FiXs Certification and Accreditation Process

V 2.0

January 15, 2016

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF APPENDICES

1 FIXS CERTIFICATION AND ACCREDITATION PROCESS

1.1 Background

The Federation for Identity and Cross-Credentialing Systems (FiXs™) is a not-for-profit 501 c (6) trade association comprised of a coalition of industry and public sector organizations whose objective is to support efforts to develop standards supporting the creation and deployment of a secure interoperable identity cross-credentialing network. These Certification and Accreditation (C&A) processes are based on requirements and security guidance contained in numerous government directives and policies as well as industry standards and best practices and define the rights, responsibilities and liabilities of FiXs Member Organizations and are a part of a larger set of governance documents that lay the foundation for establishing trust in and the operations of the FiXs Network. The other documents, known as the FiXs Foundational Documents, include:

- The Trust Model;
- FiXs Policy;
- Implementation Guidelines;
- The Technical Architecture and Specifications; and
- Security Guidelines.

The FiXs Network provides a highly-scalable, secure, auditable solution set, whereby participating organizations can authenticate FiXs-Certified Credentials (also known as FiXs Credentials) issued to users from other participating organizations or "Subscribers" as well as authenticate the credentials issued by other related organizations (i.e. cross-credential). FiXs relies on a Federated Model of Trust, which is discussed more fully in the FiXs Trust Model. The federated identity model establishes trust between member organizations through the use of agreements, standards and technologies that make an "identity credential" portable across the organizations.

Initially, FiXs established a trusted relationship between certain FiXs Member Organizations and the DoD's Defense Cross-Credentialing Identification System (DCCIS). The federation enabled participating Department of Defense (DoD) and industry facilities to achieve strong, and interoperable identity verification and authentication of participating contractor/private sector personnel who presented a company-issued trusted credential. Similarly, participating industry locations also recognized the DoD-issued Common Access Card (CAC) and the Defense Biometric Identity System (DBIDS) credential, which required no modifications in order to operate with FiXs and DCCIS. This initial proof-of-concept established the baseline for further expansion.

FiXs, which is the only organization authorized to inter-operate a cross-credentialing system with the U.S. Department of Defense, is deployed in a federated manner to enable other government agencies, first responders, and industry partners to authenticate the identity of individuals who seek access to their physical or logical assets in either the government or commercial environment.

In a federated system each sponsoring organization maintains its own database of enrolled members. Privacy and security are maintained because no identity information is held

centrally or maintained in the infrastructure except in the employee's host organization domain server.

In order to implement and achieve security standards outlined in Homeland Security Presidential Directive 12, FiXs has developed a certification and accreditation (C&A) process which is based on requirements and security guidance outlined in OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources. The FiXs C&A process incorporates both national security policy guidance outlined OMB Circular A-130 and C&A process definitions and implementation guidelines which are defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, NIST 800-53, NIST 800-79-1, and other NIST information security and PIV publications. The NIST documents, along with FiXs Operating Rules, Implementation Guidelines, and other policy and procedural documents collectively define the policy and procedural baseline for the FiXs C&A process. The FiXs C&A process is based on the following NIST and FiXs documents:

a. NIST SP 800-37, May 2004
b. NIST SP 800-53, Revision 1, Dec 2006
c. NIST SP 800-53A, Jul 2008
d. NIST SP 800-79-1, Jun 2008
e. National Information Assurance Certification and Accreditation Process (NIACAP) [NSTISSI No. 1000] , April 2000
f. NIST SP 800-37, Revision 1, Guide for Risk Management Framework, 05 June 2014
g. DoDI 88510.01, Risk Management Framework for DoD Information Technology, 12 March 2014
h. FiXs By-Laws, Version 3.2, 08 Jan. 2016
i. FiXs Security Guidelines, Version 3.1, 01 Sept. 2015
j. FiXs Implementation Guidelines, Version 3.2, 09 Jan. 2015
k. FiXs Policy Document , Version 3.2, 08 Jan. 2016
l. FIXS Operating Rules, Version 3.4, 01 Dec. 2015
m. FIXS Operating Rules, Addendum
n. FiXs Trust Model, Version. 3.1, 01 Sept. 2015

