credit card-sized device that contains an integrated circuit chip (ICC), which acts as a microprocessor that can manipulate data stored on the ICC. A smart card may also contain additional machine-readable technologies, such a magnetic stripe, bar code, contactless radio frequency transmitters (RFID), biometric data, encryption, or a photograph. The data on a smart card is accessed through the use of a smart card reader, which may require the use of a Personal Identification Number (PIN) to access the data stored on the card. FIPS 201 requires the use of smart cards, called PIV cards, for authentication of federal employees and contactors for access to federal facilities and systems.

11. What is a biometric?

A biometric is a measurable, physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an applicant. Facial images, fingerprints, and iris scans are examples of biometrics.

FIPS 201 Basics:

12. What is PIV-1

PIV-1 is the first part of the FIPS 201 standard. PIV-1 addresses the fundamental control and security objectives, such as identity proofing and registration requirements. In contrast, PIV-2 deals with the interoperability of PIV credentials and systems.

13. What is PIV-2?

PIV-2 is the second part of the FIPS 201 standard. It addresses the technical aspects of FIPS 201, such as interoperability and smart card components.

14. Does FIPS 201 modify any existing law?

No, FIPS 201 does not modify any existing law. FIPS 201 was created under the authority of HSPD-12, which was not intended to modify or nullify current laws.

15. How do other NIST publications affect implementation of FIPS 201?

NIST has published several related Special Publications that are referenced by FIPS 201. Special Publications provide guidelines for federal agencies on how to handle certain aspects of information security, and most were authorized pursuant to FISMA. Special Publications are recommendations and are not mandatory.

FIPS 201 references the following Special Publications:

- SP 800-37 – Guide for Security Certification and Accreditation of Federal Information Systems
- SP 800-53 – Recommended Security Controls for Federal Information Systems
- SP 800-63 – Electronic Authentication Guide
- SP 800-73 – Interfaces for PIV
- SP 800-76 – Biometric Data Specification for PIV
- SP 800-78 – Recommendation for Cryptographic Algorithms and Key Sizes

Additionally, FIPS 201 makes reference to FIPS 140-2 Security Requirements for Cryptographic Modules, which is mandatory for the use of cryptography within federal departments and agencies.

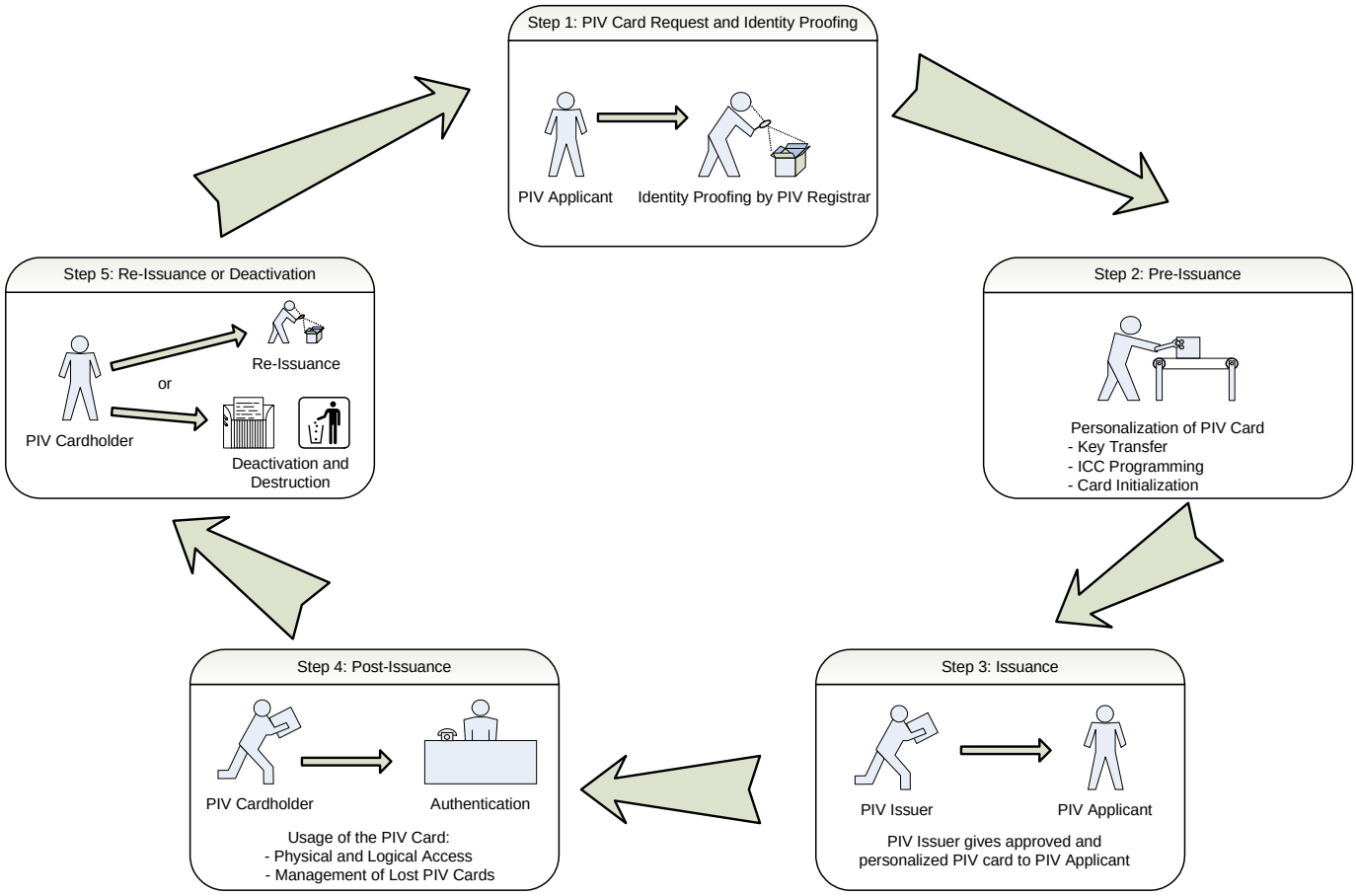
16. May an agency do more than what is required by FIPS 201?

