



The Federation for Identity and
Cross-Credentialing Systems™

FiXS™ Security Guidelines
Version 2.0
March 29, 2007

www.fixs.org

Copyright 2007 by the Federation for Identity and Cross-Credentialing Systems, Inc.

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Table of Contents

1.0	INTRODUCTION	3
A.	PURPOSE	3
B.	APPLICABILITY AND SCOPE	3
C.	DEFINITIONS	4
D.	PROONENT	4
E.	GENERAL DESCRIPTION OF INFORMATION SENSITIVITY.....	4
2.0	MANAGEMENT CONTROLS	5
A.	RISK ASSESSMENT AND MANAGEMENT	5
B.	REVIEW OF SECURITY CONTROLS	6
C.	RULES OF BEHAVIOR.....	8
D.	PLANNING FOR SECURITY IN THE LIFE CYCLE	8
E.	REQUIREMENTS TO AUTHORIZE PROCESSING.....	11
3.0	OPERATIONAL CONTROLS	12
A.	PERSONNEL SECURITY	12
B.	PHYSICAL AND ENVIRONMENTAL PROTECTION.....	13
C.	PRODUCTION, INPUT/OUTPUT CONTROLS	16
D.	CONTINGENCY PLANNING AND INCIDENT RESPONSE CAPABILITY	16
E.	HARDWARE AND SYSTEM SOFTWARE MAINTENANCE CONTROLS	18
F.	INTEGRITY CONTROLS	18
G.	DOCUMENTATION.....	19
H.	SECURITY AWARENESS & TRAINING	20
I.	KEY MANAGEMENT BACKUP/RECOVERY	21
4.0	TECHNICAL CONTROLS.....	22
A.	IDENTIFICATION AND AUTHENTICATION	22
B.	LOGICAL ACCESS CONTROLS.....	23
C.	AUDIT TRAILS	25
D.	HSM SECURITY LEVEL REQUIREMENTS.....	26
E.	OPERATING SYSTEM SECURITY REQUIREMENTS.....	26

1.0 INTRODUCTION

A. Purpose

1. This Guideline:
 - a. 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.
 - b. Designates the FiXs Executive Board responsible for overall management and integration of guidance, operating, and technical documents.

B. Applicability and Scope

1. This Guideline applies to:
 - a. 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.
 - b. 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.
 - c. 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.
 - i. Platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, to external networks.
 - ii. Information systems under contract to the federal government.
 - iii. Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.
 - iv. Stand-alone information systems.
 - v. 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.
2. 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 39) and other laws and regulations.
3. 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 of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.

C. 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 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.

D. Proponent

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

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

E. 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 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

A. Risk Assessment and Management

1. Pre-Operation

Prior to becoming an operational Participant in the FiXs Network; a Participant shall have a risk assessment conducted by an organization approved by the FiXs Executive Board. In addition, any findings listed as “to be mitigated prior to becoming operational” shall be mitigated, and a plan for the mitigation of any other findings 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 certify to the FiXs Executive Board that the Participant is ready to become operational within the FiXs Network.

2. Methodology

The risk assessment will be done in accordance with the methodology defined in NIST SP 800-30¹. The risk assessment will include checking for items included as requirements or recommendations in NIST SP 800-26², the FiXs Operating Rules³, and Trust Statement⁵ documents, OMB Circular No. A-130⁶, DoD 5220.22-M⁷, and other items found in current Information Assurance best practices. The result of the risk assessment will be a formal report to the FiXs Executive Board.

The completed report 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 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.”

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.

