



Implementation Advanced Planning Document



February 2010

California Health and Human Services Agency
Office of Systems Integration



TABLE OF CONTENTS

1. PROJECT INTRODUCTION 1-1

 1.1. Status and Background..... 1-1

2. PROJECT MANAGEMENT PLAN..... 2-1

 2.1. Introduction..... 2-1

 2.2. References 2-1

 2.3. Definitions 2-2

 2.4. Standards 2-2

 2.5. System M&O Overview 2-3

 2.6. Contract Amendment Overview 2-3

 2.7. System M&O Processes 2-3

 2.8. IHSS Addition to SFIS Processes 2-4

 2.9. System M&O Management 2-4

3. RISK MANAGEMENT PLAN..... 3-1

 3.1. Purpose..... 3-1

 3.2. Referenced Documents 3-1

 3.3. Definitions..... 3-1

 3.4. SFIS Risk Management 3-2

 3.5. Sample Reports And Forms 3-2

 3.6. Risk Management Database – 3-2

 3.7. Risk Management Database – Risk Radar™ 3-2

4. PROJECT REQUIREMENTS 4-1

 4.1. System Overview 4-1

 4.2. Reason For Proposed Change 4-2

 4.3. Proposed Project Change..... 4-2

 4.4. Impact of Proposed Change..... 4-2

5. BUDGET AND COST ALLOCATION METHODOLOGY 5-1

 5.1. IHSS Costs..... 5-1

 5.2. Yearly Costs (FFY)..... 5-4

 5.3. Cost Allocation Plan..... 5-4

6. ALTERNATIVES ANALYSIS 6-1



6.1. Introduction..... 6-1

6.2. Analysis..... 6-1

6.3. Conclusion..... 6-1

7. SYSTEM LIFE EXPECTANCY 7-1

8. SECURITY, BACKUP, AND CONTINGENCY PLANS 8-1

8.1. System Security..... 8-1

8.2. Physical Security Procedures8-11

8.3. Backup and Recovery.....8-12

9. TRAINING PLAN 9-1

9.1. Purpose..... 9-1

9.2. County Training 9-1

9.3. Staff Training..... 9-1

10. TRANSITION-IN SCHEDULE..... 10-1

ATTACHMENTS

ATTACHMENT I Master Project Plan

ATTACHMENT II Risk Management Plan

ATTACHMENT III Training Plan

ATTACHMENT IV..... Transition-In Schedule

ATTACHMENT VContract



1. PROJECT INTRODUCTION

The Office of Systems Integration (OSI) Statewide Fingerprint Imaging System (SFIS) Project Office is submitting this Implementation Advance Planning Document (IAPD) to request funding approval for the implementation/maintenance and operation of its automated fingerprint imaging system for the In-Home Supportive Services (IHSS) program.

1.1. STATUS AND BACKGROUND

1.1.1. Statewide Fingerprint Imaging System

SFIS was created in response to Senate Bill 1780 (Chapter 206, Statutes of 1996) which required applicants and recipients of the California Work Opportunity and Responsibility to Kids (CalWORKs) and Supplemental Nutrition Assistance Program (SNAP) programs to be fingerprint imaged as a condition of eligibility. The law exempts dependent children and persons who are physically unable to be fingerprint imaged. The requirement for fingerprint imaging is intended to deter and detect duplicate aid fraud in the CalWORKs and SNAP programs. In addition, 24 counties use the system to fingerprint image and match prints for their General Assistance/General Relief (GA/GR) population.

The California Department of Social Services (CDSS) and the OSI are mandated to maintain SFIS. OSI managed the development and implementation of SFIS and currently manages the Maintenance and Operations (M & O) services of the system on behalf of the CDSS.

The State of California executed a contract with Electronic Data Systems (EDS) for the design, development, implementation, and operation of the SFIS. The initial contract term ran from September 7, 1999 to September 6, 2003. Following a five month development period, implementation of SFIS began in March 2000 and was completed in December 2000.

The contract was extended to September 6, 2005 as provided under the terms of the contract. Due to delays in the re-procurement efforts, the State further extended the current contract to December 31, 2007, and has issued a Non Competitive Bids (NCB) extending SFIS service under a new contract to August 2009. On September 1, 2009 a new contract was procured and executed to provide maintenance and operations services for the eight year contract period. This contract requires the winning contractor to refresh all hardware and software to current supported versions.

In July of 2009, legislation was passed that required the California Department of Social Services (CDSS) to implement fingerprint imaging on new IHSS recipients by April 1, 2010. The existing IHSS caseload will be fingerprint imaged at reassessment.



2. PROJECT MANAGEMENT PLAN

2.1. INTRODUCTION

The Master Project Plan (MPP) defines the resources, responsibilities, and major processes for M&O for the existing SFIS. The MPP provides high-level guidance and is supplemented with separate, more detailed plans and procedures, which are identified throughout the MPP. The MPP and the supplemental plans have been developed incrementally as information is available. The MPP and the supplemental plans are living documents and are updated as needed.

