The Federation for Identity and Cross-Credentialing Systems®

Version 3.1
September 1, 2015

www.fixs.org

Copyright 2015 by the Federation for Identity and Cross-Credentialing Systems®, Inc.
All Rights Reserved
Printed in the United States of America
10300 Eaton Place, Suite 500
Fairfax, VA 22030
(703) 591-9255

TABLE OF CONTENTS

The Federation for Identity and Cross-Credentialing Systems® 1

1.0 INTRODUCTION 3

1.1 PURPOSE 3
1.2 APPLICABILITY AND SCOPE 3
1.3 DEFINITIONS 4
1.4 PROPONENT 4
1.5 GENERAL DESCRIPTION OF INFORMATION SENSITIVITY 4

2.0 MANAGEMENT CONTROLS 5

2.1 RISK ASSESSMENT AND MANAGEMENT 5
2.2 REVIEW OF SECURITY CONTROLS 6
2.3 RULES OF BEHAVIOR 8
2.4 PLANNING FOR SECURITY IN THE LIFE CYCLE 9
2.5 REQUIREMENTS TO AUTHORIZE PROCESSING 13

3.0 OPERATIONAL CONTROLS 13

3.1 PERSONNEL SECURITY 13
3.2 PHYSICAL AND ENVIRONMENTAL PROTECTION 14
3.3 PRODUCTION, INPUT/OUTPUT CONTROLS 19
3.4 CONTINGENCY PLANNING AND INCIDENT RESPONSE CAPABILITY 19
3.5 HARDWARE AND SYSTEM SOFTWARE MAINTENANCE CONTROLS 21
3.6 INTEGRITY CONTROLS 22
3.7 DOCUMENTATION 24
3.8 SECURITY AWARENESS & TRAINING 24
3.9 KEY MANAGEMENT BACKUP/RECOVERY 25

.4.0 TECHNICAL CONTROLS FOR THE FIXS NETWORK 26

REFERENCES 26

FIXS SECURITY COMPLIANCE ASSESSMENT CHECKLIST 29

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

1.0 INTRODUCTION

1.1 Purpose

This Guideline:

1. Describes a set of security guidelines and assigns responsibilities to achieve information assurance for identity management to the Participants of FiXS. Policy is based upon and consistent with the amount of risk permitted within a given community and/or group of communities.

2. Designates the FiXs Executive Board responsible for overall management and integration of guidance, operating, and technical documents.

1.2 Applicability and Scope

This Guideline applies to:

1. All Participants of FiXs (hereafter referred to as "Participants"). Participants consist of three major communities, national security, all other government entities, and the commercial sector. This policy does not supersede US Government policies or regulations.

2. All Participant-owned or -controlled information systems that receive, process, store, display or transmit FiXs identity management information, regardless of mission assurance category, classification or sensitivity.

3. Information systems that support special environments, e.g., Special Access Programs (SAP) and Special Access Requirements (SAR), as supplemented by the special needs of the program.

- Platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, to external networks.
- Information systems under contract to the federal government.
- Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.
- Stand-alone information systems.
- Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

Nothing in this Guideline shall alter or supersede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (reference Executive Order 12333, *SUBJECT: Information Assurance (IA),* October 24, 2002) and other laws and regulations. This Guideline does not apply to weapons systems as defined by DoD Directive 5137.1 or other IT components, both hardware and software, that are physically part

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.

1.3 Definitions

Terms used in this Guideline are defined in National Security Telecommunications and Information Systems Security Instruction Number 4009 or enclosure 2 of Department of Defense Directive 8500.1, Information Assurance, Department of Defense Instruciton 8520.03, Identity Authentification for Information Systems,and in the FiXs Operating Rules.

The FiXs Network is defined as all of the FiXs compliant systems that operate together as a unit to exchange identification information.

1.4 Proponent

The FiXs Security Committee has overall responsibility for the maintenance of this document and shall:

- Monitor, evaluate and provide advice to the Executive Board regarding all IA activities.
- Oversee appropriations earmarked for the IA program and manage supporting activities.
- Develop and promulgate additional IA policy guidance consistent with these Guidelines.
- Establish metrics and annually validate the IA readiness of all Participants.
- Develop and provide IA training and awareness products.
- Develop and provide security configuration guidance for IA and IA-enabled IT products.
- Develop and implement IA personnel management and skill tracking procedures and processes to ensure adequate personnel resources are available to meet critical IA requirements.
- Monitor information system security practices and conduct regular inspections of Participants processes.

1.5 General Description of Information Sensitivity

1. Information handled within the system includes that contained in Immigration Form I-9, biometrics, photographs, personal identification numbers, employer name, employee number, etc. Much of these data require protection as described in the Privacy Act of 1974.

2. The loss, misuse, or unauthorized access to, or modification of, information within the system ranges from temporary loss of access privileges, to identity theft resulting in financial, property, and/or intellectual property fraud and abuse, to personal harm and/or death, to catastrophic endangerment of national security. These levels of security vary depending on a given environment, nature

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

of use, and local access requirements. Therefore, they do not map, nor should be confused with, OMB's 4 Levels of Assurance.

3. FiXs systems are generally classified as a Mission Assurance Category (MAC) "3", Confidentiality Level "Sensitive" system for the purposes of assigning Information Assurance (IA) Controls to implement. These IA Controls are based on the Department of Defense Instruction 8500.2, "*Information Assurance (IA) Implementation*", dated February 6, 2003 (DoDI 8500.2).