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*

⁵ *FiXs Trust Model*

⁶ OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resource*

⁷ DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*

B. Review of Security Controls

1. A review 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 risk assessment or as a separate activity (at the discretion of the FiXs Executive Board). The security control assessment shall be conducted by an organization approved by the FiXs Executive Board. 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 correction of the "to be corrected prior to becoming operational" findings and the plan will be verified by the organization that performed the security control assessment, and that organization will certify to the FiXs Executive Board that the Participant is ready to become operational within the FiXs Network.
2. The purpose of the security control assessment is to determine if there are any necessary security controls that are missing. 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.
3. 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.
4. In addition to the DoD 8500.2 IA Controls, the application of the FiXs Operating Rules and FiXs Trust Model will be applied in checklist format by the prospective Issuer to substantiate their compliance to these FiXs standards and to allow the C&A assessor to perform their independent assessment.
5. 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.
6. 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>.
7. 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.

8. 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.
9. 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.
10. 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 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."
11. If the results of the security control assessment are not included in the risk assessment report, a security control assessment report will be produced and formatted similar to the assessment report described above. It will receive the same safeguards as the risk assessment report.
12. Periodic announced and unannounced security audits shall be conducted based on the FICC Recommendations⁸ 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.
13. The methodology to be followed for the audits and auditor selection shall include:
 - a. Require all FiXs Participants to have and maintain compliance audits.
 - b. Evaluate and approve independent entities that have the expertise to conduct compliance audits.
 - c. Ensure the independence of the compliance auditor.
 - d. Standardize on a specific compliance audit standard that creates uniform expectations, and enhances the ability to assess the community in a uniform manner.
 - e. All prior audit reports shall be reviewed while conducting any new audits.
 - f. Establish timelines for compliance audits and determine how frequently a compliance audit is required after commencement of services.

⁸ 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

C. Rules of Behavior

All system's rules of behavior shall be in accordance with the FiXs Operating Rules⁹.

1. The FiXs Executive Board shall assign a committee the responsibility of developing a set of FiXs system rules of behavior. These rules shall be based on the FiXs Technical Architecture and Specifications. The rules of behavior shall be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt. Each user shall use this set of rules of behavior or develop their own 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.
2. The rules of behavior shall:
 - a. Clearly delineate the responsibilities and expected behavior of all individuals with access to the system;
 - b. State the consequences of inconsistent behavior or noncompliance;
 - c. Include appropriate limits on interconnections to other systems; and
 - d. Be an appendix to the system's security plan.

D. 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 800-64¹⁰, which describes the tasks in more detail.

1. Initiation Phase
 - a. 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 199¹¹ and NIST SP 800-60¹² provide a guide for this action.
 - b. 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. Development/Acquisition Phase
 - a. 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 *FiXs Operating Rules*

¹⁰ NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*

¹¹ Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (DRAFT)

¹² NIST Special Publication 800-60, *Guide for Mapping Information and Information Types to Security Objectives and Risk Levels* (DRAFT)

- b. 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:
 - o System security environment, (i.e., enterprise information security policy and enterprise security architecture)
 - o Security functional requirements
 - c. 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.
 - d. 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.
 - e. Security Planning – The development of a System Security Plan (SSP) that ensures that, planned or in place, agreed upon security controls are 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).
 - f. 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.
 - g. 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 information system is deployed—these controls are typically management and operational controls.
 - h. 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.
3. Implementation Phase
- a. 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.
- b. 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.
 - c. 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.
 - d. 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.
 - e. Data Protection Requirements – determine the requirement for the protection of sensitive data (such as encryption). Ensure the implementation of data protection requirements.
4. Operation/Maintenance Phase
- a. Configuration Management and Control – 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.
 - b. 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.
 - c. 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.
5. Disposal Phase
- a. 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.
 - b. 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.
 - c. Media Sanitization – ensure that all sensitive data, software, and firmware is deleted, erased, and/or written over as necessary.

- d. 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.

E. Requirements to Authorize Processing

Before a new system can become an operational part of the FiXs Network it shall be evaluated and accredited by the FiXs Executive Board or their designated representative. While a NIST SP 800-37¹³ type of accreditation may at some point in time be desirable, it is not practical at this time due to the time and expense required, and the level of security necessary to protect the systems. The FiXs Executive Board shall accredit a system (authorize it to process as a part of the FiXs Network) if:

1. The operating organization has been accepted as a FiXs Participant.
2. 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).
3. 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.
4. The operating organization has agreed to announced and unannounced audits of their FiXs system (equipment, processes, and personnel).
5. 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.