Yes, FIPS 201 sets the minimum standard for federal identity management. Agencies and departments may add additional requirements to their identity proofing process, alter the physical appearance of the PIV card, or add additional data to the smart card, as long as the added requirements and data are not contrary to and do not interfere with the goals of FIPS 201. Moreover, alterations to the appearance of the PIV card must follow the strict card topology requirements. For example, an agency may require a more stringent background check, or an agency may require another asymmetric key be stored on the PIV card.

PIV Card Lifecycle:

17. What is the PIV card lifecycle?

The PIV lifecycle describes the stages of a PIV card from initiation of identity proofing to destruction of the PIV card. The general lifecycle is illustrated below.



18. What are the basic requirements for identity proofing?

Identity proofing is the verification of a person's identity for the issuance of credentials. Identity proofing pursuant to FIPS 201 requires the following:

- The use of an approved identity and proofing and registration process
- The completion of a National Agency Check with Inquiries (NACI) or a national security investigation.
- The applicant's physical appearance before a PIV official
- The applicant's presentation of two forms identification deemed acceptable on the I-9 Employment Eligibility form.
- The separation of roles during the proofing process such that no single person has the power to issue a PIV credential.

19. What is an "approved" PIV proofing, registration, and issuance process?

Federal departments and agencies must use an approved identity proofing, registration, and issuance process. An identity proofing and registration process is considered approved if it conforms to the criteria presented in Appendix A of

FIPS 201 and meets the overall PIV objectives and requirements. Appendix A describes two methods for identity proofing and registration based upon whether an agency has an existing identity management system in place. Agencies that do not have an existing identity management system and use a generic process for issuing credentials should use the role-based model. Agencies that already employ an automated identity management system should follow the system-based model. Alternatively, federal agencies and departments may use a different identity proofing and registration process if it is accredited by the agency's Office of the Inspector General as satisfying the PIV objectives and requirements, and the process is approved in writing by the head of the agency or department.

Appendix A of FIPS 201 provides the minimal level of proofing necessary to issue a PIV credential to a new or current employee or contractor. Agencies may expand this process to meet their organizational needs.

20. What is the role-based model?

The role-based model is intended for agencies that do not currently have a pre-existing PIV system. The role-based model assigns PIV identity-proofing and other responsibilities to individuals and entities based upon the role they perform. The role-based model provides for the separation of function to prevent collusion between an applicant and a credential issuer.

The following roles are involved with the identity proofing and registration process in the role-based model:

- Applicant – The individual to whom the PIV credential needs to be issued.
- PIV Sponsor – The individual who substantiates the need for a PIV credential to be issued to the applicant.
- PIV Registrar – The entity responsible for identity proofing of the applicant and ensuring the successful completion of background checks. The entity provides final approval for issuance of the PIV credential to the applicant.
- PIV Issuer – The entity that personalizes the credential for the applicant and issues the credential to the applicant. The entity is responsible for maintaining records and controls.
- PIV Digest Signatory – The entity that digitally signs the PIV biometrics and cardholder unique identifier (CHUID).
- PIV Authentication Certification Authority (CA) – The CA signs and issues the PIV Authentication Certificate.

The roles of PIV applicant, sponsor, registrar, and issuer are mutually exclusive and cannot be performed by the same person. Entities performing the roles of PIV registrar, PIV issuer, or PIV digital signatory must meet the requirements of an official accreditation process (see NIST SP 800-37).

21. How does the role-based model work for new employees and contractors?

The role-based model employs the following steps:

A. The PIV sponsor must complete a PIV request for an applicant and submit the request to the PIV registrar and PIV issuer. The request shall include:
   - ✓ Name, organization, and contact information for the PIV sponsor
   - ✓ Name, date of birth, position, and contact information of applicant
   - ✓ Name and contact information of designated PIV registrar
   - ✓ Name and contact information of designated PIV issuer
   - ✓ Signature of PIV sponsor

B. The PIV registrar shall confirm the validity of the PIV request prior to acceptance.

C. The applicant shall complete Standard Form (SF) 85, *OPM Questionnaire for Non-Sensitive Positions*, or the equivalent. The applicant shall submit the form to the PIV registrar.

D. The applicant shall appear in person and provide two forms of identification to the PIV registrar. The identification must meet the requirements of Form I-9, Employment Eligibility Verification. One form of identification must be valid state or federal government-issued picture identification. The PIV registrar shall inspect the documents, determine whether the documents are authentic and unaltered, and compare the picture on the identification with the applicant. If the identification check is successful, then the PIV registrar shall record the following information and sign the record:
   - ✓ Document title
   - ✓ Document issuing authority
   - ✓ Document number
   - ✓ Document expiration date
   - ✓ Any other information used to confirm the identity of the applicant

E. The PIV registrar shall compare the applicant's information from the PIV request with the corresponding information provided by the applicant.