2.0 MANAGEMENT CONTROLS

2.1 Risk Assessment and Management

2.1.1 Pre-Operation

Prior to becoming an operational Participant in the FiXs Network; a Participant shall have a risk assessment conducted by an independent third-party Assessor. The Participant shall select the Assessor from the list of FiXs authorized and approved certification agents. The Assessor produces the risk assessment based on the results of security controls tested as part of the Certification Phase. In addition, any findings listed as "to be mitigated prior to becoming operational" shall be mitigated, and a Plan of Actions and Milestones (POA&M) shall be completed. The mitigation of the "to be mitigated prior to becoming operational" findings and the plan will be verified by the organization that performed the risk assessment, and that organization will submit the system risk assessment along with the assessment report and POA&M.

2.1.2 Methodology

The risk assessment will be done in accordance with the methodology defined in NIST SP 800-30[1]. The risk assessment will include checking for items included as requirements or recommendations in NIST SP 800-26[2], the FiXs Operating Rules[3], and Trust Statement[4] documents, OMB Circular No. A-130[5], DoD 5220.22-M[6], and other items found in current Information Assurance best practices. The result of the risk assessment will be a risk assessment report submitted to the FiXs C&A Committee for review, evaluation, and in preparing a recommendation to the DAA.

The completed report will be considered sensitive and will not be shared with other FiXs Participants without written permission from the assessed

---

1 NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*
2 NIST Special Publication 800-26, *Security Self -Assessment Guide for Information Technology Systems*
3 *FiXs Operating Rules*
4 *FiXs Trust Model*
5 OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resource*
6 DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

organization. It shall be marked “Sensitive but Unclassified” and “The FiXs Executive Board may share the information contained in this document with the site analyzed for purposes of review and program planning; under no circumstances may any information in this document be shared with the public, other government offices or agencies, other FiXs Participants, or anyone not approved by the assessed organization.”

2.1.3 During Operation

During operation the systems (processes, equipment, facilities, and personnel) shall be reassessed every 3 years or when ever there is a significant change in the systems. In addition, the operating organization shall perform self-assessments using the methodology described above.

2.2 Review of Security Controls

An assessment of an organization’s security controls shall be conducted prior to the initiation of operation within the FiXs Network and every three years thereafter or when there is a significant change in hardware, software, or physical protection. This may be done as a part of the FiXs Certification and Accreditation Process (CAP) or as a separate activity (at the discretion of the FiXs Executive Board). The security control assessment shall be conducted by a FiXs authorized and approved certification agent. In addition, any findings listed as “to be corrected prior to becoming operational” shall be corrected, and a plan for the correction of any other findings shall be completed.

The purpose of the security control assessment is ensure that FiXs member-deployed systems and components meet federal security standards and protection guidelines for identity management information. FiXs requires a standard set of Information Assurance (IA) controls for use in evaluating the security posture of existing and prospective “Member Service Providers” (MSP) and “Credential Issuers”, hereinafter collectively referred to as “Issuers”. These IA controls provide a baseline to evaluate a prospective Issuer for Certification and Accreditation (C&A) purposes. The objective of the C&A process review is the issuance of an Authority to Operate (ATO), or Interim Authority to Operate (IATO) as applicable, with the FiXs Network.

This process will generally follow the DoD 8500.2 IA Controls for a Mission Assurance Category (MAC) III Sensitive System as the basis for IA controls and requirements for a FiXs Issuer. The DoD 8500.2 MAC III Sensitive IA controls cover all of the areas found in the FIPS 200 and the NIST SP800-53A for systems with similar criticality and sensitivity.

There are two sets of controls – the FiXs Information Systems Security Controls Checklist and the PIV Security Controls Checklist. The FiXs Information Systems Security Controls Checklist is based on NIST 800-53A controls, as well as the FiXs Operating Rules and Implementation Guidelines. The PIV Security Controls will be

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

used for systems which contain PIV information and support the issuance of PIV Cards. It is based on the controls in NIST 800-79-1 and FiXs Operating Rules and Implementation Guidelines.

Guidance for how systems must be configured will be derived from the Defense Information System Agency (DISA) published Security Technical Implementation Guides (STIGs) that are available on the DISA Information Assurance Support Environment website http://iase.disa.mil/stigs/stig/index.html . The Issuer and the C&A assessor will also use the compliance checklist for the STIG found at http://iase.disa.mil/stigs/checklist/index.html to validate that the IA Controls have been implemented. Examples of the STIGs and checklists are the Windows 2003 Server STIG; Database STIG/checklist; Network STIG/checklist; and Traditional Basic Checklist.

To check operating system security settings, the Issuer and the C&A assessor will use the DISA FSO Gold disk in the scan only mode, and for Microsoft products, the Microsoft Baseline Security Analyzer. The Gold Disk can also be found at the DISA IASE website http://iase.disa.mil/stigs/SRR/index.html and the Microsoft Baseline Security Analyzer is found at http://www.microsoft.com/technet/security/tools/mbsahome.Issuerx.
The actual STIGs or Checklist(s) used are dependent upon the proposed architecture the prospective Issuer is using; their operating system(s); databases, applications; and overall solution set and architecture.

The rationale for choosing the aforementioned baselines and tools is that they are proven to be effective, commonly applied and available, as well as kept current while providing the broadest coverage for ensuring systems security. An additional benefit of applying these standards is the increased level of trust between organizations such as FiXs and the DoD/DMDC, other government agencies, as well as many commercial concerns because they are well understood by the broader community of interest.