¹³ NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information System*

3.0 OPERATIONAL CONTROLS

A. Personnel Security

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 most sensitive, sensitive, and least sensitive.

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

- a. *Program Manager*
- b. *Domain Technical Administrator*
- c. *Domain Functional Administrator*

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

- a. *Facility Domain Administrator*
- b. *Facility Administrative Enroller*
- c. *Facility Enroller*
- d. *Facility Verifier*

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

- a. *Authentication Station Operator*

2. Screening

All personnel shall be required to have PIV-1 "equivalent" 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.

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.

4. 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.

5. 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.

B. 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.

1. FiXs Domain Server (FDS)
 - a. Physical Access: The FDS shall be:
 - i. Within a building that is protected from unauthorized access by a guard and/or receptionist or an access control system.
 - ii. Within a room that has access controlled by a locking mechanism.
 - b. Fire Safety:
 - i. The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
 - ii. The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.
 - iii. The room shall be equipped with a manual fire extinguisher and instructions for its use.
 - c. 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.
 - d. Structural Collapse: There shall be no structural damage or decay to the building.
 - e. Plumbing Leaks:
 - i. There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
 - ii. There shall be no plumbing lines running over, adjacent to, or under the FDS.
 - f. Rings of Security Requirements:
 - i. 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.
 - ii. 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.
 - iii. The FDS shall have at least 2 physical rings of security (as described above in "Physical Access.")
 - iv. The FDS shall have at least 2 electronic rings of security.
2. Enrollment Workstation
 - a. Physical Access: The Enrollment Workstation shall be:
 - i. Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
 - ii. Within a room that has access controlled by a locking mechanism.
 - b. Fire Safety:
 - i. The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.

- ii. The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.
- c. 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.
- d. Structural Collapse: There shall be no signs of structural damage or decay to the building.
- e. Plumbing Leaks:
 - i. There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
 - ii. There shall be no plumbing lines running over, adjacent to, or under the Enrollment Workstation.
- f. Interception of Data: Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.
- g. Local Authentication:
 - i. Boot or EPROM password that is changed at least every 90 days.
 - ii. Username/Password for the local domain that is changed at least every 90 days
 - iii. 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).
- h. Rings of Security Requirements:
 - i. 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.
 - ii. 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.
 - iii. The Enrollment Workstation shall have at least 2 physical rings of security (as described above in "Physical Access," more is always better.
 - iv. The Enrollment Workstation shall have at least 1 electronic ring of security.

3. Authentication Workstation

- a. Physical Access: The Authentication Workstation shall be:
 - i. Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
 - ii. In an area that is under the observation of a guard and/or receptionist during normal working hours.
- b. Fire Safety:
 - i. The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
 - ii. The area shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, or equivalent.
- c. 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.
- d. Structural Collapse: There shall be no signs of structural damage or decay to the building.
- e. Plumbing Leaks:
 - i. There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).

- ii. There shall be no plumbing lines running over, adjacent to, or under the Authentication Workstation.
- f. Interception of Data: Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.
- g. Local Authentication:
 - i. Boot or EPROM password that is changed at least every 90 days.
 - ii. Username/Password for the local domain that is changed at least every 90 days
 - iii. 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).
- h. Rings of Security Requirements:
 - i. 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.
 - ii. 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.
 - iii. The Authentication Workstation shall have at least 1 physical rings of security (as described above in "Physical Access."
 - iv. The Authentication Workstation shall have at least 1, but preferably 2, electronic rings of security.