1.2 FiXs C&A Process Overview

The FiXs C&A process provides the policies, procedures, and guidelines for ensuring that FiXs member-deployed systems and components meet federal security standards and protection guidelines for identity management information. As the guidelines established in NIST 800-37, NIST 800-53, and NIST 800-79-1, the FiXs C&A process is designed to provide a set of standard procedures and policies for security certification and accreditation which will enable a governing authority and its Designated Approval Authority (DAA) to

review and analyze the security posture and assess security risks associated with nominated information systems and/or components. In the context of the FiXs C&A process, the FiXs Board of Directors has designated the President of FiXs as its DAA. The FiXs DAA is empowered to authorize operation of a nominated FiXs-related system or component under the framework of the FiXs C&A process. The FiXs DAA will keep the Board updated on the C&A nominations and successful completion of C&A activities along with IATO's and ATO's granted. Currently, the FiXs Board of Directors has delegated C&A review authority and accreditation decision recommendation authority to the organization's selected C&A Committee. The C&A committee works under the auspices of the FiXs CCB which governs its processes and procedures and this document. The standing chair of the C&A committee is the FiXs Corporate Secretary. The FiXs C&A Committee is selected from the general membership of the FiXs organization on a case-by-case basis when an application for C&A has been accepted and nominated for C&A. The selected members are selected based upon the type and nature of review contemplated and their area of expertise at it relates to the review and they are vetted to insure objectivity and no vested interest in the outcome of the C&A being performed.

Following the completion of the certification phase of the C&A process, the FiXs C&A Committee provides an accreditation recommendation to the FiXs DAA. The FiXs DAA analyzes the recommendations from the C&A committee and makes the accreditation decision on behalf of the FiXs organization. .