It is recognized that some of the IA controls may prove to be difficult for a commercial entity to implement, such as using the DoD Vulnerability Management system to register their system and manage vulnerabilities. With this in mind FiXs must approach any implementation of IA controls and security guidelines with a common sense approach that takes into account the risk and the cost of compliance. Many of these issues will be based on sound business decisions. Such determinations will need to be made on a situational basis taking into account the overall security risks and business requirements inherent in the specific solution architecture.

The results of the assessment will be considered sensitive and will not be shared with other FiXs Participants without written permission from the assessed organization. It shall be marked “Sensitive but Unclassified” and “The FiXs

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

Executive Board may share the information contained in this document with the site analyzed for purposes of review and program planning; under no circumstances may any information in this document be shared with the public, other government offices or agencies, other FiXs Participants, or anyone not approved by the assessed organization."

Following the completion of assessment activities, a security control assessment report will be produced and formatted similar to the assessment report described above. The assessment report will document the findings 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 Risk Assessment Report and the POA&M.

Periodic announced and unannounced security audits shall be conducted based on the FICC Recommendations[7] to ensure that the FiXs Network Participants remain in compliance with the security requirements. These audits may be combined with other types of audits. The type and frequency will be determined by the FiXs Executive Board.

The methodology to be followed for the audits and auditor selection shall include:

- Require all FiXs Participants to have and maintain compliance audits.
- Evaluate and approve independent entities that have the expertise to conduct compliance audits.
- Ensure the independence of the compliance auditor.
- Standardize on a specific compliance audit standard that creates uniform expectations, and enhances the ability to assess the community in a uniform manner.
- All prior audit reports shall be reviewed while conducting any new audits.
- Establish timelines for compliance audits and determine how frequently a compliance audit is required after commencement of services.
-

2.3 Rules of Behavior

The system's rules of behavior located within the FiXs Operating Rules[8], Implementation Guidelines, and Trust Model.

The rules of behavior are made available to every user prior to receiving access to the system. Each user shall use this set of rules of behavior or develop their own

[7] Federal Identity Credentialing Committee, Shared Service Provider Subcommittee, *FICC Audit Standards for PKI Shared Service Provider Entities: An Analysis of Requirements and Alternatives*, January 16, 2004

[8] *FiXs Operating Rules*

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

set of rules of behavior (based on the FiXs set) and have it approved by the FiXs Executive Board prior to commencing operation as a part of the FiXs Network.

The rules of behavior:

- Clearly delineate the responsibilities and expected behavior of all individuals with access to the system;
- State the consequences of inconsistent behavior or noncompliance;
- Include appropriate limits on interconnections to other systems; and
- Are an appendix to the system's security plan.

2.4 Planning for Security in the Life Cycle

FiXs Participants will wish to plan to accomplish specific security requirements during each phase of the security life cycle of their FiXs systems in order to enhance the security of the system. While all Participants may not perform all of the tasks described below, this is provided as a guide of possible security activities during the system's life cycle. The section below was taken from NIST SP 800-64[9], which describes the tasks in more detail.

2.4.1 Initiation Phase

2.4.1.1 Security Categorization

An organization shall define which of the three levels (i.e., low, moderate, or high) of potential impact will exist on FiXs, their organization, or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). Security categorization standards assist organizations in making the appropriate selection of security controls for their information systems. FIPS 199[10] and NIST SP 800-60[11] provide a guide for this action.

2.4.1.2 Preliminary Risk Assessment

Based on the results in an initial description of the basic security needs of the system, a preliminary risk assessment shall be done to define the threat environment in which the system will operate. NIST SP 800-26 provides a guide for this action.

2.4.2 Development/Acquisition Phase

2.4.2.1 Risk Assessment

Analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation Phase, but will be more in-depth and specific.

---

[9] NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*

[10] Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (DRAFT)

[11] NIST Special Publication 800-60, *Guide for Mapping Information and Information Types to Security Objectives and Risk Levels* (DRAFT)

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

2.4.2.2 Security Functional Requirements Analysis

Analysis of organizational specific requirements and any requirement to interface FiXs with internal, organizational systems. This may include the following components:

- System security environment, (i.e., enterprise information security policy and enterprise security architecture)
- Security functional requirements

2.4.2.3 Security Assurance Requirements Analysis

Analysis of requirements that address the activities required and assurance evidence needed to produce the desired level of confidence that the information security within the Participants organizational structure while meeting all FiXs rules and policies, and enable the system to work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.

2.4.2.4 Cost Considerations and Reporting

Determines how much of the development, implementation, and operation costs can be attributed to information security over the life cycle of the system. These costs include hardware, software, facilities, personnel, and training.

2.4.2.5 Security Planning

The development of a System Security Plan (SSP) that ensures that, planned or in place, agreed upon security controls is fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the organization's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan of action and milestones).

2.4.2.6 Security Control Development

This activity ensures that security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective.

2.4.2.7 Developmental Security Test and Evaluation

Ensures that security controls developed to supplement FiXs are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

information system is deployed—these controls are typically management and operational controls.

2.4.2.8 Other Planning Components

This activity ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type (if implementation, maintenance, operation, etc. are selected for the organization's FiXs), participation by all necessary functional groups within an organization, and development and execution of the necessary contracting plans and processes.

2.4.3 Implementation Phase

2.4.3.1 Inspection and Acceptance

This activity ensures that the organization validates and verifies that the functionality described in the specification is included in the implemented system. This also ensures that the deployed system meets applicable federal laws, regulations, policies, guidelines, and standards.

2.4.3.2 Security Control Integration

Ensuring that security controls are integrated at the operational site where the information system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.

2.4.3.3 Security Certification

Ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information and systems. Security certification also uncovers and describes any known vulnerabilities in the system.

