Summary of Changes

Core structural changes and rationale
Original FIPS 201

- Specified four major activities and systemic components in one flow
  - ID Verification and Validation
  - Credential issuance (Card management)
  - Logical access control systems (PKI management)
  - Physical access control systems (CHUID and Biometrics)
- Did not enable clean guidance for technical solutions and procurement
PIV Identity Verification and Issuance

1. Employee Application
2. Employer/Sponsorship
3. Approval Authority
4. Enrollment
5. Identity Management System (IDMS)
6. Identity Verification
7. Card Production & Personalization
8. Issuer - Card Activation

- 1:n biometric search
- Confirm employment
- ID Validation through standard government wide services
  - Government DB’s
  - Threat risk

Numbers Indicate Functional Areas of Responsibility

Green functions manage Chain of Trust for Identity Verification

Employee Enrolls

Employee Application

Issuer - Card Activation

PIV Activated for Operational Use
Proposed FIPS 201

• Focuses intently on the Identity Management issue for HSPD-12 compliance
  – Strong chain of trust for credentialing using electronic processes
  – Identity verification and validation, not trustworthiness
  – Clean separation between ID management and card management
  – Future proofs the solution by placing technology specific issues within SP800-73 (e.g., cryptographic and biometric issues)

• Operational use is specified in use case scenarios
  – Clarifies inter-agency interoperability requirements

• Enables flexibility in procurement of all systemic components
  – IDMS
  – ID validation and verification solution
  – Card production/issuance
  – Enrollment
  – Logical solutions (PKI)
  – Physical access control solutions