

Policy Overview for A Government-Wide Framework for Secure and Reliable Identification

The following components are necessary to establish a Government-wide framework for secure and reliable identification. The basic outline for each document is provided below. The documents are presented in order of the most high-level policy to those containing most specific implementation requirements. Copies of these documents as developed for the FiXs System can be accessed at www.FiXs.org.

- I. **A Trust Statement** establishes the basis for the system along with the reasons for employing the model. The statement establishes the entities, delineates the responsibilities, and refers to the most fundamental, high-level policy elements that ensure compliance with the intent of the system. The document's sub-headings are:

Introduction – an explanation of the problem, background, and rationale of the proposed program

Establishment of Entities - the methods and underlying purpose of establishing a Federation of organizations to solve the identity management problem

Rules – an overview of the rules to which a Federation member must abide

Standards and Specification – an overview of the minimum technical compliance required along with the rationale for compliance.

- II. **A Policy Statement** defines the exact mandates the system must follow in order to be successful and lawful. Included are existing policies and policies enacted specifically to support the system. The document's sub-headings are:

Introduction – an explanation of the document's purpose and an overview of the policy embedded.

Policy – an exhaustive list of policy directly affecting the system. It includes overarching policy as well as policy local to the system.

Trust Model – the basis for which an agreement must be made among participants to the Federation.

Responsibilities – a finite list of actions that participants must accomplish in order to participate in the system. This paragraph also signifies how the Federation will police itself along with the structure for that oversight. This paragraph describes the different roles assumed by the government and industry in support of government.

- III. **Operating Rules** outline the roles and responsibilities of parties to authentication transactions. Operating Rules have been used for decades by the financial services community to outline the "rules of the road" for electronic networks, such as the ACH network for Direct Deposit and Visa and MasterCard. They set out requirements for the networks. They are a blend of policy (why we must do it), process (how we must do it), and practice (the day-to-day timeframes and maintenance activities required to ensure compliance with policy). Operating Rules reference existing technical standards, but typically do not create new technical standards themselves. The Operating Rules developed for the FiXs network contain the following headings:

1 GENERAL REQUIREMENTS AND DEFINITIONS

- 1.1 PERSONNEL DEFINITIONS AND REQUIREMENTS
 - 1.1.1 *Program Manager*
 - 1.1.1.1 Domain Technical Administrator
 - 1.1.1.2 Domain Functional Administrator
 - 1.1.2 *Enrollment Personnel Requirements*
 - 1.1.2.1 Facility Administrative Enrollers
 - 1.1.2.2 Facility Enrollers
 - 1.1.2.3 Facility Verifiers
 - 1.1.3 *Authentication Personnel Requirements*
 - 1.1.3.1 Facility Domain Administrators
 - 1.1.3.2 Authentication Station Operators
- 1.2 SYSTEMS FACILITY DEFINITIONS AND REQUIREMENTS
 - 1.2.1 *PIV Trust Gateway Broker Interface Requirements*
 - 1.2.2 *Credential Issuer System Site Requirements*
 - 1.2.2.1 Enrollment Site Certification Requirements
 - 1.2.2.2 Enrollment System Requirements
 - 1.2.2.3 PIV Domain System Requirements
 - 1.2.3 *Relying Party System Site Requirements*
 - 1.2.3.1 Relying Party Authentication Site Certification Requirements
 - 1.2.3.2 Relying Party Authentication System Requirements
 - 1.2.4 *Records/Files Maintenance Requirements*
 - 1.2.4.1 PIV File Updates
 - 1.2.4.2 Notification of Revocation of PIV Status/Dis-Enrollment
 - 1.2.4.3 Audit Requirements