2.4.3.4 Security Accreditation

Provides the necessary authorization for the organization's system to process, store, or transmit information that is required to become a part of the FiXs Network. This authorization is granted by the FiXs Executive Board and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to organizational assets or operations and the FiXs community.

2.4.3.5 Data Protection Requirements

Determine the requirement for the protection of sensitive data (such as encryption). Ensure the implementation of data protection requirements.

2.4.4 Operation/Maintenance Phase

2.4.4.1 Configuration Management and Control

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

These activities ensure adequate consideration of the potential security impacts due to specific changes to a system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, firmware, environment, and personnel components for the system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

2.4.4.2 Continuous Monitoring

This will ensure that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the system to the appropriate organizational and FiXs officials is an essential activity of a comprehensive security program.

2.4.4.3 System Security Plan Updates

If a SSP was developed, it shall be updated whenever there is a change to the system that is documented in the plan. The SSP shall be considered a "living document" that is continually updated as changes occur.

2.4.5 Disposal Phase

2.4.5.1 Information Preservation

This activity ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the current retrieval method obsolete.

2.4.5.2 Hardware and Software Disposal

Ensure that hardware and software is disposed of as directed by organizational and federal policies and laws, the organizational security and information system security officers.

2.4.5.3 Media Sanitization

Ensure that all sensitive data, software, and firmware is deleted, erased, and/or written over as necessary.

2.4.5.4 Data Transfer

Ensure that all organizational and federal policies, laws, regulations, etc. are followed when moving data or programs to another system as well as during archiving, discarding, purging, clearing, overwriting, degaussing, or destroying (memory or media) activities. Ensure that only those with the proper need-to-know and authorization are permitted access to sensitive data even during these activities.

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

2.5 Requirements to Authorize Processing

Before a new system can become an operational part of the FiXs Network it shall be assessed by a FiXs authorized certifier and approved by the FiXs DAA. The FiXs DAA shall accredit a system (authorize it to process as a part of the FiXs Network) if:

- The operating organization has been accepted as a FiXs Participant.
- The system (equipment, processes, and personnel) has successfully passed a risk assessment (all significant findings mitigated and a plan to mitigate non-significant findings is approved).
- The system (equipment, processes, and personnel) has successfully passed a security controls assessment (all significant findings corrected and a plan to correct non-significant findings is approved). The security controls review may be combined with the risk assessment.
- There is a compliant System Security Plan in place that contains the security policies of the system
- The operating organization has agreed to announced and unannounced audits of their FiXs system (equipment, processes, and personnel).
- The operating organization must pass any audit that is performed or suspend processing until any significant finding from an audit are mitigated or corrected, and a plan to mitigate or correct any non-significant findings is presented to and approved by the FiXs Executive Board or their designated representative.

3.0 Operational Controls

3.1 Personnel Security

3.1.1 Definitions and Requirements

Participants of the FiXs organization must designate access permissions and responsibilities to their personnel based on their need for such access in order to fulfill their functional responsibilities as outlined in the FiXs Operating Rules, Section 1.1.

This guideline classifies personnel as Level 4, Level 3 and above, and Level 2.

The following Personnel are considered *Level 4* and shall be subject to additional screening due to their overall control and access to the FiXs system.

- *Program Manager*
- *Domain Technical Administrator*
- *Domain Functional Administrator*

The following personnel are considered *Level 3 and above*, due to their access to enrollment processes and procedures.

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

- *Facility Domain Administrator*
- *Facility Administrative Enroller*

The following personnel are considered *Level 2* in the FiXs system, due to their low level of access to systems beyond their local Participant facility.

- *Facility Enroller*
- *Facility Verifier*
- *Authentication Station Operator*

Note: The Facility Enroller and Facility Verifier cannot process FiXs card requests at a level higher than the level FiXs card they possess.

3.1.2 Screening

All personnel shall be required to have FiXs compliant background checks of criminal, employment, and financial information. Sensitive personnel shall be subject to routine criminal background checks. Least sensitive personnel shall be subject to screening at the Participants discretion.

1. **3.1.3 Audit Requirements**

   Each participating organization is responsible for maintaining complete and up-to-date records of events related to their participation in FiXs. It is a requirement that all FiXs transactions have the ability to be re-created from start to finish including records of the personnel performing the transaction. Event logs and transaction audit data will be held for 7 years by each participating organization.

2. **Separation of Duties**

   The identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person.

3. **Access Controls**

   Each class of sensitive and least sensitive personnel may access FiXs systems using Role Based Access Control methods. The Program Manager shall be responsible for ensuring the appropriate issuance and revocation of access credentials for Participant personnel, including the immediate revocation of credentials for terminated employees, and the audit of terminated employees FiXs activities where appropriate.

3.2 Physical and Environmental Protection

The requirements for physical protection for the systems (e.g., locks on terminals, physical barriers around the building and processing area, etc.) are presented below.

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

4. **3.2.1 FiXs Domain Server (FDS)**

3.2.1.1 Physical Access:

The FDS shall be:

- Within a building that is protected from unauthorized access by a guard and/or receptionist or an access control system.
- Within a room that has access controlled by a locking mechanism.

3.2.1.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.
- The room shall be equipped with a manual fire extinguisher and instructions for its use.

3.2.1.3 Failure of Supporting Utilities:

The equipment shall be equipped with an Uninterruptible Power Supply for the FDS (may be supplied by the building) that allows the system to operate for a sufficient period for the FDS to be gracefully shut down.

3.2.1.4 Structural Collapse:

There shall be no structural damage or decay to the building.