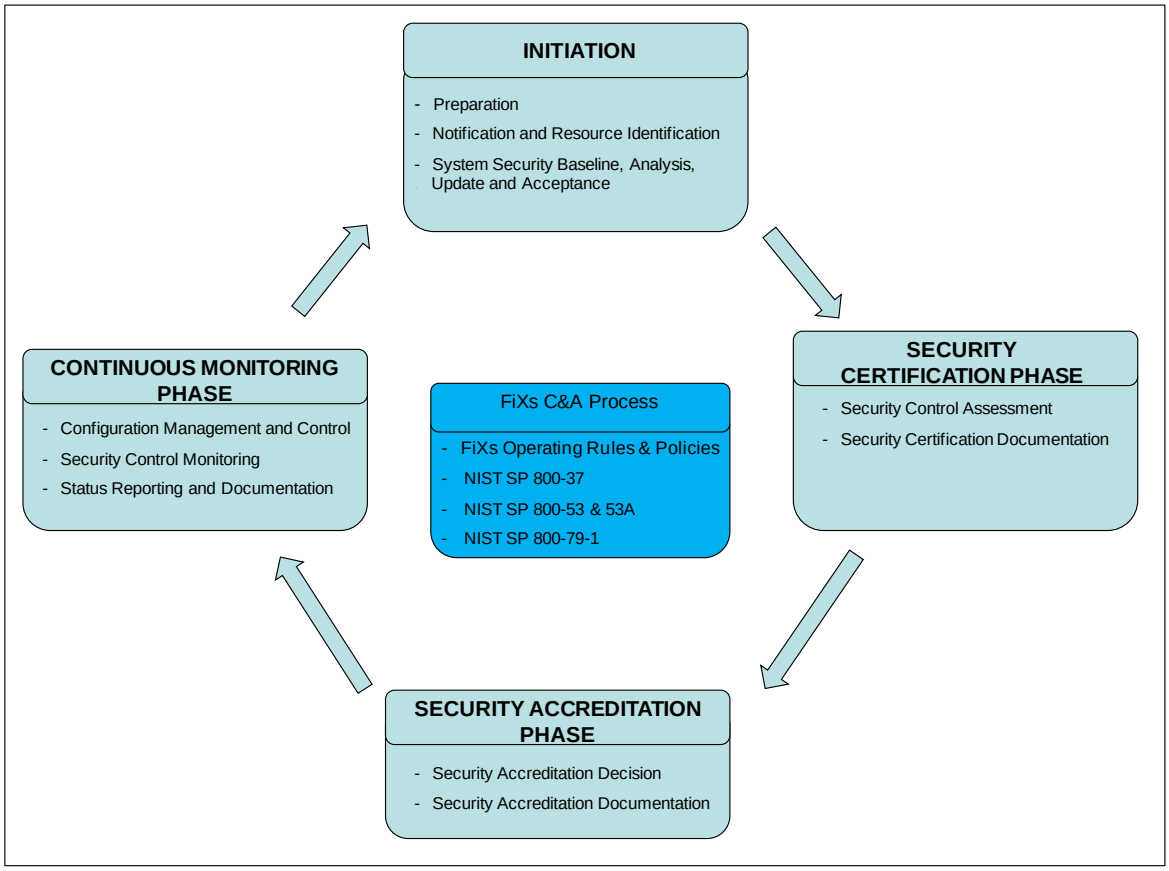

Figure 1: FiXs C&A Process

The FiXs C&A process, similar to the C&A process of the U. S. Federal Government, consists of four distinct phases:

- Initiation
- Security Certification
- Security Accreditation
- Continuous Monitoring

Upon the completion of the certification phase of the FiXs C&A process, the FiXs DAA will review the certification package and issue an accreditation decision on the nominated system or component. The accreditation decision, which is based on the DAA's determination of whether the nominated system or component meets the processes and criteria set forth in this document, to include OMB Circular A-130 NIST 800-37, NIST 800-53, and NIST 800-79-1 mandated information protection and security requirements, results in an "Authorization to Operate," "Interim Authorization to Operate," or "Denial of Authorization to Operate" decision.

2 FIXS C&A INITIATION PHASE

The Initiation Phase consists of three tasks: (i) preparation; (ii) notification and resource identification; and (iii) system security baseline documentation analysis, update, and acceptance. The primary focus during this phase is the establishment of the system's security baseline and the development of the system's supporting security documentation.

The initiation phase of the C&A process begins during the design, implementation, and testing of the proposed information system. Security system certification and accreditation must be factored into these initial phases of the system's lifecycle. Development of the system's security certification and accreditation package should be considered during the early phases of the systems lifecycle. The system's baseline security baseline documentation should be developed prior to the deployment phase. The security baseline assessment as a minimum includes the following actions:

a. Conducting an initial security assessment of the nominated system using the FiXs Baseline Security Assessment Checklist,
b. Preparing a draft System Security Plan (SSP),
c. Conducting an initial System Risk Assessment and preparing a Risk Assessment Report,
d. Developing an initial Plan of Action and Milestones (POA&M)

When the system is nearing the deployment phase, the baseline documentation along with the FiXs ATO application should be submitted to the FiXs C&A Committee.

A key focus of this phase of the C&A process is to ensure that the FiXs DAA and the organization's C&A Committee are in agreement with the contents of the system baseline before the assignment of a certification agent and initiation of the certification phase of the process.