F. The PIV registrar shall capture the facial image of the applicant.

G. The PIV registrar shall fingerprint the applicant.

H. The PIV registrar shall initiate the NACI.

I. When all of these steps are completed, the PIV registrar shall notify the PIV sponsor and PIV issuer that the applicant has been approved or disapproved for issuance of a PIV credential.

J. If the applicant has been approved, then the Registrar shall make available through a secure process to the PIV issuer the following information:
   - ✓ Applicant's facial image
   - ✓ Copy of results of applicant's background investigation
   - ✓ Other data associated with the applicant

K. If the applicant has been approved, then the Registrar shall make available through a secure process to the PIV Digital Signatory the following information:
   - ✓ Electronic biometric data for card personalization
   - ✓ Other data associated with the applicant that is required for the generation of signed objects for card personalization

L. The PIV registrar is responsible for maintaining the following:
   - ✓ Completed and signed PIV request
   - ✓ Completed and signed SF 85
   - ✓ Information related to identification documents
   - ✓ Results of required background check
   - ✓ Any other materials used to prove the identity of the applicant

22. How does the role-based model work for current employees and contractors?

The identity verification and proofing process described for new employees and contractors shall be followed except that background checks are not required if the results of a previous background check can be verified by the PIV registrar.

23. How does PIV card issuance work for the role-based model?

Federal departments and agencies must meet the following functional security requirements. However, departments and agencies may enhance the process to meet additional agency needs.

- ✓ The PIV issuer shall confirm the validity of the PIV request from the sponsor and the approval notification from the PIV registrar. The PIV issuer shall also confirm that the approval notification matches the results of the background investigation.
- ✓ The PIV issuer shall control the creation and personalization of the credential.

- ✓ The PIV issuer shall initiate the creation of the CHUID for the new PIV credential. The CHUID shall be made available through a secure means to the PIV digital signatory.
- ✓ The PIV digital signatory shall create digitally signed credential elements needed for the card personalization process. The digitally signed credentials shall be made available to the PIV issuer.
- ✓ The applicant shall appear in person to the PIV issuer to collect the PIV credential. The PIV issuer shall verify the credential matches the identity of the individual through the following steps:
  - o The individual shall present a state or federally-issued picture identification document.
  - o The PIV issuer shall compare the identification document to the PIV credential.
  - o The PIV issuer shall check that the fingerprint of the individual matches the biometric credential stored on the PIV card.
  - o The individual may be asked to provide a PIN, or the PIV issuer may generate a PIN on the individual's behalf
  - o The PIV issuer shall personalize the PIV card.
  - o The individual may generate cryptographic keys for the PIV card and obtain the corresponding certificates from the CA at this time. Alternatively, the individual may be supplied a one-time authenticator for use in a subsequent certificate request.
  - o The recipient's name, issuer identity, card number, and possibly Public Key Infrastructure (PKI) certificate identification information shall be enrolled and registered in a backend data store.
  - o The PIV issuer shall obtain a signature from the individual attesting to the individual's acceptance of the PIV credential and related responsibilities.
  - o The PIV issuer shall notify the PIV sponsor and PIV registrar of the outcome of the issuance process.
- ✓ The PIV issuer shall be responsible for maintenance of the following:
  - o The completed and formally authorized PIV request
  - o The approval notice from the PIV registrar
  - o The name of the PIV credential holder
  - o The credential identifier
  - o The expiration of the PIV credential
  - o The signed acceptance form from the PIV credential holder

24. What is the systems-based model?

The system-based model is intended for agencies that already have an automated IDMS. The system-based model also provides for the separation of functions to prevent collusion in obtaining a credential.

The roles and responsibilities for the system-based model are defined as follows:

- Applicant – The individual to whom the PIV credential needs to be issued. This individual shall provide supporting documentation to prove the individual's claimed identity. Additionally, this person must appear in person at least once during the identity proofing process.
- Employer/Sponsor – The individual who substantiates the relationship to the applicant, provides sponsorship, and authorizes the request for a PIV credential. This individual must be pre-registered in the IDMS.
- Enrollment Official – The individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind the applicant to their biometric, and validate the identity-source documentation. The Enrollment Official delivers the secured enrollment package to the IDMS for adjudication.
- Approval Authority – The entity that establishes the organizational chain of command with in the IDMS for PIV application approvals, which include:
    - Establishing approved Employer/Sponsors
    - May designate automated or manual approval processes for completed PIV applications
    - Shall manage the total scope of the chain of trust established in functional process
    - Shall manage the appropriate privacy and security controls
- Issuing Authority (Issuer) – The entity that issues the PIV credential to the applicant after completion of identity proofing and approval of the application. The issuer issues the credential by:
    - Completing the chain of trust by performing a 1:1 biometric check of the applicant against the PIV enrollment record
    - Activating the card
    - Releasing the credential to the applicant

The approval authority must provide for the separation of duties so that at least two persons perform different functions within the chain of trust process.

The components associated with PIV identity proofing and credential issuance are:

- Identity Management System (IDMS) – The IDMS is a system of records maintained by the approval authority. It establishes the validity of a claimed identity through performance of the following processes:
    - Shall perform 1:many search to ensure applicant has not enrolled under a different name
    - Shall confirm employment appropriate to the PIV request
    - Shall manage identity validation and verification services through government-wide standardized services
    - Shall manage adjudication of identity claim
    - Shall approve issuance of PIV to applicant upon successful adjudication
- Enrollment System – The enrollment system initiates the chain of trust for identity proofing. Enrollment shall be provided trusted services to confirm

employee sponsorship, bind the applicants to their biometric data, and validate identity claim documentation. Enrollment delivers a secured enrollment package to the IDMS for adjudication.