OSI SFIS Project Management Office/ Quality Assurance (PMO/ QA) staff will update the MPP periodically as a result of continuous process improvement efforts and changes in the Project status.

The SFIS has been in M&O since December 2000. The MPP is a required document and has been in production use for several years. We have provided the current version of the documents including the revision history as an attachment. A summary of this document has been provided in the body of the IAPD for your convenience. The complete SFIS Master Project Plan Version 3.0) may be found in ATTACHMENT I.

2.2. REFERENCES

The following documents were used as reference material in the development of the SFIS Master Project Plan.

- IEEE Standard 1062-1998: IEEE Recommended Practice for Software Acquisition, December 8, 1998, Reaffirmed September 11, 2002.
- IEEE/EIA Guide 12207.1-1997: Software Life Cycle Processes—Life Cycle Data, April 1998.
- Master Project Plan Outline,
[http://www.bestpractices.cahwnet.gov/New_web/Primary Processes/2-Planning/M3-Plans Approved/Master Project Plan/mpp_outline.htm](http://www.bestpractices.cahwnet.gov/New_web/Primary%20Processes/2-Planning/M3-Plans%20Approved/Master%20Project%20Plan/mpp_outline.htm).
- CMIPS Master Project Plan, June 19, 2001.
- CWS-CMS Maintenance and Operations Procurement and Transition Support Services Project Management Plan, October 13, 2000.
- WDTIP Project Management Plan, December 13, 2000.
- A Guide to the Project Management Body of Knowledge (PMBOK), William R. Duncan, PMI Standards Committee, Project Management Institute, 2000.
- OSI Best practices Master Project Plan Template, January 20, 2009,
<http://www.bestpractices.osi.ca.gov/sysacq/documents/Master%20Project%20Management%20Plan.doc>.



2.3. DEFINITIONS

A complete list of terms used in this PMP is included in the complete SFIS Master Project Plan: ATTACHMENT I.

Additional terms and definitions, particularly acronyms in use at the State of California can be found in the State of California Telephone Book and OSI's Organization Chart.

2.4. STANDARDS

The list of standards below includes those applicable to system acquisition. Some of the standards listed below may not be directly applicable to SFIS but all have some level of relevance. In addition, standards are included that presume the State will secure the services of an oversight provider; although this may be unnecessary under the Office of the Chief Information Officer (OCIO) Information Technology Project Oversight Framework (see reference below). Possible applicable standards to SFIS include:

- IEEE Standard 1062-1998: IEEE Recommended Practice for Software Acquisition, December 8, 1998, Reaffirmed September 11, 2002.
- IEEE/EIA Guide 12207.1-1997: Software Life Cycle Processes—Life Cycle Data, April 1998.
- A Guide to the Project Management Body of Knowledge (PMBOK), William R. Duncan, PMI Standards Committee, Project Management Institute, 2000.
- IEEE Standard 1465-1998: IEEE Standard Adoption of International Standard ISO/IEC 12119: 1994(E) Information Technology — Software Packages—Quality Requirements and Testing, June 25, 1998.
- IEEE Standard 730-2002: IEEE Standard for Software Quality Assurance Plans, June 25, 2002.
- Criminal Justice Information Services (CJIS), Electronic Fingerprint Transmission Specification, January 1999, Department of Justice, Federal Bureau of Investigation, CJIS-RS-0010 (V7).
- Annex C, Finger Imaging, AAMVA National Standard for Driver's License/Identification Card, 2000-06-30, American Association of Motor Vehicle Administrators,
- IEEE Standard 1012-2004: IEEE Standard for Software Verification and Validation, March 9, 2004.
- IEEE Standard 1540-2001: IEEE Standard for Software Life Cycle Processes — Risk Management, March 17, 2001.
- IEEE Standard 1059-1993: IEEE Guide for Software Verification and Validation Plans, December 2, 1993.



- Transition of IT Project Review, Approval and Oversight Responsibilities from the Department of Finance to the Office of the State Chief Information Officer, and Information Technology Budgeting Guidelines, Office of the State Chief Information Officer (OCIO), Budget Letter 08-06, March 13, 2008.

2.5. SYSTEM M&O OVERVIEW

OSI's SFIS management and staff manage the activities of the SFIS Contractor to provide SFIS system services to the Project's end users, both State and County, and takes direction from the CDSS, particularly in the area of program priorities and requirements. The components of the M&O support for SFIS include human, technical, and procedural resources. Many of these components are the same for the Procurement Project. These components include:

- SFIS Project Organization;
- Roles and Responsibilities;
- Schedule; and
- Tools.

Each of these components is described in its own section of the SFIS Master Project Plan: ATTACHMENT I.

2.6. CONTRACT AMENDMENT OVERVIEW

- Planning for adding the IHSS program to the SFIS has commenced.