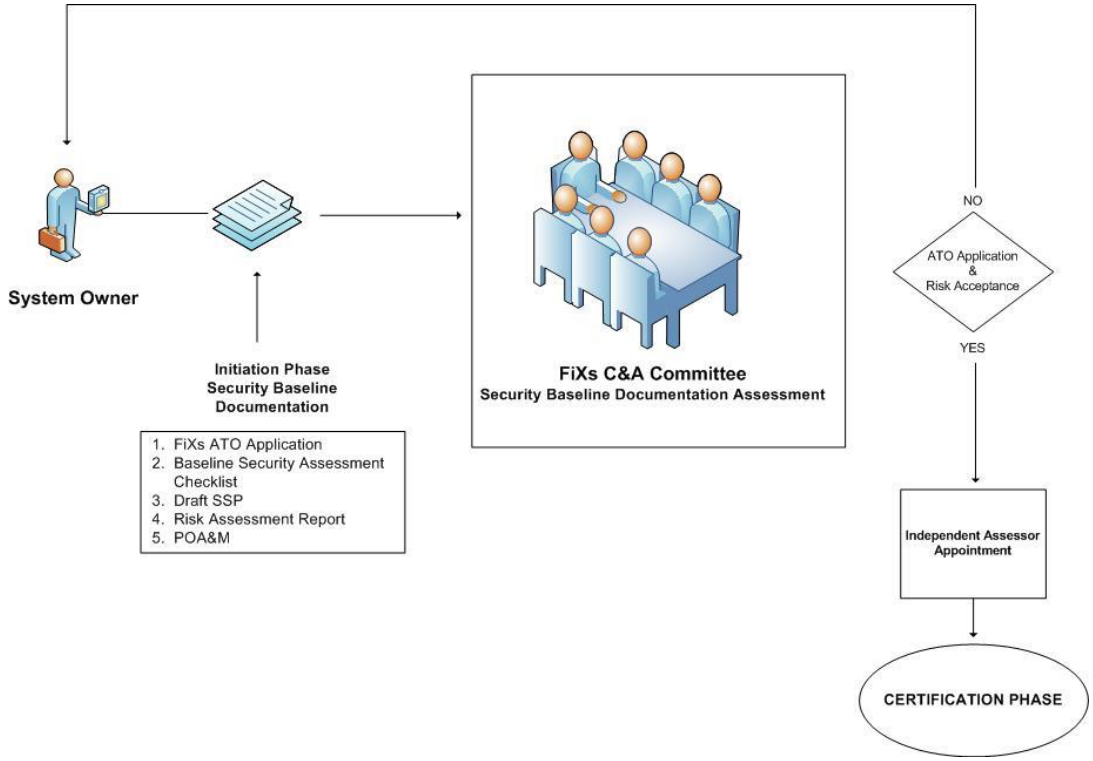

Figure 2: System Baseline Documentation Analysis Process

The C&A Committee will review the submitted security baseline documentation and advise the DAA on the completeness of the submitted documentation and acceptability of the identified risks. After coordination and negotiation on these issues, the system owner is given approval to move into the certification phase of the process. Once activities of the initiation phase have been completed, the FiXs system of records notice (SORN) is updated by the FiXs C&A Committee and the FiXs-approved independent Third-Party Assessor (s) are notified. The system owner negotiates a contract with the independent Third-Party Assessor for conducting an independent system certification and developing a security assessment report and accreditation recommendations.

The FiXs SORN is used to uniquely identify FiXs operating systems and components which are involved in the retrieval and or storage of information which contain personal identity information, e.g., the name of an individual, or some identifying number, symbol, or other identifier assigned to the individual. In compliance with this federal mandate, the FiXs organization will maintain and update the SORN to reflect systems descriptions and a list of identity attributes utilized by each FiXs system or component. The FiXs SORN will be made available to federal authorities for inspection.

3 FIXS SECURITY CERTIFICATION PHASE

All systems nominated for connection and approval to operate over the FiXs Network must be assessed by an independent third-party Assessor. The Applicant must select the Assessor from the list of FiXs authorized and approved certification agents. Once the appropriate support agreements are in place, the Applicant and the Assessor are responsible for gathering appropriate supporting materials which are necessary to support the assessment effort. Typically, all documents and supporting materials included or referenced in the SSP and the FiXs C&A checklist are required to support the assessment effort. Additionally, the results from previous audits, security certifications, security reviews, self-assessments, security test, and privacy impact assessments should be made available to the Assessor.