3.2.1.4.1 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
- There shall be no plumbing lines running over, adjacent to, or under the FDS.

.A.4..1.

.A.4..2.3.2.1.4.2 Rings of Security Requirements:

- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
- The FDS shall have at least 4 rings of security in total (at least 2 physical and 2 electronic). Note: If there is only 1 electronic security barrier, there shall be 3 physical barriers.
- The FDS shall have at least 2 physical rings of security (as described above in “Physical Access.”
- The FDS shall have at least 2 electronic rings of security.

3.2.1.5 Enrollment Workstation

.A.4..3.3.2.1.5.1 Physical Access:

The Enrollment Workstation shall be:

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

- Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
- Within a room that has access controlled by a locking mechanism.

.A.4..4.

.A.4..5.3.2.1.5.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.

.A.4..6.

.A.4..7.3.2.1.5.3 Failure of Supporting Utilities:

It is desirable, but not required that the office be equipped with an UPS for the Enrollment Workstation (may be supplied by the building) that allows the system to operate for a sufficient period for the workstation to be gracefully shut down.

3.2.1.5.4 Structural Collapse:

There shall be no signs of structural damage or decay to the building.

3.2.1.5.5 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
- There shall be no plumbing lines running over, adjacent to, or under the Enrollment Workstation.

3.2.1.5.6 Interception of Data:

Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.

3.2.1.5.7 Local Authentication:

- Boot or EPROM password that is changed at least every 90 days.
- Username/Password for the local domain that is changed at least every 90 days
- A Trusted Platform Module must be present in compliance with Trusted Computing Group standards, and used for local or PKI authentication where appropriate for the local domain (ref 49).
-

3.2.1.5.8 Rings of Security Requirements:

- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
- The Enrollment Workstation shall have at least 4 rings of security (at least 2 physical and 2 electronic) in total. Note: If there is only 1 electronic security barrier, there shall be 3 physical barriers.

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

- The Enrollment Workstation shall have at least 2 physical rings of security (as described above in “Physical Access,” more is always better.
- The Enrollment Workstation shall have at least 1 electronic ring of security.

3.2.1.6 Authentication Workstation

3.2.1.6.1 Physical Access:

The Authentication Workstation shall be:

- Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
- In an area that is under the observation of a guard and/or receptionist during normal working hours.

.A.4..8.

.A.4..9.3.2.1.6.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The area shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, or equivalent.

3.2.1.6.3 Failure of Supporting Utilities:

It is desirable, but not required to have an UPS for the Authentication Workstation (may be supplied by the building) that allows the system to operate for a sufficient period for the workstation to be gracefully shut down.

.A.4..10.

.A.4..11. 3.2.1.6.4 Structural Collapse:

There shall be no signs of structural damage or decay to the building.

3.2.1.6.5 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
- There shall be no plumbing lines running over, adjacent to, or under the Authentication Workstation.

3.2.1.6.6 Interception of Data:

Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.

3.2.1.6.7 Local Authentication:

- Boot or EPROM password that is changed at least every 90 days.
- Username/Password for the local domain that is changed at least every 90 days

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

- A Trusted Platform Module must be present in compliance with Trusted Computing Group standards, and used for local or PKI authentication where appropriate for the local domain (ref 49).

.A.4..12.

.A.4..13. 3.2.1.6.8 Rings of Security Requirements:

- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
- The Authentication Workstation shall have at least 3 rings of security (at least 1 physical and 1 electronic) in total. Note: If there is only 1 physical security barrier, there shall be 2 electronic barriers.
- The Authentication Workstation shall have at least 1 physical rings of security (as described above in "Physical Access."
- The Authentication Workstation shall have at least 1, but preferably 2, electronic rings of security.

5. **3.2.2 FiXs Trust Broker**

3.2.2.1 Physical Access:

The FiXs Trust Broker shall be:

- Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
- Within a room that has access controlled by a locking mechanism.

3.2.2.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.
- The room shall be equipped with a manual fire extinguisher and instructions for its use.

3.2.2.3 Failure of Supporting Utilities:

The room shall be equipped with an UPS for the FiXs Trust Broker (may be supplied by the building) that allows the system to operate for at least 2 hours following a power failure.

3.2.2.4 Structural Collapse:

There shall be no signs of structural damage or decay to the building.

3.2.2.5 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

- There shall be no plumbing lines running over, adjacent to, or under the FiXs Trust Broker.

3.2.2.6 Interception of Data:
Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.

3.2.2.7 Rings of Security Requirements:

- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
- The FiXs Trust Broker shall have at least 4 rings of security (at least 2 physical and 2 electronic) in total.
- The FDS shall have at least 2 physical rings of security (as described above in ”Physical Access.”
- The FDS shall have at least 2 electronic rings of security.

3.3 Production, Input/Output Controls

All input and output from FiXs systems shall involve transactions subject to audit trails.

All FiXs Participants shall establish controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. Such controls shall be consistent, at minimum, with the Privacy Act of 1974, and shall cover the following:

1. Storage/handling of I-9, privacy and release forms.
2. Physical protection of printed or electronic information.
3. Policy and process for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
4. Restricting access to output (reports, back-up media, external storage devices, etc.).
5. Procedures for transporting or mailing media or printed output.
6. Labeling based on sensitivity (e.g., Privacy Act, Proprietary).
7. Media storage vaults and physical document libraries, including environmental protection controls/procedures.
8. Sanitization procedures preparing electronic media for reuse (e.g., overwriting or degaussing).
9. Policies for shredding or other destructive measures for hardcopy media when no longer required or electronic media not intended for reuse.