2.7. SYSTEM M&O PROCESSES

A variety of business processes support the M&O Phase of SFIS. These include:

- Risk Management;
- Communications;
- Configuration Management;
- Quality Assurance;
- Deliverable Review;
- Training;
- Disaster Recovery;
- Contract Management;
- Transfer Plan; and
- Transition-In.

Each of these general sets of business process is described in separate plans. Each of these plans is described in the SFIS Master Project Plan: ATTACHMENT I.



2.8. IHSS ADDITION TO SFIS PROCESSES

Planning for adding the IHSS program to the SFIS has begun. System processes for adding the IHSS program to the SFIS have not yet been completely determined.

2.9. SYSTEM M&O MANAGEMENT

System M&O management contains those plans necessary to effectively manage the M&O Phase of SFIS, and include:

- Communication Plan;
- Contract Management Plan;
- Metrics / Evaluation Plans;
- Configuration Management Plan;
- Risk Management Plan;
- Deliverable Review Plan;
- Quality Assurance Plan;
- Transition-In Plan;
- Technology Refreshment Plan;
- Raw Image (Bitmap) Retrieval and Storage Plan;
- Contingency Plan;
- Fingerprint Database Quality Assessment;
- Capacity Planning Report;
- Portable Workstation Maintenance Plan;
- Security Assessment;
- Testing Approach Document; and
- Deviation Policy.

Each of these plans is described in the SFIS Master Project Plan: ATTACHMENT I.



3. RISK MANAGEMENT PLAN

3.1. PURPOSE

This document describes the OSI Risk Management Plan (RMP) for the SFIS Project. The plan is used for SFIS M&O, as well as adding the IHSS program to the SFIS activities. The RMP defines the Risk Management process to be followed by the SFIS Project, including the roles and responsibilities of OSI's SFIS PMO/ QA support as well as the contractor when necessary.

OSI's SFIS PMO/ QA staff will update the RMP periodically as a result of continuous process improvement efforts and changes to applicable standards.

The SFIS has been in M&O since December 2000. The RMP is a required document and has been in production use for several years. We have provided the current version of the document including the revision history as an attachment. A summary of this document has been provided in the body of the IAPD for your convenience. The complete SFIS Risk Management Plan is ATTACHMENT II-RMP.

3.2. REFERENCED DOCUMENTS

The following documents are a sample of those used as reference material in the development of the SFIS Risk Management Plan.

- IEEE Standard 1540-2001: IEEE Standard for Software Life Cycle Processes — Risk Management, March 17, 2001.
- IEEE Standard 1012-1998: IEEE Standard for Software Verification and Validation, March 9, 1998.
- Taxonomy-Based Risk Identification, Marvin J. Carr, Suresh L. Konda, Ira Monarch, F. Carol Ulrich, and Clay F. Walker, Software Engineering Institute, June 1993.

3.3. DEFINITIONS

Terms used in this RMP are consistent with and in many cases are the exact definitions used in IEEE Standard 1540-2001. Definitions appear in Section 3 of the IEEE Standard.¹

Definitions for other key terms, developed for this RMP, are presented below. The Project Management Institute (PMI) and the Software Engineering Institute (SEI) were also used as resources in developing the following definitions, specifically:

- *A Guide to the Project Management Body of Knowledge, 2000.*
- *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, 1997, Version 1.0, 1997.*

¹ IEEE Std 1540-2001, p. 3-4.



- *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, Version 1.02, 1999.*

Additional terms and definitions, particularly acronyms in use at the State of California can be found in the State of California Telephone Book and OSI's organization Chart.

3.4. SFIS RISK MANAGEMENT

Risk management is a key discipline for making effective decisions and communicating the results within concerned organizations. The purpose of risk management is to identify potential managerial and technical problems before they occur so that actions can be taken that reduce or eliminate the likelihood and/or impact of these problems should they occur. It is a critical tool for continuously determining the feasibility of project plans, for improving the search for and identification of potential problems that can affect information technology systems or software life cycle activities and the quality and performance of software products, and for improving the active management of projects.

SFIS risk management is based on a discipline built upon the framework of the SEI Risk Management Paradigm. OSI SFIS staff, CDSS staff and contractor staff work together with respect to M&O risk management in team risk management to anticipate and avoid problems by managing project risks. Team risk management establishes a cooperative working environment throughout all levels of the project that gives everyone in the project the ability and motivation to look ahead and handle risks before they become problems.

3.5. SAMPLE REPORTS AND FORMS

A complete list of reports and forms can be found in Section 5 of the SFIS Risk Management Plan: ATTACHMENT II-RMP.

3.6. RISK MANAGEMENT DATABASE –

Sample screen prints were taken from the Project Administration and Control System (PACS) and illustrate the capabilities of the Risk Management Database. These screen prints can be found in Section 6 of the SFIS Risk Management Plan: ATTACHMENT II-RMP.

3.7. RISK MANAGEMENT DATABASE – RISK RADAR™

Sample screen prints were taken from the Risk Radar™ and illustrate the capabilities of the Risk Management Database. Risk Radar™ screen prints can be found in Section 7 of the SFIS Risk Management Plan: ATTACHMENT II-RMP.



