Federal Information Processing Standard (FIPS) 201, Personal Identity Verification for Federal Employees and Contractors: Control Objectives

Donna F Dodson

donna.dodson@nist.gov

June 27, 2005

FIPS 201 REQUIREMENTS
Phased- Implementation In Two Parts

- Part 1 – Common Identification and Security Requirements
  HSPD 12 Control Objectives
  Identity Proofing, Registration and Issuance Requirements
  Privacy Requirements
  (Effective October 2005)

- Part 2 - Common Interoperability Requirements
  Detailed Technical Specifications
  No set deadline for implementation in PIV standard

Control Objectives

- **Secure and reliable forms of identification**
  - Issued based on sound criteria for verifying an individual employee's identity
  - Strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation
  - Can be rapidly authenticated electronically
  - Is issued only by providers whose reliability has been established by an official accreditation process

FIPS 201 REQUIREMENTS

- Credentials are issued to individuals whose true identity has been verified and after a proper authority has authorized issuance of the credential
- 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, as 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

FIPS 201 REQUIREMENTS (Cont)

- 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
- No credential is issued unless requested by proper authority
- A credential remains serviceable only up to its expiration date

FIPS 201 REQUIREMENTS (Cont)

- 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

PIV Identity Proofing and Registration Requirements

- Organization shall adopt and use an approved identity proofing and registration process.
- Process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment.
- National Agency Check (NAC) component of the NACI shall be completed before credential issuance.
- Applicant must appear in-person at least once before the issuance of a PIV credential.

PIV Identity Proofing and Registration Requirements (Cont.)

- Applicant shall be required to provide two forms of identity source documents in original form. Source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal government-issued picture identification (ID).

- PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

PIV Issuance and Maintenance Requirements

- The organization shall use an approved PIV credential issuance and maintenance process.
- Ensure completion and successful adjudication of a National Agency Check (NAC), National Agency Check with Written Inquiries (NACI), or other OPM or National Security community investigation as required for Federal employment. The PIV credential shall be revoked if the results of the investigation so justify.
- At the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority.

PIV Issuance and Maintenance Requirements (Cont.)

- The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited).

FIPS 201 REQUIREMENTS

Privacy Requirements

- HSPD 12 requires that PIV systems are implemented with all privacy controls specified in this standard, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002, the Privacy Act of 1974, and Office of Management and Budget (OMB) Memorandum M-03-22, as applicable.

- All agencies must:
  - have a privacy official role,
  - conduct Privacy Impact Assessment (PIA) in accordance with standards,
  - have procedures to handle Information in Identifiable Form (IIF),
  - have procedures to handle privacy violations,
  - maintain appeals procedures for denials/revocation of credentials.