- Card Production and Personalization- It shall provide inventory and personalization/printing functions for the card stock. It shall provide mechanisms to track status, control inventory, and protect blank card stock and personalized card stock prior to activation.
- The system must also be capable of creating an auditable trail.

25. How does the system-based model work?

A. PIV application process components:
   - ✓ Applicant PIV request and identity documentation
   - ✓ Employer/Sponsor approval of applicant request
   - ✓ Approval authority confirms and approves PIV application, appropriate sponsorship
   - ✓ Approval authority approves PIV request

B. PIV enrollment process steps:
   - ✓ Applicant shall appear for enrollment with supporting documentation
   - ✓ Enrollment shall inspect and confirm supporting documentation, preferably in automated manner
   - ✓ Enrollment shall establish the individual present matches the supporting documents
   - ✓ Enrollment shall conform employer/sponsor approval for PIV
   - ✓ Enrollment shall scan all supporting documents
   - ✓ Enrollment shall take biometric samples and a photograph of the applicant
   - ✓ Enrollment shall manage the quality assurance of the biometric and photographic capture of the applicant
   - ✓ Enrollment shall bind the completed electronic package with a digital signature and forward the package to the IDMS for verification and validation
     - o The complete electronic package shall include:
       - ▪ Scanned documents that support the identity claim
       - ▪ Biometric samples and digital photograph
       - ▪ Personal biographical and organizational information
       - ▪ Digital signature of enrollment official

C. Identification verification process:
   - ✓ The IDMS shall receive the completed enrollment package and verify the integrity of the package by confirming completeness, accuracy, and the digital signature
   - ✓ The IDMS shall provide a means to confirm employment and sponsorship as identified in the package

- ✓ The IDMS shall perform a 1:many search to ensure that the individual identified in the package has not applied previously under a different name
- ✓ The IDMS shall conduct appropriate verification and validation using government-wide databases and services
- ✓ The approval authority shall provide adjudication of the identity claim should any of these core checks identify a potential risk
- ✓ After successful completion of the identity verification process, the approval authority shall approve the credential. If the identity verification exceeds ten days, then the approval authority may approve the credential without successful completion.

D. Card production services:
- ✓ Card production may be performed centrally or in a distributed location, and it shall:
  - Maintain full inventory of card stock, consumables, and manufacturing materials
  - Maintain a list of approved IDMS that can submit requests for PIV card production
  - Provide acknowledgement of IDMS request to produce a PIV card
  - Notify IDMS upon completion of PIV card
  - Maintain a list of approved issuers that can activate and issue PIV cards
  - Only send information regarding production of PIV credentials to approved authorities
  - Only send fully completed and personalized PIV credentials to approved issuing agents
  - Document, implement, and maintain a card production, activation, and issuance security policy

E. Suspension, revocation, and destruction
- ✓ A card registry for all PIV cards issued shall be established and maintained to keep track of the status of all PIV cards, such as whether a PIV card is valid or revoked

F. Re-issuance to current PIV credential holders
- ✓ The issuing authority shall:
  - Ensure the IDMS record for the individual states that the credential is not expired
  - Verify the individual with a 1:1 biometric match against the IDMS record
  - Verify individual against the photograph in the IDMS record
  - Recapture biometrics
  - Issue a new credential and update the IDMS record

- ✓ The issuing authority shall digitally sign the recaptured biometrics and new credential record

26. Who is required to have a background check? What about current employees?

All employees and contractors are required to have a background check in the form of a National Agency Check (NAC) or National Agency Check with Inquiries (NACI), which are performed by the Office of Personnel Management (OPM). Some positions may also require a national security community investigation. However, current employees are not required to have a background check if their most recent background check is on file and can be verified by a PIV official.

These requirements also apply to citizens of foreign countries who are working for the federal government, except those working for a military commander. The registration process for foreign employees must also be approved by the Department of State's Bureau of Diplomatic Security.

27. How long is a PIV card valid?

A PIV card shall be valid for no more than five years.

28. What happens to the PIV card if someone quits or is terminated?

A termination procedure shall be maintained for situations where an employee quits, is terminated, no longer needs access (contractual change), or dies.

The termination procedure shall include the following steps:

- ✓ The PIV card is collected and destroyed.
- ✓ The PIV card itself is revoked. The associated FASC-N (Federal Agency Smart Credential Number) stored in a local database shall be updated to reflect this change in status.
- ✓ The CA shall be informed and the certificate corresponding to the PIV authentication key shall be revoked.
- ✓ Online Certificate Status Protocol (OCSP) responders shall be updated.
- ✓ The information in identifiable form (IIF) that has been collected from the cardholder is disposed of in accordance with departmentally-established procedures.

29. What happens if a PIV card is lost or stolen?

The department shall have a reporting mechanism in place. The cardholder shall immediately report the loss and apply for re-issuance. The termination procedure must be followed within eighteen hours of the report.

Technical Details:

30. What information is stored on the PIV card?

The PIV card stores the following items:

A. A Personal Identification Number (PIN), which is used to prove the identity of the cardholder to the card.
B. A Cardholder Unique Identifier (CHUID), which is used by the card to prove the identity of the cardholder to an external entity, such as a contactless card reader.
C. PIV Authentication Data (one asymmetric key and corresponding certificate), which is used by the card to prove the identity of the cardholder to an external entity, such as a network.
D. Two Biometric Fingerprints, which are used to prove the identity of the cardholder to an external entity, such as a contact card reader for physical access.