4. PROJECT REQUIREMENTS

4.1. SYSTEM OVERVIEW

4.1.1. Existing System

The existing SFIS Central Site houses database servers, process-coordinator workstations, and the MorphoTrak (formerly known as Motorola/Printrak) Automated Fingerprint Identification System (AFIS). There are approximately 275 SFIS workstations located in county welfare offices statewide with the capability to capture images, and another approximately 100 workstations supporting various management and administrative tasks, including training. The Wide Area Network (WAN), the Local Area Network (LAN) within the counties and the Central Site LAN is provided by The Office of Technology Services (OTech).

Currently, the system processes approximately 6000 fingerprint transactions per day. Our current database size is approximately five Million records (ten million fingerprint images).

SFIS searches for proof of duplicate records by matching a client with fingerprints on record for CalWORKs and/or SNAP and depending on the county, GA/GR. The System does not:

- Detect other types of payee fraud;
- Interface to non-welfare systems; or
- Provide Eligibility Records Management or Case History Information.

A detailed description of the existing system can be found in SFIS RFP OSI 2046 (http://www.sfis.ca.gov/SFIS_RFPdocs.html).

4.1.2. Changes to Existing System

The In-home Supportive Services (IHSS) program is supported by the counties in about 100 sites statewide. New applicants average about 8,000 per month with an existing case load of 430,000 recipients. The program has about 2,400 active caseworkers that need access to the system. Changes to the existing system require changes to the Prime Vendor contract, the current SFIS network and State staffing level. The changes are as follows:

- The current SFIS Prime Vendor contract was executed September 1, 2009 and will be in place for eight years. In order to accommodate the IHSS program and its unique imaging requirements, the contract needs to be amended in the following areas:
 - Increase the number of concurrent users supported.



- Increase the number of workstations supported.
- Add a portable handheld fingerprint/photo capture device and backup fingerprint ink/card camera kit.
- The IHSS program houses its county caseworkers in about 100 sites statewide. The SFIS currently has existing circuits to about half of these sites. Some of these existing circuits will have to be upgraded to accommodate the increase in network traffic. The other half of the sites are new to SFIS, so new circuits and networking hardware need to be installed. We also need to add additional network hardware in each of the IHSS offices and the SFIS Central site to accommodate the portable handheld scanner.
- Two additional staff is needed to provide support to the 2400 caseworkers and hardware for 100 sites. These two new positions will provide support to the SFIS Training Coordinator by creating and maintaining the SFIS Web Based Training program, providing classroom training, and network support,

4.2. REASON FOR PROPOSED CHANGE

In July of 2009, legislation was passed that requires the fingerprint imaging of new IHSS recipients beginning April 1, 2009. This legislation also requires that the 430,000 existing recipients be fingerprinted at reassessment. The law further states that the fingerprints will be captured in the homes of the recipients not in the county offices like SFIS for Food Stamp and CalWORKS.

4.3. PROPOSED PROJECT CHANGE

Provide additional project funding for the IHSS program. The funding will be used to purchase additional hardware, support services, network connectivity and staffing to support the program.

4.4. IMPACT OF PROPOSED CHANGE

CMS approval of this IAPD would result in federal reimbursement for a beneficial program.



5. BUDGET AND COST ALLOCATION METHODOLOGY

This section details cost estimates for the addition of the IHSS program into the SFIS.

Based on the cost allocation, the State's cost share for the Project is expected to total \$21,573,858 for the remaining SFIS Prime Vendor contract period, while the federal share is expected to total \$20,026,141. No inflationary factor has been applied for *any* costs.

Major subsections which outline cost projections for the SFIS system follow.

- Subsection 5.1 outlines the onetime and ongoing M&O costs associated with adding the IHSS population to the SFIS the system.
- Subsection 5.2 presents the total costs of the system by federal fiscal year.
- Subsection 5.3 describes the methodology used to allocate the costs of the new system between State, and federal funding sources.

5.1. IHSS COSTS

This section addresses costs for adding the IHSS population to the SFIS. Costs are segmented into the following categories:

- Contractor Services;
- SFIS Personnel and Operating Expense and Equipment (OE&E);
- SFIS Network

5.1.1. Contractor Services

Costs have been estimated to add the IHSS recipients to the current SFIS Prime Vendor contract. These costs include both services and equipment necessary to process all the IHSS recipients in their homes. Total contractor costs include estimates for the following:

- SFIS Desktop Workstations – There are 100 IHSS sites located statewide. At least one SFIS Desktop is required at each of these sites. Each of these workstations will perform the following functions:
 - Print the match responses.
 - Administer the security functions.
 - Resolve any unexpected results.
 - Refer Match responses to Fraud
 - Upload transactions to the SFIS Central Site



- SFIS Handheld Workstations – The Legislation requires that the recipients be imaged in their homes. We have determined that the current SFIS portable equipment would be cumbersome to enroll clients in their homes. They were designed to perform enrollments for outreach/disaster type scenarios. The proposed handheld workstation provides the same functionality as the current SFIS portable workstation but in a more compact, rugged and portable package.
- HPES Integration – These costs include the following
 - Integrate the IHSS population into the SFIS.
 - Integrate the handheld device into the SFIS application.
 - Modify the SFIS application to include processing for IHSS
 - Maintain the hardware.
 - Provide Help Desk Services to an additional 2,400 caseworkers.