4. FiXs Trust Broker

- a. Physical Access: The FiXs Trust Broker shall be:
 - i. Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
 - ii. Within a room that has access controlled by a locking mechanism.
- b. Fire Safety:
 - i. The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
 - ii. The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.
 - iii. The room shall be equipped with a manual fire extinguisher and instructions for its use.
- c. 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.
- d. Structural Collapse: There shall be no signs of structural damage or decay to the building.
- e. Plumbing Leaks:
 - i. There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
 - ii. There shall be no plumbing lines running over, adjacent to, or under the FiXs Trust Broker.
- f. Interception of Data: Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.
- g. Rings of Security Requirements:
 - i. 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.
 - ii. The FiXs Trust Broker shall have at least 4 rings of security (at least 2 physical and 2 electronic) in total.

- iii. The FDS shall have at least 2 physical rings of security (as described above in "Physical Access.")
- iv. The FDS shall have at least 2 electronic rings of security.

C. 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.

D. 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. 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 800-34¹⁴ 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).

¹⁴ NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*

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:
 - a. Annual test that includes actually switching the system to and bringing up the systems at the support facility.
 - b. Quarterly desk top tests where the responsible parties talk through the actions required to accomplish the COOP or DRP.
 - c. 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 of incidents (e.g., what files and logs shall be kept, who to contact, and when). NIST SP 800-61¹⁵ 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

¹⁵ NIST Special Publication 800-61, *Computer Security Incident Handling Guide*

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:
 - o For more than 30 minutes during normal business hours.
 - o For more than 2 hours during non-business hours.

E. Hardware and System Software Maintenance Controls

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.

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. 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.

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.).

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.

F. Integrity Controls

1. General Requirements

- a. All systems shall be continuously monitored by FiXs Participant personnel to ensure adequate performance of FiXs tasks.

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

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:

- a. All computers shall be automatically scanned on a regular basis where possible.
- b. Scanning software shall be capable of detecting and regularly updating profiles for:
 - i. Traditional .exe and .com viruses
 - ii. Automated hidden software installations (spyware)
 - iii. The presence, regardless of source, of password compromising systems
- c. All anti-virus software shall be subscribed to that software vendor's automatic virus signature system.
- d. 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.
- e. 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.
- f. All diskettes containing executable software (software with .EXE and .COM extensions) shall be write protected wherever possible.
- g. 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.
- h. New commercial software shall be scanned before it is installed as it occasionally contains viruses.
- i. To enable data to be recovered in the event of a virus outbreak, regular backups will be taken by FiXs Participants.
- j. Users will be kept informed of current procedures and policies.
- k. Users will be notified of virus incidents.
- l. FiXs Participant employees will be held directly accountable for any breaches of the Company's anti-virus policies.
- m. Anti-virus policies, procedures and software will be reviewed regularly (at least annually).

G. Documentation

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.

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.

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.

H. Security Awareness & Training

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.

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.

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

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.

5. Help Desk

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

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:

- a. Password policies
- b. Data encryption and key management
- c. Privacy policies
- d. Data preservation and destruction policies
- e. Social engineering prevention
- f. Antivirus policies and procedures
- g. Laptop security
- h. Security event communication protocols

I. Key Management Backup/Recovery

1. Architecture

FiXs architecture should make use of a FiXs approved Security Solution, using Trusted Platform Modules (TPMs) for key storage (see https://www.trustedcomputinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf) or better, ensuring that strong hardware based authentication of the platforms is used.

2. Affected Platforms

Relevant platforms include, but are not limited to:

- a. Enrollment stations
- b. Authentication stations
- c. FiXs Domain Servers
- d. FiXs Trust Broker

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

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.

A. Identification and Authentication

For most systems, identification and authentication (I&A) is the first line of defense. I&A is a technical measure that prevents unauthorized people (or unauthorized processes) from entering a computer system.

Identification is the means by which a user provides a claimed identity to the system.

Authentication is the means of establishing the validity of this claim.

1. Password Management

FiXs requires the use of a password to access the FiXs Trust Broker and DoD TGB, enrollment client, FDS server, and the authentication client machines. Policy here shall be consistent with local domain – company, agency, etc.

2. Password Usage

Must be consistent with local domain.

