FIPS 201-3 Public Workshop:

PIV Identity Proofing, Enrollment/Registration

David Temoshok
Applied Cybersecurity Division
Information Technology Laboratory (ITL)

Jim Fenton
Altmode Networks

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Topics

- Alignment with SP 800-63-3 *Digital Identity Guidelines*
- PIV Enrollment Record
- PIV Biometric Collection and Comparison
- PIV Identity Proofing Documentation Strength and Validation
- Supervised Remote Identity Proofing

Alignment with SP 800-63-3 *Digital Identity Guidelines*

- Assurance level alignment – alignment to SP 800-63-3 assurance scheme (IAL, AAL, FAL) from 4 LOA model
  - PIV Identity Proofing – IAL3
  - PIV logical authentication – AAL2/3 authentication processes
  - Federation – FAL 1/2/3 federation assurance
  - PIV card – multifactor cryptographic authenticator
- Terms/concepts alignment
  - examples: authenticator, federation, federation assurance level (FAL), (PIV) enrollment record, assertion (federation assertion), supervised remote identity proofing

PIV Enrollment Record

- Transition from previous optional “chain of trust” to mandatory PIV enrollment record
- Recorded and maintained by the PIV card issuer
- Auditable record of key enrollment /security events
  - Background investigation adjudication and PIV eligibility determination
  - Log/record of key enrollment and identity proofing steps
  - Identity evidence documentation
  - Biometric records
  - Subsequent changes in enrollment information/documentation
- Used to support PIV processes
  - PIV card replacement and reissuance
  - Inter-Agency transfers for PIV enrollment and issuance processes
  - Grace period for temporary lapses in PIV status

PIV Biometric Collection and Comparison

- Restatement/clarification of requirement for PIV enrollment fingerprint (FP) biometric collection and comparison to 10-print collected for background checks
  - PIV enrollment may use 2 FP from 10-print FP collected for background check
  - Biometric comparison is required for PIV FP collection and 10-print FP collected for background check if collection occurs in separate sessions
- Clarification of requirement for biometric comparison for multi-session PIV enrollment
  - Biometric collection and positive comparison to previous biometrics collected and recorded in the Enrollment Record for PIV enrollment occurring over more than one session.

PIV Identity Proofing Documentation Strength and Validation

- Identity evidence required at SUPERIOR/STRONG strength + FAIR based on SP 800-63A and Agency response to BRM response on document evidence.
- Primary source document:
  - Specified list of primary source documents
  - Meet SP 800-63 STRONG evidence requirements
  - Driver's licenses and state ID must be REAL-ID compliant
- Secondary source document:
  - Must meet SP 800-63A FAIR evidence requirements
  - Obsolete documents removed from document examples list
- Compensating controls applied from employee hiring, background checks, suitability determination, vetting processes for evidence validation and verification of binding to meet SP 800-63A IAL3

Supervised Remote Identity Proofing

- Optional capability for remote identity proofing to meet comparability with FIPS 201 in-person identity proofing requirements
- Intended to reduce cost and travel associated with PIV enrollment and issuance
  - May be used to address health/security concerns due to the circumstances such as the coronavirus pandemic
- Station operated and controlled by issuer connected with central operator via broadband connection
- Specific requirements
  - Controlled-access environment, monitored by minimally-trained staff (e.g., guard)
  - Overview camera allowing operator to monitor applicant and environment
  - Specialized sensors to validate physical and cryptographic security features of evidence and collect biometric data
  - Operators undergo training to perform identity proofing sessions and detect fraud