Total costs for contractor services:

	FFY 9/10	FFY 10/11	FFY 11/12	FFY 12/13	FFY 13/14	FFY 14/15	FFY 15/16	FFY 16/17 *	Total
SFIS Desktop	575,000	300,000	300,000	300,000	300,000	300,000	300,000	275,000	2,650,000
HandHelds	5,450,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000	1,100,000	13,750,000
HP Integration	1,700,000	800,000	800,000	800,000	800,000	800,000	800,000	733,333	7,233,333
Total	7,725,000	2,300,000	2,300,000	2,300,000	2,300,000	2,300,000	2,300,000	2,108,333	23,633,333

* Prime Vendor contract ends August 31, 2017

5.1.2. SFIS Personnel and Operating Expense and Equipment

This section describes the additional costs for SFIS personnel, and the Operating Expense and Equipment (OE&E) costs. This APD requests two new SFIS positions to staff the project for implementation of the SFIS for IHSS recipients. Adding the IHSS to the statewide imaging requirement will, at a minimum, add 2,400 caseworkers and increase the number of supported workstations by at least 200 percent. Below is a description of the requested positions.

SFIS Moves, Adds and Changes (MAC) Coordinator/SFIS Trainer (SISA – 1.0 PY)

The SFIS MAC Coordinator/SFIS Trainer is responsible for coordinating county requests for changes in office locations, adding new sites and other changes in the SFIS sites. They will also provide training (classroom and on-site training) to new and existing SFIS users. Additional responsibilities include the following:



- Upon receipt of a county MAC request independently analyze requests to determine county requirements related to the change in service. Independently coordinate and oversee network/vendor equipment, repair, installation, de-installation, and changes, circuit moves, adds, deletes and changes to ensure county needs and requirements are met.
- Complete installation of network connectivity equipment and computer hardware at SFIS county sites. Troubleshoot network or network hardware problems at county sites. When appropriate, this task will also include responding to help desk calls that cannot be resolved by the first level help desk staff.
- Performs physical site assessment and LAN/WAN assessment.
- Independently monitor and document vendor performance to ensure contractual and service level agreement obligations with OSI are met.
- Deliver end-user training, as well as ongoing evaluation of the overall SFIS training program.
- Work with SFIS Training Coordinator to maintain and update the SFIS Training program.

SFIS Webmaster/ SFIS MAC Analyst (SISA – 1.0 PY)

The SFIS Webmaster/SFIS MAC Analyst is responsible for the SFIS Website, SFIS Web Based Training modules and works with the SFIS MAC Coordinator to complete county MAC requests. Additional responsibilities include the following:

- Maintain and enhance the current SFIS website and SFIS Web Based Training modules.
- Work with SFIS Training Coordinator to maintain and update the Web Based Training program.
- Upon receipt of a county MAC request independently analyze requests to determine county requirements related to the change in service. Independently coordinate and oversee network/vendor equipment, repair, installation, de-installation, and changes, circuit moves, adds, deletes and changes to ensure county needs and requirements are met..
- Complete installation of network connectivity equipment and computer hardware at SFIS county sites. Troubleshoot network or network hardware problems at county sites. When appropriate, this task will also include responding to help desk calls that cannot be resolved by the first level help desk staff.
- Perform physical site assessment and LAN/WAN assessment.
- Independently monitor and document vendor performance to ensure contractual and service level agreement obligations with OSI are

Total costs for additional personnel:



	FFY 9/10	FFY 10/11	FFY 11/12	FFY 12/13	FFY 13/14	FFY 14/15	FFY 15/16	FFY 16/17 *	Total
Personnel	250,000	200,000	200,000	200,000	200,000	200,000	200,000	183,333	1,633,333

* Prime Vendor contract ends August 31, 2017

5.1.3. SFIS Network

This section describes the additional costs for the SFIS network. An additional 100 IHSS sites will be added to the existing SFIS network managed by OTech. OTech is responsible for the design, engineering, implementation, and operation of the SFIS WAN and for the SFIS portion of the LANs. The SFIS project team determines the WAN and LAN specifications based on SFIS application requirements. From these specifications, OTech procures equipment, provides data circuits, and manages the installation of the data service. Once installed and operational, OTech is responsible for ongoing monitoring, support, and maintenance of the WAN and SFIS portion of the LANs. The following costs contain both onetime costs for installation and upgrading circuits and ongoing monthly charges:

	FFY 9/10	FFY 10/11	FFY 11/12	FFY 12/13	FFY 13/14	FFY 14/15	FFY 15/16	FFY 16/17 *	Total
Network	2,500,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	1,833,333	16,333,333

* Prime Vendor contract ends August 31, 2017

5.2. YEARLY COSTS (FFY)

For purposes of specific *year-by-year* budgeting, the following spreadsheets are also included. These spreadsheets itemize the same set of cost categories and cost items, but correspond directly to the year-by-year costs included in the selected contractor's price proposal. As a result, the costs shown in these spreadsheets will fluctuate annually depending on the occurrence of such events as technical refreshment.