3. Minimum Password Length

All passwords shall be at least eight characters in length. Due to technology vulnerabilities associated with the use of passwords for authentication, this minimum has been set in excess of the FIPS requirement. Passwords shall be composed of representatives of at least two of the following character sets: upper case English; lower case English; numeric characters; and special characters. It is strongly recommended to use at a minimum three of the character sets.

4. Password Lifetime

All passwords will have a maximum password lifetime of 90 days. Systems shall have an automated mechanism to ensure that users change their passwords at an interval not greater than 90 days. In addition, user IDs are to be suspended after three invalid password attempts.

5. Initial Password

An initial password is a password defined by a system administrator or computer systems security officer and given to a user to enable access. FIPS 112, Section 3.5, Ownership, requires that "personal passwords used to authenticate identity shall be owned (i.e., known) only by the individual who created the private data." Therefore, agency systems shall have the ability to allow new users to change their passwords after initial access to a system. Systems shall be configured to require the user to select a new password after signing on with an initial password. Any operating system or applications system "feature" that would allow a system administrator to view passwords shall be disabled. All system default passwords, including service accounts, shall be changed as soon as possible after system installation and before becoming operational.

6. Password Generation

FIPS 112 states that "Since many user-created passwords are particularly easy to guess, all passwords shall be machine generated using an algorithm that meets the specification in Appendix E.1," (i.e., a random password). Because the use of random passwords introduces a vulnerability of having users write down passwords, systems may require user-selected passwords if the following conditions can be met:

a. User ID Suspension

A user ID is suspended after three invalid password attempts such that manual action by a security administrator is required to reactivate the ID.

b. Password Construction

A restricted password list or algorithmic means (e.g., password masking, required use of special characters, etc.) is used to limit the selection of trivial passwords.

c. Biometrics Controls

Subject to policy of local domain, for logging into the computer

d. Token Controls

Subject to policy of local domain, for logging into the computer

e. Issuing Parties

Issuing Parties (or, Identity Providers) shall maintain the database of users (employees), operators and systems administrators. Failure to properly maintain this database is considered a violation of the terms in the FiXs Operating Rules.

B. Logical Access Controls

1. Administrator Accounts

The "administrator" account of the host operating system shall NOT be used for accessing ANY of the FiXs software, applications, drivers, etc.

2. Monitors

Avoid locating monitors on which you display confidential data close to the outer wall of your building.

Consider the use of a 'flat screen' LCD terminal which omits little, if any radiation.

For confidential applications consider the use of specialized shielding against electromagnetic waves

3. Warning Banner

There MUST be a warning banner at the time of log into the computer, AND at the time the FiXs enrollment/authentication application is initiated.

Sample Banner:

This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority may be prosecuted to the fullest extent of the law. The information, data, and graphics contained in the FiXs/DCCIS are private and proprietary. Access to the information, data, and graphics is with the understanding that it will be held confidential and not used or disclosed without the prior written consent of the owner. Attempts to upload or change information on this service without authorization or to download and copy with the intent to defraud are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act. Use of any robot, spider, web crawler, automated query device, or other automatic device, or manual process to monitor or copy FiXs/DCCIS data or the content contained herein without our prior express written permission is prohibited. Use of any device, software or routine to interfere or attempt to interfere with the proper working of the system or any transaction being conducted by the system is also prohibited.

Each warning banner shall be accompanied by a button which, when selected, acknowledges and gives consent to the content of the banner message.

4. Application Access

Access to the FiXs applications shall be strictly controlled. Only authorized system administrators shall be granted access to maintain the portals, FDS server and/or enrollment and/or authentication machine/s. Only authorized operators shall be granted access to operate the FiXs enrollment application. Only authorized operators shall be granted access to operate the FiXs authentication & cross-authentication applications. The System Administrator shall maintain regular and up-to-date list of current operators. Operators who no longer require, desire access to the system – or those who have terminated their relationship with the system – shall be removed from access within 24 hours.