2 CREDENTIAL ISSUER RESPONSIBILITIES

- 2.1 CREDENTIAL ISSUANCE
 - 2.1.1 *Validate Applicant's need for PIV Credentials*
 - 2.1.2 *Verify Applicant Identification (Vetting/Identity Proofing)*
 - 2.1.2.1 Verify Employees Identification Documents
 - 2.1.3 *Enroll Applicant Into PIV System*
 - 2.1.3.1 Verify Applicant's Biometric
 - 2.1.3.2 Enroll Applicant into PIV DDS System
 - 2.1.4 *Issue Participant Valid PIV Identifier*
 - 2.1.4.1 DoD EDI PIN for CAC Cardholders
 - 2.1.4.2 Organization Name and Employee ID for non-CAC Cardholders
 - 2.1.4.3 Identifier Access Method
- 2.2 TRANSACTION REQUEST PROCESSING
 - 2.2.1 *Processing Authentication Inquiries*
 - 2.2.2 *Initiating Authentication Responses*

3 RELYING PARTY RESPONSIBILITIES

- 3.1 VISITOR TRANSACTION PROCESSING
 - 3.1.1 *Credential validation and Transaction Routing*
 - 3.1.1.1 Initiating Authentication Inquiry
 - 3.1.1.2 Transaction Routing
 - 3.1.2 *Processing Authentication Responses*
 - 3.1.2.1 Complete Credential Holder Authentication
 - 3.1.2.2 Determine Access Authorization
- 3.2 EXCEPTION PROCESSING
 - 3.2.1 *Badge/Token-Not-Present*
 - 3.2.2 *Other Exceptions*

4 PIV TRUST GATEWAY BROKER OPERATOR RESPONSIBILITIES

4.1 SYSTEM ADMINISTRATION REQUIREMENTS ERROR! BOOKMARK NOT DEFINED.

4.1.1 *Designate PIV Trust Gateway Broker System Administrator*

4.1.2 *Member Interface Management*

4.1.3 *Maintenance of Control Data*

4.1.4 *Activation and De-Activation of PIV Domains*

4.1.4.1 *Initiation of Domain Enrollment Process*

4.1.4.2 *Activation of PIV Domains*

4.1.4.3 *De-Activation of PIV Domains*

4.1.5 *System Performance Requirements*

4.2 TRANSACTION PROCESSING AND ROUTING

4.2.1 *Authentication Inquiries*

4.2.2 *Authentication Responses*

4.2.3 *Audit Control Data Transactions*

5 LIABILITIES AND INDEMNIFICATION

5.1 **LIABILITY UNDER THESE RULES**

5.2 **LIABILITY TO MEMBERS AND PARTICIPANTS**

6 SECURITY AND PRIVACY

6.1 **GENERAL SECURITY REQUIREMENTS**

6.2 **INFRASTRUCTURE REQUIREMENTS**

6.3 **AUDIT REQUIREMENTS**

6.4 **SECURITY AUTHORIZATIONS**

6.4.1 *General*

6.4.2 *domain Technical Administrator*

6.4.3 *Domain Functional Administrator*

6.4.4 *Facility Domain Administrators*

6.4.5 *Facility Administrative Enrollement*

6.5 **PRIVACY**

7 PIV/PIV GOVERNANCE

7.1 **PIV BUSINESS REQUIREMENTS**

7.1.1 *Establish PIV Member Partnership Agreement(s)*

7.1.2 *Effect of Rules*

7.2 **PIV OPERATING ENTITY RESPONSIBILITIES**

7.2.1 *PIV Member Admission Management*

7.2.2 *Member Site Certification Management*

7.2.3 *PIV DOrain authorizations and revocations*

7.2.4 *PIV System Documentation Management*

7.2.4.1 *PIV Operating Rules*

7.2.4.2 *PIV Technical Architecture*

7.2.4.3 *PIV Trust Statement*

7.2.4.4 *PIV Policy Statement*

7.2.4.5 *PIV Governance Procedures*

7.3 **PUBLIC STATEMENTS**

8 DEFINITIONS

IV. Technical Requirements (Embodied in FIPS 201)

V. Memoranda of Understanding

Memoranda of Understanding bind participants to the documents referenced above. They are currently executed between FiXs, DoD and participating companies. Large companies may execute MOUs with small business to handle the vetting, enrolling and credential issuance for the small business' employees.