	FFY 9/10	FFY 10/11	FFY 11/12	FFY 12/13	FFY 13/14	FFY 14/15	FFY 15/16	FFY 16/17 *	Total
Contractor Services	7,725,000	2,300,000	2,300,000	2,300,000	2,300,000	2,300,000	2,300,000	2,108,333	23,633,333
Personnel	250,000	200,000	200,000	200,000	200,000	200,000	200,000	183,333	1,633,333
Network	2,500,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	1,833,333	16,333,333
Total	\$10,475,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,124,999	41,599,999

* Prime Vendor contract ends August 31, 2017

5.3. COST ALLOCATION PLAN

The purpose of the CAP is to distribute the costs of the SFIS Project across each funding agency in accordance with current federal and State funding agreements. The goal of the plan is to achieve an equitable distribution of costs based on the functionality and usage of the system. The methodology employed for the SFIS CAP is described below.

5.3.1. Cost Allocation Methodology

The basic tenet of the cost allocation methodology for the SFIS Project is to distribute costs in such a way that the benefiting program is charged directly for the support provided for that program. If a single program benefits from the support



then 100 percent of the costs associated with that support are charged to that program. If more than a single program benefits from a support function then the benefiting programs share the cost based on the percentage of the individuals (person count) represented by each program. The OSI tracks each automation project by establishing unique cost centers for each project. Via interagency agreements, CDSS reimburses all costs identified to these cost centers by project. These cost centers receive an appropriate allocation of overhead and project management cost in conformance with OSI's federally approved CAP. OSI invoices to CDSS reflect costs allocated in conformance with their federally approved CAP and federal requirements contained in OMB A-87 for cost allocation of public assistance programs.

5.3.2. Funding Ratios

This chart reflects the funding ratios for the SFIS implementation for the IHSS.

	State	Reimbursement
FY 2009/10	54.02	45.98
FY 2010/11	51.33	48.67
>FY 2011/12	51.33	48.67

CDSS updates the funding ratios annually by identifying the Personal Care Services Program (PCSP)/IHSS Plus Option (IPO) and Residual caseloads and calculating corresponding percentages. The categories of that report include a portion of the IHSS programs' federally-eligible recipients under the state-only IHSS Residual program. Through the use of a separate report with an identifier that provides an accurate count of the Residual population, a calculation is subsequently made to determine the cost and number of recipients in the original report under the IHSS Residual program who should be identified as federally-eligible.

The following chart shows the Title XIX Reimbursement and State share of cost for the duration of the SFIS Prime Vendor Contract.

	FFY 9/10	FFY 10/11	FFY 11/12	FFY 12/13	FFY 13/14	FFY 14/15	FFY 15/16	FFY 16/17 *	Total
State	\$5,597,397	\$2,309,850	\$2,309,850	\$2,309,850	\$2,309,850	\$2,309,850	\$2,309,850	\$2,117,361	\$21,573,858
Title XIX Reimbursement	\$4,877,603	\$2,190,150	\$2,190,150	\$2,190,150	\$2,190,150	\$2,190,150	\$2,190,150	\$2,007,638	\$20,026,141
Total	\$10,475,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,500,000	\$4,124,999	\$41,599,999

* Prime Vendor contract ends August 31, 2017



6. ALTERNATIVES ANALYSIS

6.1. INTRODUCTION

The Alternatives Analysis of fingerprinting the IHSS recipients demonstrates that the only option available was to use the SFIS to satisfy the requirement..

In the past, CDSS was asked to look at alternatives for the SFIS but neither of the alternatives met all the legislatively mandated requirements:

1. Moving the Fingerprint System to the Department of Justice.
2. Using the Department of Motor Vehicles (DMV) fingerprints and photos.

6.2. ANALYSIS

1. The regulations that created the SFIS prohibit any sharing with law enforcement agencies unless they are investigating duplicate aid fraud in SNAP or CalWORKS.
2. Federal legislation was enacted requiring the DMV to implement a more rigorous process in the application for driver's licenses and Identification cards. Once a system meeting these requirements are in place and the entire state's caseload is converted, a hybrid system could be created to allow the state to use DMV's fingerprints/photos where available. .
3. The SFIS is the only civil fingerprint system in the State of California that meets the requirements in the legislation. In fact, the SFIS already has network connectivity to half the offices that houses IHSS caseworkers.

6.3. CONCLUSION

With April 1, 2010 deadline rapidly approaching; the State concluded that it was in the State's best interest to add the IHSS recipients to the existing SFIS system.