31. What is activation and how is information on the PIV card accessed?

The PIV card must be activated in one of two ways for the data on the PIV card to be accessible. Activation is required to access biometric data and asymmetric keys. First, the PIV card can be activated directly by the cardholder when the cardholder enters a PIN into the card reader. Second, the PIV card can be activated by the card management system during card personalization and for updates.

The CHUID and the biometric data must be digitally signed to protect the authenticity and the integrity of the stored data.

Note that the CHUID is accessible without activation, and it is accessible to a contactless RFID reader.

32. Can someone fake a PIV card or tamper with its data?

The PIV card was designed to prevent counterfeiting and tampering. All PIV cards must incorporate the following security features:

- ✓ Optical varying structures
- ✓ Optical varying links

- ✓ Laser etching and engraving
- ✓ Holograms
- ✓ Holographic images
- ✓ Watermarks

Moreover, departments and agencies may incorporate additional methods to prevent tampering and counterfeiting attempts.

33. How is the CHUID created?

The CHUID is based on the FASC-N. The FASC-N is assigned by each agency. The CHUID also contains the expiration date of the credential.

34. May an agency alter the appearance of a PIV card?

Yes, an agency may alter certain physical aspects of a PIV card (see FIPS 201 for an illustration of the card zones).

The following items may be added to the front of the PIV card:

- In Zone 3, an agency may add a signature line.
- In Zone 4, an agency may add an agency specific piece of information, such as employee status.
- In Zone 5, an agency may add a cardholder's rank within the agency.
- In Zone 6, an agency may add a portable data file two-dimensional bar code (PDF). If a PDF is used, then the signature line may be affected.
- In Zone 9, an agency may add a header, such as "United States Government" or "Federal Emergency Responder."
- In Zone 11, an agency may add its agency seal.
- In Zone 12, an agency may add footer information that it deems relevant, such as "Firefighter."
- In Zone 13, an agency may the issuance date of the PIV card.
- In Zone 15, an agency may add color-coding for additional identification. Note that the colors blue, green, and red are reserved and cannot be used.
- In Zone 16, an agency may use a photo border to further identify a cardholder.
- In Zone 17, an agency may use this area for additional agency-specific data, if other defined optional areas are not used.

The following items may be added to the back of the PIV card:

- In Zone 3, a magnetic stripe may be added if it is of high coercivity and conforms to ISO 7811.
- In Zone 4, an agency may add information about returning the PIV card if lost.

- In Zone 5, an agency may print the physical characteristics of the cardholder.
- In Zone 6, an agency may add more descriptive information about an emergency responder, such as authorized access.
- In Zone 7, an agency may add warning language against counterfeiting, fraud, or misusing the PIV card.
- In Zone 8, an agency may add information to linear 3 of 9 bar code.
- In Zone 9, an agency may use this area for additional agency-specific data, if other defined optional areas are not used.
- In Zone 10, an agency may use this area for additional agency-specific data, if other defined optional areas are not used.

The following data may be added to the logical data stored on the chip:

- An agency may add an asymmetric key pair and corresponding key certificate for digital signatures.
- An agency may add an asymmetric key pair and corresponding key certificate for key management
- An agency may add symmetric or asymmetric card authentication keys for supporting additional physical access applications
- An agency may add symmetric keys associated with the card management system.

35. Does FIPS 201 require the use of cryptography?

Yes, cryptography is used for strong authentication in FIPS 201. The PIV card contains one asymmetric key that is used for authentication. The authentication key cannot be exported from the PIV card, and the card contains all functions necessary to perform operations using the key directly on the PIV card. NIST SP 800-78, entitled *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, provides technical guidelines for cryptographic algorithms and key sizes that should be used for FIPS 201.

FIPS 201 also provides for the optional use of additional cryptographic keys for digital signatures, key management, and card management. All of these keys can only be accessed using the contact interface of the PIV card. NIST SP 800-78 may also be consulted for guidance in using these optional keys.

36. What is an x.509 certificate?

An x.509 certificate is a digitally signed statement from a trusted entity that verifies that a public key is associated with a purported entity. X.509 refers to a particular standard for certificates, which requires that specific information is included using a particular format. FIPS 201 requires the PIV card to store an x.509 certificate to verify the authenticity of the PIV card's corresponding public

key. The certificate must be signed by a CA that participates in the hierarchical PKI for the Common Policy (see http://www.cio.gov/ficc/cpl.htm for a list of participating CAs).

37. What are the PIV card authentication mechanisms?

The PIV card contains several authentication mechanisms, which are described in the following table:

Type	How does it work?	When is it used?	Special Notes
Visual Authentication	A human guard visually inspects the PIV card for validity, matches the picture with the cardholder, and checks the expiration date. Optionally, the guard may ask for the cardholder's signature to compare to the signature on the PIV card.	It should be used for areas that do not have a card reader.	It is not recommended for high traffic areas.
CHUID Authentication	A contact or contactless reader reads the CHUID, checks the digital signature of the CHUID, and checks the expiration date of the PIV card to grant access to an area.	It should be used for high traffic areas that have a card reader and do not require a high level of assurance.	Non-cardholders cannot be detected because CHUID can be read without cardholder activation. Also, altered cards cannot be detected because there is no human inspection of the PIV card.