3.4 Contingency Planning and Incident Response Capability

In the occurrence of a disaster or other situation that interrupts the ability of FiXs’ ability to function, it may be necessary to have a recovery/back-up plan and process.

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

There are two types of recovery/back-up plans: both a Disaster Recovery Plan (DRP) and Continuity of Operations Plan (COOP). It is required that there be both a DRP and a COOP for the FiXs Trust Broker. It is desired, but not required, that FiXs Participants have a DRP and a COOP for their FDS. Having a COOP or DRP for the Authentication or Enrollment Workstation is up to the individual organizations. NIST SP 800-34[12] shall be used as a guide for the development of COOPs and DRPs.

1. Continuity of Operations Plan (COOP) – this is a plan with associated procedures that describes how to continue operations during the period of time that a system is down (for up to 30 days) until recovery of operation is accomplished.
2. Disaster Recovery Plan (DRP) – this is a plan and associated procedures that describes how to recover operation capability at an alternate site (it may also include recovery of capability at the damaged site).
3. Any requirements within COOP or DRP for backup processing that relies on support from another organization (or department within an organization) shall be documented with a formal agreement (Memorandum of Understanding) between the organizations (departments).
4. The COOP or DRP shall include the requirements for documented backup and the backup procedures including frequency (daily, weekly, and monthly) and scope (full, incremental, and differential backup). It is suggested that backup be:
    a. Daily incremental
    b. Weekly full
    c. Monthly full
    d. With off-site storage of the weekly and monthly backups
    e. Tapes are rotated so that there are:
        - 2 weeks of daily tapes
        - 2 months of weekly tapes
        - 12 months of monthly tapes
5. Off-site storage of backups and generations of backups shall be kept at a secure facility in a different building than the systems, and preferably a sufficient distance from the systems to avoid a single disaster from damaging both the system and the backups. (But not so far away that it takes an inordinate amount of time to obtain a backup tape when it is needed.)
6. COOPs and DRPs shall be tested on a regular basis. The frequency of testing shall be defined in the plan. The minimum recommended testing frequency is:
    - Annual test that includes actually switching the system to and bringing up the systems at the support facility.

[12] NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

- Quarterly desk top tests where the responsible parties talk through the actions required to accomplish the COOP or DRP.
- It may be possible to combine the tests. In the event of an actual disaster, both plans may have to be implemented.

7. All employees that may be involved in the execution of a COOP or DRP shall be trained in their roles and responsibilities relative to the plans. These same employees shall execute their roles and responsibilities relative to the plans when the plans are tested. New employees with plan responsibilities or roles shall receive plan training as soon as possible.
8. All incidents that affect a FiXs component shall be reported immediately to the Organizational FiXs Program Manager. If the incident has the potential to affect other FiXs components (outside the organization) or the integrity or reliability of the FiXs Network or data, the Organizational FiXs Program Manager shall report the incident to the other FiXs Participants and the Executive Board.
9. Every FiXs Participant shall have an incident handling policy. This policy shall include the recognition and handling or incidents (e.g., what files and logs shall be kept, who to contact, and when). NIST SP 800-61[13] provides a guide for the development of incident handling policies.
10. Every FiXs Participant shall have policies concerning who receives and responds to alerts/advisories (e.g., vendor patches, exploited vulnerabilities).
11. Every FiXs Participant shall have policies concerning preventative measures that shall be in place (e.g., intrusion detection tools, automated audit logs, periodic penetration testing). As a minimum, every FiXs Participant shall have policies requiring the installation and constant updating/monitoring of Virus Protection software and TripWire (or equivalent) software on the FDS, Authentication Workstation, and Enrollment Workstation.
12. Every FiXs Participant shall notify the other FiXs Participants when ever their FDS will be or is out of service:
    - For more than 30 minutes during normal business hours.
    - For more than 2 hours during non-business hours.

3.5 Hardware and System Software Maintenance Controls

6. **3.5.1 Personnel**

   The Domain Technical Administrator has direct responsibility for the ongoing maintenance and installation of FiXs System hardware and software. They may perform this work unsupervised, or may delegate such maintenances provided such personnel are directly supervised at all times.

[13] NIST Special Publication 800-61, *Computer Security Incident Handling Guide*

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

3.5.2 Emergency Repair and Maintenance

The Domain Technical Administrator may direct that emergency repair or maintenance necessary to meet the uptime requirements outlined in the FiXs Operating Rules. The Domain Technical Administrator is then required to audit the work done within 30 days to ensure system integrity.

3.5.3 Outside Service

Should outside contractors, vendor technicians, or similar personnel be required to perform or assist in hardware or software maintenance, such personnel shall be escorted by Participant personnel at all times, and shall be directly supervised during the actual performance of work. Under no circumstances shall media containing either FiXs software or FiXs data leave their installed locations except under direct and continuous control of the Domain Technical Administrator.

3.5.4 Introduction of New Components

All software or hardware added to an extant FiXs system shall first be tested in a mock environment for 24 hours. During this period, hardware or software components shall be directly tested with their desired functions (bandwidth loading, sample transactions, failure modes, etc.).

3.5.5 Training and Documentation

Any changes to an extant FiXs system, either hardware or software, shall be documented with specific and objective rational for the changes, including cost/benefit analysis and affidavits by the Domain Technical Administrator that such changes will not compromise or degrade the performance of the system. All changes shall be communicated to downstream Participant personnel, preferably with sufficient time to engage in retraining where necessary.