5. Communications

All communications (between any FiXs client and the server and also between the FDS server and the FiXs Trust Broker) MUST be encrypted with (at least) SSL encryption, or as otherwise specified in the FiXs Operating Rules. Further, appropriate traffic segregation shall be enforced (e.g., preventing non-DoD traffic from crossing through DoD TGBs).

6. System Access

Only authorized personnel shall be granted access to the system. Only authorized System Administrators shall be granted access to system administrator functions and privileges on the FiXs machines. Only authorized FiXs Operators shall be granted access to FiXs functions.

C. Audit Trails

Identity federation shall be predicated upon prior written agreement between the relying and issuing parties. It shall be additionally predicated upon providing notice to the user, obtaining the user's consent, and recording both the notice and consent in an auditable fashion. Providing an auditable record of notice and consent will enable both users and providers to show that notice and consent were provided. In addition, it will document that the consent is bound to a particular interaction. Such documentation will increase consumer trust of the online services. Implementers and deployers of FiXs-enabled technology shall ensure that FiXs-enabled notice and user consent interactions with users are recorded in an auditable manner, as appropriate.

1. System Administrators Responsibility

For Privacy Act compliance, System Administrators shall be responsible for accepting and processing requests for Audit Records. Further, System Administrators may work with appropriate Security, Personnel, Human Resource, and/or Law Enforcement staffs to initiate and/or support investigations requiring the use of Audit Records.

Under "normal operating conditions," Audit Logs shall be reviewed thoroughly at a minimum of once every week to check for transactions that appear inconsistent, anomalous and/or inaccurate. All suspicious conditions shall be investigated.

Under "other than normal operating conditions," the System Administrator shall review audit logs several times each week. All suspicious conditions shall be investigated.

2. Audit Trail Requirements

Audit Trails shall record every transaction. Each transaction shall be recorded, by name of the event, along with date and time (using GMT as a baseline reference). Specific requirements are laid out in the Applications Security Guidelines Document.

a. FiXs Trust Broker Transactions

The following events shall be recorded by the FiXs Trust Broker.

- i. All incoming and outgoing transactions, by date and time (in GMT format), along with the name of the source/destination, and a status indication, reflecting whether the transmission was sent/received successfully or not.
- ii. Updates to Organization Code tables, Country Code tables, or any other FiXs - related dynamic tables shall be recorded.
- iii. All outgoing transmissions, intended to update tables on its Participant FDS servers.
- iv. Adding, deleting and/or modifications to list of organizations participating in FiXs.

b. Reporting Options

Audit Trails shall provide an option where statistics can be reported and/or collected according to the following general guidelines:

- i. Daily, weekly, monthly statistics
- ii. By Operator – either enrollment operator or authentication operator, or by a particular system administrator
- iii. By individual ID#
- iv. By specific remote site
- v. All remote transactions
- vi. All local transactions

- vii. By number of (un)successfully retrieved transactions
- c. Audit Trail Security

Audit Trails shall be available only to selected privileged users. Audit Trails shall not be available to the general public.

D. HSM Security Level Requirements

1. The HSM used shall be certified to FIPS 140 level 2, Security Level 3 or greater. The use of an HSM allows the various servers to deliver the highest security and data integrity for key migration services.
2. Key management backup/recovery procedures shall be developed and used, consistent with FiXs Security Guidelines Section III Paragraph I.

E. Operating System Security Requirements

1. 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.
2. 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>.

APPENDIX I 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*
 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*
 27. *Federal Information Processing Standards (FIPS) Publication 201 (DRAFT)*
- 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 <http://www.dtic.mil/whs/directives/corres/xml/d85001x.xml#cr7#cr7>
 40. National Security Telecommunications and Information Systems Security Instruction Number 4009
 41. NSA, Security Recommendation Guides, <http://nsa1.www.conxion.com/win2k/index.html>
 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, https://www.trustedcomputinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf
 50. Windows 2003/XP/2000 Addendum Version 5, Release 1 Developed by DISA for the DOD

APPENDIX II 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 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.

[NOTE: Current approved C&A checklist should be appended]