Biometric Authentication	The CHUID is read from the PIV card by a contact reader that checks the expiration date. The cardholder must then enter her PIN number into the reader to activate the card. The biometric is read, and the cardholder is prompted to submit a live biometric sample. The cardholder authenticated and granted access if the stored biometric matches the live biometric.	It should be used for low traffic areas that require strong two-factor authentication.	This process may be supervised or unsupervised by an attendant. The digital signature associated with the stored biometric may also be verified.
PKI Authentication	The CHUID is read from the PIV card by a contact reader that checks the expiration date. The cardholder must then enter her PIN number into the reader to activate the card. The reader issues a challenge and requests an asymmetric operation. The card responds to the challenge and signs it using the PIV authentication key. The response is verified through the PKI. The cardholder is granted access.	It should be used for access to systems and facilities where a very high level of confidence is required. It is best for low traffic areas.	It requires access to an online certificate status checking infrastructure. It requires contact-based readers.

E-Authentication:

38. What is E-authentication?

E-Authentication was first addressed in the OMB's publication 04-04, entitled *E-Authentication Guidance for Federal Agencies.* The OMB defined E-authentication as the process of establishing confidence in user identities that are electronically presented to an information system. OMB 04-04 is mandatory for all federal transactions that require authentication. NIST SP 800-63 supplements OMB 04-04 by providing implementation details and technical requirements for the four levels of assurance defined in the OMB publication. The four levels of assurance describe the degree of certainty that a user has presented a credential which actually refers to the user's identity. OMB issued criteria for determining the level of authentication assurance required for specific systems based on risks and likelihood of the risks occurring.

According to OMB 04-04, agencies should determine assurance levels using the following steps:

A. Conduct a risk assessment of the e-government system
B. Map identified risks to the applicable assurance level
C. Select technology based on e-authentication technical guidance
D. Validate that the implemented system has achieved the required assurance level
E. Periodically reassess the system to determine technology refresh requirements

NIST published a standard for the security categorization of information systems referred to as FIPS 199, which is mandatory for all federal systems, except national security systems and systems dealing with classified information. Additionally, NIST SP 800-60, entitled *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides further guidance for mapping security risks in federal systems.

39. What are the four levels of assurance and how does that apply to FIPS 201?

The levels of assurance establish the level of confidence in an issued credential. The parameters that define confidence are:

- The thoroughness of the identity proofing process implemented by the agencies
- The security of the PIV card issuance and maintenance process implemented by the agencies
- The technical authentication mechanisms, which are used to verify that the PIV cardholder is the rightful owner of that PIV card

Note that FIPS 201 only uses levels two through four because the goal of HSPD-12 is to ensure a basic level of identity assurance for every PIV cardholder.

The levels of authentication based on the criteria of OMB 04-04 and SP 800-63 are described in the table below.

Levels	Description Based on SP 800-63 & OMB 04-04
Level 1	There is no identity proofing requirement. Names are assumed to be pseudonyms. Authentication generally involves password plus a challenge. Common protocols are APOP, S/KEY, and Kerberos. Remote registration is permitted. *This level is not used for FIPS 201.*
Level 2	Identity proofing requires the presentation of identifying materials. Level 2 provides single-factor authentication. Names must be specified as a pseudonym or verified name. Authentication requires proof of token ownership, and the use cryptographic protocols are required. A common protocol is secure TLS.
Level 3	Identity proofing requires identifying materials and verification of identity materials. Level 3 provides multi-factor authentication. Only verified names are allowed. Authentication requires proof of possession of a cryptographic key using a cryptographic protocol and another factor, such as a password or biometric. Common protocols are the use of soft tokens (TLS with client certificates), hard tokens (physical token), or one-time password device tokens.
Level 4	Level 4 has the same identity proofing requirements of Level 3, but has the additional requirement for the use of "hard" cryptographic tokens. Authentication is based on proof of possession of key through a cryptographic protocol. Level 4 also provides multi-factor authentication. Only verified names are allowed. Authentication requires proof of possession of a cryptographic key using a cryptographic protocol, and another factor, such as a password or biometric. The token must be a hard token.

The OMB levels of authentication correspond to the levels used in FIPS 201.

OMB Level	Description of OMB Level	Comparable FIPS 201 PIV Level
Level 1	Little or no confidence in the asserted identity's validity	Does not exist
Level 2	Some confidence in the asserted identity's validity	Level 2 - SOME confidence
Level 3	High confidence in the asserted identity's validity	Level 3 - HIGH confidence
Level 4	Very high confidence in the asserted identity's validity	Level 4 - VERY HIGH confidence

40. How does the PIV card support graduated assurance levels for authentication?

The PIV card supports graduated levels of assurance by mapping the level of assurance to a particular authentication type for both logical and physical access.

Physical Access:

Required PIV Assurance Level	Description of Level	Applicable Authentication Type
Level 2	SOME confidence	Visual or CHUID
Level 3	HIGH confidence	Biometric
Level 4	VERY HIGH confidence	Attended Biometric or PKI

Logical Access:

Required PIV Assurance Level	Description of Level	Applicable Authentication Type	
		Local Workstation	Remote/Network
Level 2	SOME confidence	CHUID	PKI
Level 3	HIGH confidence	Biometric	
Level 4	VERY HIGH confidence	Attended Biometric or PKI	

Privacy Requirements:

41. Does FIPS 201 have any privacy requirements?

Yes, the design of the IDMS standard in FIPS 201 is the result of HSPD-12, which specifically lists protecting personal privacy as one of the president's goals. Since agencies may have a wide variety of uses for the PIV card, the agencies must consider the impact on personal privacy when determining appropriate uses for the PIV card. Moreover, FIPS 201 also requires the following privacy-enhancing actions:

- Assign an individual the role of senior official for privacy. This person must implement the privacy requirements for the PIV system. Also, this person may not perform any other role in the PIV system.
- Write, publish, and maintain a comprehensive document listing the following:
    - The types of information that will be collected
    - The purpose of the collection
    - What information will be disclosed to whom during the life of the credential
    - How the information will be protected
    - The complete set of uses for the credential
- Provide full disclosure to the applicant of the comprehensive listing above, as well as any related privacy implications
- Completely comply with the fair information practices set forth in the Privacy Act of 1974

- Maintain an appeals procedure for denied or revoked credentials
- Ensure that only personnel with legitimate needs have access to the PIV system and its data
- Coordinate with the appropriate department or agency official to describe the consequences for violating the privacy policies of the PIV system
- Assure that technologies used to implement the PIV system allow for continuous auditing of the stated privacy polices and applicable laws
- Utilize the security controls described in SP 800-53
- Ensure that the technologies used to implement PIV do not erode privacy protections
- Employ an electromagnetically opaque sleeve to protect against unauthorized contactless access to the CHUID on the PIV card

42. Do other federal privacy laws apply to the PIV system?

As stated in FIPS 201, all agencies must comply with all relevant federal privacy laws, including but not limited to:

A. The Privacy Act of 1974

The Privacy Act of 1974 applies to FIPS 201 because the act of authenticating entails retrieving a record based on a unique identifier in a system of records. The Privacy Act requires data to be protected from unauthorized disclosure and modification. Additionally, the Privacy Act requires that users have access to their data, and they can request to have inaccurate data amended. Finally, the Privacy Act requires that the data may only be shared with other agencies in accordance with Privacy Act requirements, which requires a written agreement between the two agencies.

The Privacy Act also set forth the Fair Information Practices, which are mandatory for the PIV system. Each Agency shall:

- Only maintain in its records individual information that is relevant and necessary to accomplish its purpose as defined by statute or executive order
- Collect information to the greatest extent possible directly from the individual when the information may result in adverse determinations about an individual's rights, privileges, or benefits under federal programs
- Inform each individual on the form used to collect the information of the following information:
    - The authority which authorizes the solicitation of information
    - The principal purposes for which the information will be used
    - The routine uses of the information

- Provide notice of the system of records in the Federal Register
- Maintain all records with such accuracy, relevance, timeliness, and completeness as is reasonable necessary to assure fairness to the individual
- Ensure the relevance, timeliness, accuracy, and completeness of any record before it is disseminated to another agency
- Provide reasonable notice to an individual when any record is made available under compulsory legal process
- Establish rules of conduct for persons involved in the design, development, or maintenance of systems of records
- Provide administrative, technical, and physical safeguards to ensure the confidentiality and security of the records
- Provide notice in the Federal Register of any new uses of the information at least 30 days prior to the new use
- Provide notice in the Federal Register of any data-matching program for the information at least 30 days prior to matching
- Establish a procedure so that the individual has access to information collected about that individual
- Establish a procedure for allowing an individual to make amendments to information about that individual

B. The E-Government Act of 2002

Section 208 of the E-Government Act of 2002 provides additional privacy requirements if certain criteria are met:

- Section 208 applies to the development or procurement of information technology that collects, maintains, or disseminates information in an identifiable form, or
- The initiation of a collection of information that will be collected, maintained, or disseminated using information technology, and
- Section 8 includes IIF that permits physical or online contact of a specific individual, if identical questions have been posed to or identical reporting requirements imposed on ten or more persons other than government employees.
- If the criteria are met, the agency shall:
    - Conduct a privacy impact assessment (PIA)
    - Ensure review of the PIA by the CIO, and
    - Make the PIA publicly available unless the PIA contains classified, sensitive, or private information.
- The PIA must be sent to the Director for each system for which funding is requested.
- The PIA must take into account the size of the information system, the sensitivity of the identifiable information in the system, and the risk of harm from unauthorized release.
- The PIA shall address:

- What information is to be collected
- Why the information is to be collected
- The agency's intended use of the information
- With whom the information will be shared
- What notices or opportunities for consent will be provided
- How the information will be shared
- How the information will be secured, and
- Whether a system of records is being created under The Privacy Act of 1974, Section 552a.

C. OMB Memorandum 03-22

OMB 03-22 provides additional guidance to federal agencies in implementing the privacy requirements of the E-Government Act and other federal privacy laws. OMB 03-22 does not provide additional requirements for agencies, but it does provide substantial detail to assist agencies in complying with the relevant federal privacy laws.

Oversight and Review:

43. How will agencies be monitored for compliance?

Oversight will be the responsibility of each agency's Inspector General, the Office of Management and Budget, the Government Accountability Office, and oversight committees of Congress. The consequences of noncompliance may include a variety of sanctions, such as negative audit reports and budgetary impacts.

44. How will conformance testing be performed?

Funding permitting, NIST plans to develop a PIV validation plan to test agency implementations for conformance with FIPS 201. Information will become available as it is completed. Please check: http://csrc.nist.gov/piv-project/conformance/.

45. Will NIST review the standard?

NIST will ask all agencies and departments for input in one year to determine if a full review of the standard is necessary. Otherwise, the standard will be reviewed in five years.

References and Additional Information:

- HSPD-12 – Homeland Security Presidential Directive 12

  HSPD-12 was the presidential directive that authorized the creation of FIPS 201. HSPD-12 aimed to increase security and efficiency at government facilities through the creation of a standard for federal identity management systems. HSPD-12 led to the development of the PIV card, which is a smart card that reduces the risk of unauthorized access to federal facilities and systems using strong multi-factor authentication.

- Federal Identity Management Handbook by GSA (Draft)

  The Federal Identity Management Handbook is a 150-page document created by the General Services Administration. It was intended to help federal agencies understand the requirements and implementation procedures for FIPS 201. The handbook is currently in draft form.

- FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems

  FIPS 199 was created pursuant to FISMA and provides a mandatory method of classifying federal information and information systems based on the impact to an agency's ability carryout its mission and daily functions. FIPS 201 organizes information into "information types," such as financial or medical, and assigns impact levels (high, moderate, or low) to its security objectives, which are confidentiality, integrity, and availability. The format for expressing a FIPS 199 categorization is as follows:

  $SC_{information\ type}$ = { (confidentiality, impact), (integrity, impact), (availability, impact) }

- FIPS 201 – Personal Identity Verification (PIV) of Federal Employees and Contractors

  FIPS 201 was created in response to HSPD-12 and sets forth the mandatory standard for federal identity management. It requires a uniform identity proofing procedure for federal employees and contractors, as well as the issuance and use of a smart card to authenticate the identity of federal employees and contractors for access to federal facilities and systems. The only exemption to FIPS 201 is physical and logical access to national security systems.

- FISMA – Federal Information Security Management Act of 2002

  FISMA is contained in Title III of the E-Government Act of 2002. The aim of FISMA was to provide a comprehensive framework for the management of federal information security, including the establishment of minimum level of controls to protect information systems, the improved oversight of agency information security programs, and the use of robust commercially developed information security products. Additionally, FISMA granted NIST the authority to develop information security guidelines to assist the agencies in conforming to the requirements of FISMA. The guidelines resulted in the development of the special publications 800 series, which is regularly referred to in FIPS 201.

- OMB 04-04 – E-Authentication Guidance for Federal Agencies

  OMB 04-04 was a memorandum sent to each federal CIO under the authority of Paperwork Reduction Act of 1998 (PRA) and in furtherance of Section 203 of the E-Government Act of 2002. It provided guidance to federal agencies in conducting e-authentication risk assessments to determine the correct authentication level for access to federal resources. OMB 04-04 set forth four levels of authentication based on the risks and potential for the risks to occur for each resource.

- SP 800-37 – Guide for Security Certification and Accreditation of Federal Information Systems

  SP 800-37 was created as authorized by FISMA to provide guidance about conducting a security certification assessment and about the process of accreditation for a system. The goal of SP 800-37 was to provide a method for consistent assessments of security controls, provide accountability for information security, and promote a better understanding of agency risk related to information security. SP 800-37 provides a method for conducting the certification assessment. After certification is completed, the senior agency official accredits the certification meaning that the individual is willing to accept the risks and takes responsibility for the security of the systems.

- SP 800-53 – Recommended Security Controls for Federal Information Systems

  SP 800-53 was authorized by FISMA and provides guidance to federal agencies in selecting and specifying security controls. SP 800-53

provides a procedure for implementing security controls based on nine steps, it begins with a FIPS 199 system categorization, and it concludes with monitoring the selected controls for efficacy. SP 800-53 includes a lengthy appendix that provides very specific technical guidance on possible controls for specific security policies.

- SP 800-59 – Guideline for Identifying an Information System as a National Security System

  SP 800-59 was created to help agencies determine whether a system is a national security system, as defined by 44 USC 3542(b)(2), and is therefore exempt from FIPS 201 requirements. SP 800-59 states the head of each agency is responsible for making the determination. SP 800-59 provides a helpful checklist in Appendix A to assist in making the determination.

- SP 800-63 – Electronic Authentication Guideline (Version 1.0.1)

  Based on the authority provided by FISMA, NIST drafted SP 800-53 to supplement the four levels of authentication created in OMB 04-04 with technical guidelines. SP 800-63 describes the recommended authentication type, such as two-factor authentication with passwords and biometrics, for each authentication level. Additionally, it describes the level of identity proofing necessary for each level of authentication.

- SP 800-73 – Interfaces for PIV (Second Draft)

  SP 800-73 specifies the interface requirements for retrieving and using the identity credentials stored on a PIV card. The specification ensures the interoperability requirement of the PIV card. It provides details for developing the PIV card and the card reader by presenting the applications programming interfaces (API), the data model, and the security architecture. SP 800-73 also provides helpful use-case diagrams to assist with implementation.

- SP 800-76 – Biometric Data Specification for PIV (Draft)

  SP 800-76 defines the technical specification for the biometric data stored on the PIV card. The specification ensures interoperability of the PIV card and improves the performance of the PIV card. SP 800-76 specifies how the biometrics should be captured and in what formats they should be stored.

- SP 800-78 – Recommendation for Cryptographic Algorithms and Key Sizes (Draft)

  SP 800-76 provides the technical specification for the cryptographic objects and methods used by the PIV card. The specification establishes guidelines for the algorithms and key sizes to be used for the PIV card. SP 800-76 also provides dates for when different algorithms or stronger keys should be used.

- The Privacy Act of 1974

  The Privacy Act was enacted in 1974, and it applies to all federal systems of records maintained by federal agencies that have the capability of retrieving the individual records with a unique identifier. The Privacy Act requires data to be protected from unauthorized disclosure and modification. It essentially codifies fair information practices for federal databases.

Glossary of Acronyms:

Acronym	Definition
API	Application Programming Interface
APOP	Authenticated Post Office Protocol
CA	Certificate Authority
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HSPD-12	Homeland Security Presidential Directive - 12
IDMS	Identity Management System
IIF	Information in Identifiable Form
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Control
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFID	Radio Frequency Identifier
S/KEY	One time password scheme
SF	Standard Form
SP	Special Publication
TLS	Transport Layer Security