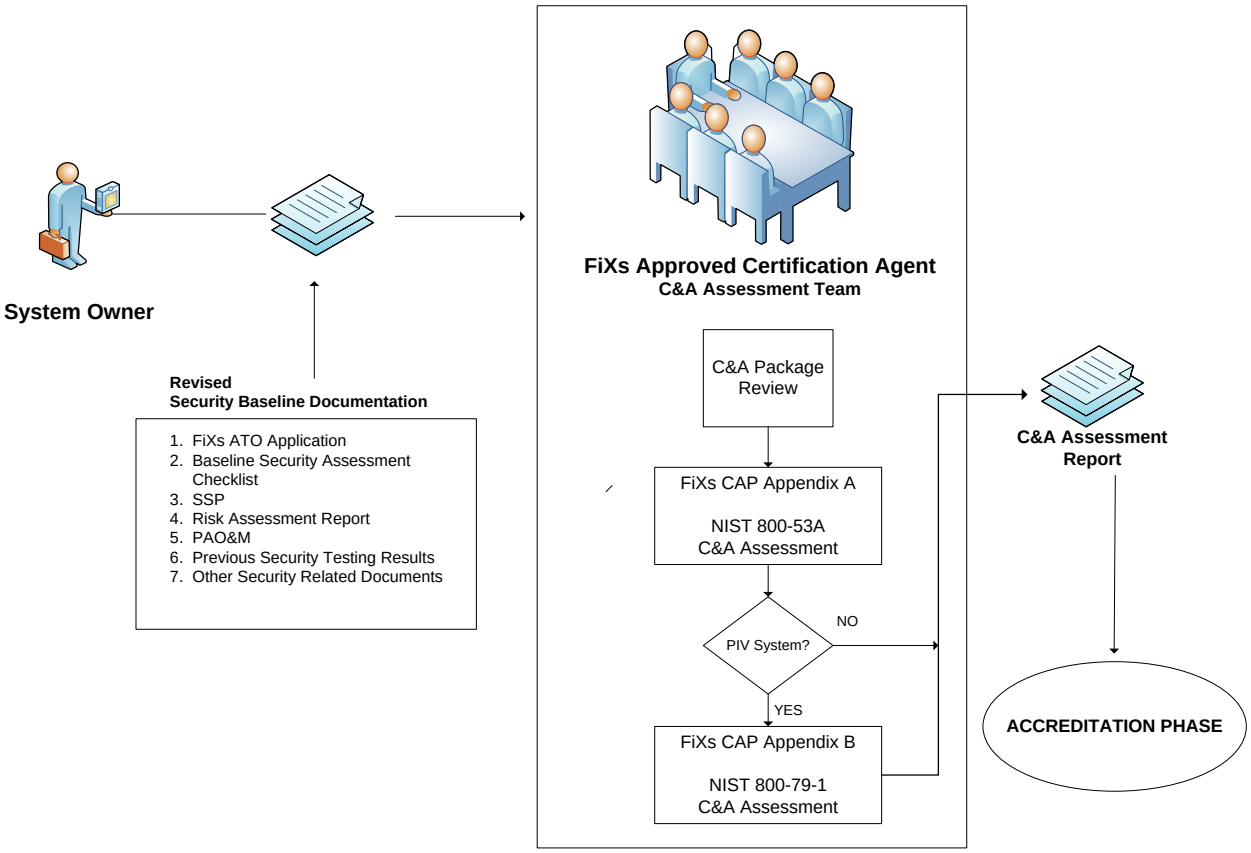

Figure 3: FiXs System Certification Process

The FiXs certification security assessment process outlines assessment criteria for the general information technology system functionality as well as functionality provided in Personal Identity Verification (PIV) systems. General information system assessment criteria and procedures are outlined in the FiXs Security Requirements Checklist, Appendix A. The assessment criteria and procedures for systems that include PIV information are contained in Appendix B, the FiXs PIV Security Requirements Checklist. Depending on the proposed role of the nominated system indicated in the FiXs connection application, one or both of the above checklists may be used to assess the security controls of a nominated system.

When the nominated system or component includes PIV functionality, the NIST 800-53A based IT security controls must be assessed first. Following the completion of the NIST SP 800-53A based security controls assessment, the NIST 800-79-1 based PIV assessment is conducted.

3.1 FiXs General Information System Certification Assessment

Once the security baseline documentation submitted during the initiation phase is assessed and validated by the FiXs C&A Committee, a FiXs-approved Independent Assessor must be selected. Based on guidance resulting from the FiXs C&A Committee review of the submitted security baseline documentation, the Assessor and system owner must select, or develop when needed, appropriate methods and procedures to assess the management, operational, and technical security controls of the nominated information system. The Assessor and system owner will apply the security control tailoring process outlined in NIST SP 800-100 to select the recommended set of security controls from the FiXs Security Requirements Checklist which are applicable to the nominated system. The recommended security controls list for the nominated system should be based on the tailoring guidance contained in NIST SP 800-100, FiXs C&A Committee's comments from system's baseline documentation review, and risks identified in the nominated system's security baseline Risk Assessment Report.