3.6 Integrity Controls

7. **3.6.1 General Requirements**

- All systems shall be continuously monitored by FiXs Participant personnel to ensure adequate performance of FiXs tasks.
- All core networks relevant to FiXs operations shall employ commercially reasonable intrusion detection systems.
- All systems shall use commercially reasonable verification systems to detect tampering, errors, and omissions in FiXs processes.
- All systems shall be subject to penetration testing on at least an annual basis, and ideally performed by a third party.
- All clear text transmission protocols (e.g., FTP, Telnet) shall be disabled on any platforms containing FiXs software and supporting applications.

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

8. **3.6.2 Antivirus/Spyware/Malware**

All computers (servers and workstations) connected to the network will have available up to date virus/spyware/malware scanning software for the scanning and removal of suspected viruses. Specifically:

- All computers shall be automatically scanned on a regular basis where possible.
- Scanning software shall be capable of detecting and regularly updating profiles for:
    - Traditional .exe and .com viruses
    - Automated hidden software installations (spyware)
    - The presence, regardless of source, of password compromising systems
- All anti-virus software shall be subscribed to that software vendor's automatic virus signature system.
- No disk that is brought in from outside the FiXs Participant shall be used until it has been scanned on a standalone machine that is used for no other purpose and not connected to the network. The scanning software on this machine shall be manually checked and updated regularly.
- All systems shall be built from original, clean master copies whose write protection has always been in place. Only original master copies shall be used until virus scanning has taken place.
- All diskettes containing executable software (software with .EXE and .COM extensions) shall be write protected wherever possible.
- Shareware shall not to be used; shareware on disk or downloaded from a bulletin board is one of the most common infection sources. If it is absolutely necessary to use shareware it shall be thoroughly scanned before use.
- New commercial software shall be scanned before it is installed as it occasionally contains viruses.
- To enable data to be recovered in the event of a virus outbreak, regular backups will be taken by FiXs Participants.
- Users will be kept informed of current procedures and policies.
- Users will be notified of virus incidents.
- FiXs Participant employees will be held directly accountable for any breaches of the Company's anti-virus policies.
- Anti-virus policies, procedures and software will be reviewed regularly (at least annually).

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

3.7 Documentation

9. **3.7.1 Initial Documentation**

   At the time of installation, the Domain Technical Administrator shall document the hardware and software, with specifications, version numbers, and integration notes. Additionally, all policies and procedures with regards to the implementation of the FiXs Operating Rules, approval and access procedures, emergency/contingency plans, and other relevant procedures shall be included.

10. **3.7.2 Access**

    All security policies and procedures shall be documented in a single location (e.g., binders, a commonly accessible share). All new employees shall be briefed by senior IT personnel on security policies and procedures before accessing any portion of the FiXs system. Any changes to the FiXs Security Guidelines shall be distributed through normal corporate communications channels, and retraining shall occur where needed.

11. **3.7.3 Review**

    All documentation shall be reviewed at least annually, or in response to any structural or environmental changes to the system. Further, the Program Administrator is responsible for providing any changes in the FiXs Operating Rules, this security policy, or any other relevant FiXs initiated communication to the Domain Technical Administrator so that they may review and update policies and procedures.

3.8 Security Awareness & Training

12. **3.8.1 Preliminary Employment Training**

    All employees shall undergo thorough training for their designated role in the FiXs system. Such training shall include a detailed briefing on the security procedures in place to ensure the integrity of both the Participant's facilities, and the data used and collected by the system. Employees shall undergo formal testing of their understanding of these procedures before assuming the responsibilities for which they have been trained.

13. **3.8.2 Hands-on training**

    Before operating any component of the FiXs system unsupervised, each employee shall be paired with an existing employee, where possible, or under direct supervision from their superior, for a minimum of 8 hours. Part of hands-on training shall be the simulation of various system failures and unusual circumstances designed to test the trainee's knowledge of security procedures.

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

14. **3.8.3 Currency**

All FiXs system personnel shall be required to attend at least one retraining session (in-house, industry seminar, or additional on-the job training). Such sessions, their content, and their frequency are at the discretion of the Program Manager

15. **3.8.4 Ongoing Education**

The Program Manager is responsible for implementing an ongoing program to reinforce the messages of Security Awareness and Training. Traditional employee training methods (posters, brown bag lunches, seminars, events, etc.) shall be employed on a periodic basis and the Program Manager's discretion.

16. **3.8.5 Help Desk**

FiXs Participants shall establish a help desk for employee questions, reporting of technical problems, and general issues.

17. **3.8.6 Content**

While the primary focus of FiXs security training should be those areas that impact FiXs systems directly, these requirements shall be part of the Participant's overall security training program. Such programs shall include:

- Password policies
- Date encryption and key management
- Privacy policies
- Data preservation and destruction policies
- Social engineering prevention
- Antivirus policies and procedures
- Laptop security
- Security event communication protocols

3.9 Key Management Backup/Recovery

18. **3.9.1 Architecture**

FiXs architecture should make use of a FiXs approved Security Solution, using Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs) for key storage or better, ensuring that strong hardware based authentication of the platforms is used to the greatest extent possible.

19. **3.9.2 Affected Platforms**

Relevant platforms include, but are not limited to:

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

Enrollment stations
Authentication stations
FiXs Domain Servers
FiXs Trust Broker

20. **3.9.3 Use of Keys and Backup**

All data generated and stored on these platforms shall be encrypted, with corresponding keys stored in compliance with DCCIS Software Specification 2.0. Keys shall be backed up to external servers securely using secure SSL. The servers shall have access to a domain management system (e.g., active directory) and keys stored on HSMs. (See IV D.) Keys shall be recoverable with minimal disruption and effort. Keys shall be migratable to replacement hardware with approval and key authorization of the Domain Technical Administrator.

