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

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.