After the recommended security controls have been selected, the Assessor and system owner will designate the recommended assessment method for each selected security control. The list of recommended security controls will be listed in a Systems Requirements Test Matrix (SRTM). The prepared SRTM will indicate one of the following proposed methods for assessing each identified security control:

a. **I**nterview
b. **D**emonstrate
c. **T**est
d. **O**bserve

The Assessor will submit the SRTM to the FiXs C&A committee for review and ratification.

The validated SRTM will define the scope of the information system's security controls assessment effort. The Assessor will conduct the assessment in accordance with the criteria outlined in the validated SRTM.

Once a validated SRTM is established for a common FiXs infrastructure component, the SRTM will generally be used as the baseline for future implementations of components with similar risk characteristics which perform the same functionality. When a pre-existing SRTM is available for a nominated system or component, tailoring recommendations for a nominated system should be based on the established SRTM baseline. A sample SRTM template is provided at Appendix H.

3.2 FiXs PIV Certification Assessment

The FiXs PIV Security Requirements Checklist, Appendix B outlines certification assessment criteria for systems which contain PIV information and support the issuance of PIV Cards. Nominated systems which contain PIV information and support PIV related functionality must undergo assessments under both the FiXs Security Requirements Checklist and the FiXs PIV Security Requirements Checklist. The PIV assessment effort is usually conducted in conjunction with the information systems security assessment. The Assessor will conduct the PIV portion of the assessment in accordance with the criteria outlined in Appendix B. The results of both elements of the assessment effort must be forwarded to the FiXs C&A Committee as part of the forwarded certification and accreditation package.

In addition to undergoing an assessment conducted under the security controls outlined in Appendix B, the nominated PIV system must be completely described in a PIV Card Issuer (PCI) operations plan. This comprehensive document incorporates all the information about the nominated system that is needed for the Assessor to review and assess the capability and reliability of the nominated system's operations. The PCI operations plan includes a description of the structure of the nominated PIV system, its facilities, any external service providers, and the roles and responsibilities within the system owner's PCI facility. A template for a PCI operations plan is provided in Appendix I.

3.3 FiXs Compliance Assessment Report

Following the completion of assessment activities, the Assessor must prepare and submit an assessment report. The assessment report will document the findings found during each phase of the assessment and provide the results of each assessed security control. Based on the assessment results, the system owner with the assistance of the Assessor will update the system's Risk Assessment Report and POA&M. The updates to these documents must also be included with the submitted assessment report.

The assessment report along with the accompanying system risk assessment and POA&M will be submitted to the FiXs C&A Committee for review, evaluation, and in preparing a recommendation to the DAA.

4 FIXS ACCREDITATION PHASE

Upon receipt of the detailed report from the certified Assessor, the FiXs C&A Committee Chairperson will convene a meeting of the C&A committee to review the submitted findings. This committee will be assembled with a minimum of three members. The FiXs C&A Committee Chairman will select impartial committee members, which have an understanding of the process involved and are capable in rendering an objective recommendation. Upon the completion of a detailed review of the assessment report, the C&A Committee may submit follow-up questions and seek clarification of findings supplied in the assessment report.

Once questions and any issues relating the assessment report are resolved, the C&A Committee will make a written recommendation to the FiXs DAA to either grant or deny ATO Certification or provide a conditional interim ATO (IATO) pending completion of open, low-risk requirements and open items identified on the submitted POA&M.

4.1 ATO Decision

The FiXs DAA will analyze recommendations from the C&A committee and make the accreditation decision on behalf FiXs.

If an IATO is granted, the interim period of operations will not to exceed 90 days. It is incumbent upon the Applicant to remedy open issues and to come in full compliance with ATO requirements within the designated period to include having any identified follow-up or incremental assessments completed.

An approval of an ATO or IATO Certification will grant the Applicant the authority to officially operate.

4.2 FiXs ATO Decision Appeals Process

Any applicant whose ATO is denied by the DAA may appeal the decision to a review panel comprised of members of the FiXs Board of Directors.