7. SYSTEM LIFE EXPECTANCY

The SFIS requires that all components incorporated within the system utilize advanced, but proven technologies. Hardware and software used in support of the SFIS application are required to be technologically advanced at the point of installation. Additionally, this hardware and software, especially the AFIS and associated components, will conform to internationally recognized standards. With the current rate that technological advances are being achieved, systems quickly become obsolete. To maintain system longevity and performance, hardware and software must remain within industry standard levels. OSI and CDSS believe that the system's life expectancy can be augmented based on two important factors:

1. **Scheduled Technology Refreshment.** The SFIS hardware and software will be refreshed with manufacturer supported hardware, software or upgrades as often as every year for any or all components and at a maximum of every five years for any remote workstation component. The scheduled refreshment is in addition to any required replacements of failed equipment that may occur during M&O. The Contractor will produce a SFIS Technology Refreshment Plan, annually for the next contract year. The objective of the SFIS Technology Refreshment Plan is to ensure that all components used in SFIS are currently supported by their manufacturer or developer, and that SFIS complies with all current applicable fingerprint standards. SFIS Technology Refreshment Plans shall describe the Contractor's plans to assure that:

- All SFIS Central Site and Remote Workstation hardware components are still being supported, by the manufacturer.
- All SFIS software including operating systems, database management systems, and compilers are currently supported, by their developer.
- The SFIS complies with all current applicable fingerprint standards and best practices.

The SFIS Technology Refreshment Plan in the fifth contract year shall include complete replacement of remote workstation hardware and software. Central Site hardware and software shall be refreshed at the option of the State each year. The required Transition-In Plan assures that current Central Site hardware and software will be replaced with new hardware and supported software. Adherence to appropriate standards is required by SFIS. For example, The Technology Refreshment Plans shall include storage fingerprint images in the "Biometric Specific Memory Block" of the Common Biometric Exchange File Format (CBEFF), as currently defined in NIST "Common Biometric Exchange File Format (CBEFF)", January 3, 2001, NISTIR 6529 or the most recent ANSI/NIST version of CBEFF. Provision is made for the future inclusion of minutiae files in the SFIS CBEFF files using the emerging ISO/IEC 19794-2 standard.



- 2. Modular Application Architecture.** The SFIS uses software and hardware that is designed for scalable application processing, allowing for the deployment of required processing power as needed. The net result is a technical architecture that is cost-effective to implement, operate, and refresh, without compromising the system's usability. The proposed application architecture divides the core business workload into independently manageable modules designed to support a common, redesigned, business model. This feature will allow SFIS to be able to take advantage of the extra flexibility of the architecture. Since only the pieces of the system that are being changed need to be unavailable to the end user, maintenance and upgrades to systems and application software can often be performed with very little application downtime. Furthermore, the SFIS architecture will minimize the impact of required modifications and changes by reducing the number of affected programs and data structures. Additionally, the SFIS architecture permits processing by end users using remote workstations when Central Site and/or network services are unavailable through Stored Transaction processing. SFIS architecture ensures that the State will be well positioned to migrate to new tools during the system's lifecycle as they become available and are proven effective.

The State fully expects that these factors will combine to extend system life expectancy to at least 13 years after the next contract award. This is based on the life span of the existing SFIS, first procured in 1999 with no provision for technology refreshment that is still in production in 2010.

The current SFIS contract is for eight years. This provides SFIS services with eight years of operation. At the time of contract expiration SFIS will have current hardware and software thanks to the required technology refreshment. It is reasonable to assume that this hardware and software will continue to be of use for the next eight years based on experience of the current SFIS. SFIS will continue to be modified with the most advanced technology and expertise available today, and be continually refreshed over the life of the new contract.



8. SECURITY, BACKUP, AND CONTINGENCY PLANS

Major information systems, such as SFIS, require extensive safeguards to protect the integrity of the program administered and to prevent unauthorized access to the SFIS system or its information. First, the system must safeguard data and processing capability while providing effective access control to SFIS data and systems software. The system must incorporate elements for maintaining program integrity to ensure the fiscal capabilities of the system are not compromised. Second, it must ensure that the system itself is physically secure and protected from abuse and potential fraud. Third, adequate back-up and recovery features are required to ensure the service delivery function can continue in cases of system unavailability and the system can be reconstructed in the event of a disaster. The existing SFIS satisfies these requirements. Enhanced security features will be implemented when a new M&O contractor is selected and are described in this document.

SFIS was also cognizant of the requirements to meet both State and Federal regulations related to security, confidentiality, and auditing during the M&O phase of the project. SFIS has incorporated into its solution, compliance with the specifications of the following publications:

- Automatic Data Processing Physical Security and Risk Management (federal Information Processing Standards, Pub 31),
- Computer Security Guidelines for Implementing the Privacy Act of 1974 (federal Information Processing Standards, Pub 41), and
- Guidelines for Security of Computer Applications (Federal Information Processing Standards, Pub 73).