4.0 Technical Controls For the FiXs Network

FiXs-based identities and credentials shall be used exclusively for the purposes of FiXs-based systems and applications. Any identities and/or credentials that are presented, displayed and/or transmitted shall not be used, copied, duplicated or deleted for any other purposes. Such use is considered a misuse and violation of the terms of the FiXs agreements.

No FiXs-based identities and/or credentials shall be transmitted unless explicitly solicited by a valid authentication client, FDS server, and/or FiXs Trust Broker and DoD Trust Gateway Broker (TGB) router.

The technical controls for the FiXs Network have been developed from NIST SP 800-26, NIST SP 800-53, NIST SP 800-64, NIST SP 800-73, DOD 8500.1, DODI 8500.2, FiXs Operating Rules, FiXs Trust Model, FiXs Certification and Accreditation Process Document, and FiXs Security Guidelines.

References

The policies, laws, regulations, directives, etc. that affect this system include, but are not limited to:

- NIST Special Publications.
  1. NIST Special Publication 800-12, *An Introduction to Computer Security - The NIST Handbook*
  2. NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*
  3. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

4. NIST Special Publication 800-26, *Security Self -Assessment Guide for Information Technology Systems*
5. NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
6. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*
7. NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*
8. NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information System*
9. NIST Special Publication 800-41, *Guidelines for Firewalls and Firewall Policy*, January, 2002
10. NIST Special Publication 800-42, *Guideline on Network Security Testing*
11. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
12. NIST Special Publication 800-53 (Final Public Draft), *Recommended Security Controls for Federal Information Systems*, January 26, 2005
13. NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems* (DRAFT)
14. NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*
15. NIST Special Publication 800-60, Initial Public Draft, Version 1.0, *Guide for Mapping Types of Information and Information Systems to Security Categories*, December, 2003
16. NIST Special Publication 800-61, *Computer Security Incident Handling Guide*
17. NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*
18. NIST Special Publication 800-73, Interfaces for Personal Identity Verification (PIV) (DRAFT)
19. NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification (PIV) (DRAFT)
20. NIST Special Publication 80-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals

- FIPS Documents
  21. Federal Information Processing Standards (FIPS) PUB 73, *Guidelines for Security of Computer Applications*
  22. FIPS Pub 112, *Password Usage and*
  23. FIPS Pub 180-1, *Secure Hash Standard*
  24. *FIPS 181, Automated Password Generator*
  25. FIPS Pub 186, *Digital Signature Standard*
  26. FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

27. Federal Information Processing Standards (FIPS) Publication 201

- DoD Documents
  28. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*
  29. DoD 8500.1, *Information Assurance*
  30. DoD 8510.1-M, *Information Technology Security Certification and Accreditation Process (DITSCAP)*

- DISA Documents
  31. DISA Instruction 630-230-19, *Information Systems Security Program*
  32. DISA, *Security Technical Implementation Guides (STIGs) and Checklists*, http://csrc.nist.gov/pcig/cig.html

- OMB Documents
  33. OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*

- DCCIS Documents
  34. *FiXs/DCIS Operating Rules, Version 5.4*
  35. *FiXs/DCIS Policy Document, Version 2.0*
  36. *FiXs/DCIS Trust Statement, Version 1.0*
  37. *FiXs/DCIS Technical Architecture and Specifications, Version 1.1*

- Other Documents
  38. Federal Identity Credentialing Committee, Shared Service Provider Subcommittee, *FICC Audit Standards for PKI Shared Service Provider Entities: An Analysis of Requirements and Alternatives*, January 16, 2004
  39. Executive Order 12333, *SUBJECT: Information Assurance (IA),* October 24, 2002
  40. National Security Telecommunications and Information Systems Security Instruction Number 4009
  41. NSA, Security Recommendation Guides
  42. Computer Fraud and Abuse Act
  43. Computer Security Act of 1987
  44. Information Technology Management Reform Act of 1996
  45. Government Information Security Reform Act
  46. Federal Information Security Management Act
  47. Privacy Act of 1974, amended
  48. Electronic Communications Privacy Act, Public Law 99-508, 1986
  49. Trusted Computing Group Architecture Overview
  50. Windows 2003/XP/2000 Addendum Version 5, Release 1 Developed by DISA for the DOD

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®

FiXs Security Compliance Assessment Checklist

The checklist in this section is a compilation of information assurance controls and risk and vulnerability assessment statement that have been developed from NIST SP 800-26, NIST SP 800-53, DOD 8500.1, DODI 8500.2, FiXs Operating Rules, FiXs Trust Model, FiXs Certification and Accreditation Process, and FiXs Security Guidelines. The table below provides a crosswalk between the DoDI 8500.2 IA controls and the FIPS 200 guidance. This has been done to provide assurances to the FiXs members, service providers, issuers and relying parties that FiXs systems have been assessed to meet both DoD, Federal, and commercial best practices in the area of security and information assurance.

This checklist is included for convenience only and is subject to change at the discretion of FiXs. Members and potential members should contact the FiXs executive board for updated Assessment procedures.

The FiXs Baseline Security Assessment Checklist is located in Appendix D of the FiXs Certification and Accreditation Process document:

http://www.fixs.org/Websites/fixs/Images/FiXs%20CAP%20V.%201.1%2015%20Sept%202008_ALL.pdf

Proprietary information of the Federation for Identity and Cross-Credentialing Systems, Inc. ®