Upon receipt of an Appeal Request from an applicant, FiXs will appoint a three-member review panel from among the FiXs Board of Directors to hear the appeal request. The panel may request any additional information from the applicant or schedule a hearing to permit the Applicant to further clarify and present his/her position(s). The panel may also make its determination solely upon the information presented in the appeal request. The appointed panel will consider the evidence submitted during the appeal process and make a final determination on the accreditation status of the system.

5 FIXS CONTINUOUS MONITORING PHASE

The Applicant will be required to submit an Annual Renewal Compliance Statement for an ATO Certification to remain in effect. The Applicant must warrant continued compliance with the requirements set forth in the assessment process and shall agree to provide annual audit results. FiXs reserves the right to perform a follow-up compliance assessment or a random compliance assessment at any time. This follow-up assessment will be done with advance notice and coordination with the party being reviewed; however, it will be accomplished without undue delay. The party being reviewed may be required to bear the costs of such reassessment if the conditions are such that the standards then required for being granted an ATO are not being complied with. If such conditions are warranted, any ATO may be cancelled effective immediately.

5.1 Reassessment and Audit

The Applicant must notify the Assessor and the FiXs C&A Committee of any organizational or material changes at least 60 days before the change is performed or immediately upon the occurrence of any unplanned change. FiXs will determine if a reassessment is required for the changes.

The Applicant must also agree to the following conditions to maintain ATO Certification:

- A FiXs-designated Assessor may conduct an on-site reassessment or POA&M review of an Applicant within one year after certification.
- A FiXs-designated Assessor must audit any certified Applicant at least every three years or as needed.
- The Applicant may be required to submit other internal audits, as deemed necessary.
- Additional maintenance activities may be stipulated between FiXs and the Applicant.

5.2 Random-compliance Assessments

Accredited Applicants will be assessed on a random, periodic basis for compliance with FiXs policies and procedures and security compliance. Such random compliance assessments will be performed by independent Assessors, which shall be conducted using the matrix of compliance factors relevant to the system(s) being audited.

5.3 Government-compliance Assessment

Under the terms of the FiXs Memoranda of Understanding (MOU) with the Department of Defense and the flowdown MOU with the Applicant, federal agencies may assess the entire FiXs Network or any of its components to ensure compliance with its regulations and

conformance with the requirements and intent of agreed-to policies. These assessments are random, with or without notice, prompted by indicators from the network or other forms of inspection.

6 ACRONYMS AND ABBREVIATIONS

Term	Definition
Assessor	The individual or organization responsible for conducting assessment activities under the guidance and direction of a Designated Accreditation Authority.
ATO	Authorization to Operate; one of three possible decisions concerning a nominated system made by a Designated Accreditation Authority after all assessment activities have been performed stating that the reliability of the system is accredited and the system is authorized to perform specific PIV of information system functions.
C&A	Certification and Accreditation
DAA	Designated Approval Authority
FiXs	Federation for Identity and Cross-Credentialing Systems
IATO	Interim Approval to Operate
MOU	Memoranda of Understanding
NIACAP	National Information Assurance Certification and Accreditation Process
NIST SP	National Institute of Standards and Technology Special Publication
PCI	PIV Card Issuer
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SRTM	Security Requirements Traceability Matrix
SSP	System Security Plan
TGB	Trusted Gateway Broker

7 REVISION HISTORY

Version	Date	Comments
1.0	September 11, 2008	FiXs Board of Directors approved version 1.0 as baseline.
1.1	September 15, 2008	FiXs Board of Directors on September 11, 2008 approved Change Control Board (CCB) oversight of the Certification and Accreditation Subcommittee (C&A) ***after*** they voted approval of version 1.0. The CAP document was then edited to reflect these CCB and C&A subcommittee changes and reviewed/updated for consistency based on this set of changes. The CAP document version was then updated to Version 1.1.These changes were completed on 9/15/2008.
2.1	January 15, 2016	Revisions to reflect changes to FiXs Bylaws, FiXs Security Guidelines, FiXs Implementation Guidelines, FiXs Policy Documents, FiXs Operating Rules, and the FiXs trust model.
2.1	January 15, 2016	Added NIST SP 800-37, revision 1, and DoDI 88510.01 Guidelines