8.1. SYSTEM SECURITY

Security considerations were of paramount importance when initially implementing SFIS. SFIS used the following security methodology, which was based on a combination of experience and industry best practices, as a foundation for making security-related decisions for the SFIS Project.

- Least Privilege. Allow an entity only the access required to perform its tasks.
- Defense in Depth. Use multiple security measures to ensure that failure of one system or process does not result in total compromise.
- Failsafe Stance. Security systems that fail close access points (like a circuit breaker) instead of leaving them open.
- Default Deny. Deny that which is not expressly permitted.
- Universal Participation. Users cannot choose to bypass security systems and mechanisms (e.g., by alternate paths).



- Diversity of Defense. Use a variety of types of security systems to protect the environment.
- Simplicity. Keep security as simple as possible to aid understanding of the mechanisms and to avoid errors in configuration.
- Separation of Duties. Separate administration and security functions at all times. It is unreasonable to expect effective security and effective systems administration when a single organization or individual performs both functions.

8.1.1. Security Terms

The SFIS project was built on architecture with a layered approach to address overall security within the environment. The SFIS security approach was structured according to a standard security model that addresses the following processes:

- Identification and Authentication. This is the process of verifying a user's identity through any one of several means, and based on that identify, providing the user a specific level of access to the system.
- Access Control. This is the process of granting a user or application the level of information and resources required for their job or business function.
- Physical Security. This is the process of providing a physically secure environment for all resources and assets.
- Confidentiality. This is the process of verifying that information or data has not been disclosed to an unauthorized individual or in an undesirable manner.
- Integrity. This is the process of verifying that the information is authentic, accurate, and complete, without undesired or unauthorized changes.
- Auditing, Logging, and Alerting. This process tracks selected security-related events (such as log-ins, updates or changes to data), storing the audit trail information in a system-protected file to provide a means of accountability, and notifying appropriate individuals of security issues that require response. This information is particularly useful in the detection and prevention of the fraudulent use of the system.

8.1.2. Security Management

A centralized information security staff that is a combination of resources drawn from the State SFIS staff, contractor staff, OTech staff, and OSI staff is responsible for security operations and manages SFIS as well as system and network security tools, platforms, and procedures. At the county office level, local personnel are responsible for physical security administration. Policies, procedures, standards, and guidelines have been created and regularly updated to ensure that appropriate security measures are applied consistently and effectively.



8.1.2.1. Central Administration

For the SFIS project, which is managed by OSI, the OSI Information Security Office will work in conjunction with CDSS and be responsible for incident reporting as a result of any project related security incidents. The central security team is operated by the SFIS contractor with oversight provided by the State SFIS Team, the OSI Information Security Officer (ISO), and OTech security personnel. The SFIS contractor is responsible for the security and operational management of devices and systems associated with the centralized firewall architecture at the application level. Network security services are provided by a combination of State SFIS and OTech personnel, with participation of the OSI ISO as an advisor. In addition, this team:

- Implemented and operates a security automation/management tool that systematically and transparently maintains user access to applications and network operating systems;
- Proactively monitors the SFIS network using scanning tools such as HP OpenView and CA Unicenter;
- Manages anti-virus technologies dispersed throughout the environment and distributes updates;
- Acts as a single point of contact for security issues and incidents reported by counties;
- Provides historical, statistical, and logging information; and
- Develops and conducts periodic testing of the security system to ensure it provides adequate protection for the SFIS system (conducts configuration audits, identify new risk areas, etc).

8.1.2.2. Local Administration

County personnel will continue to be trained through the formal SFIS training program on system security controls, the information classification scheme, and applicable security standards and are responsible for implementing security controls that are mandated in the policies, procedures, standards, and guidelines at county locations. Counties are responsible for physical security at their sites. Although SFIS is the primary mechanism used to create, modify, and delete ID's in the SFIS environment, County Coordinators have the capability to perform these functions on the devices used by their county's end users.

8.1.2.3. Access Restrictions

SFIS restricts system and data access to prevent unauthorized access to or modification of confidential information. Following are brief descriptions of some of the access restrictions SFIS has implemented.



8.1.2.3.1 Securing of Executable Code

Executable code and/or tables are secured using operating system file system capability. Permissions to these resources follow the least privilege rule, which states that “any entity should only have the access required to perform its tasks.” In fact, no application except SFIS is available on SFIS remote workstations. Only authorized personnel have access to operating system resources. In most cases this is limited to the contractor’s system administrator and State SFIS technical staff. SFIS source code is stored in a secure offsite storage facility, so that executable code can always be restored to its most current production version.

8.1.2.3.2 Protecting Against Inappropriate Access of Data

Each component that contains data requires individual users to authenticate. *No global access to data and systems is available to any login.* Once a user is authenticated, access restrictions are associated with their ID to ensure that the ID can only access certain data. In addition, this activity is audited to track who is using the system and for what purpose. SFIS uses an information classification scheme developed by OSI and based on the State Administrative Manual (SAM) sections 5300 – 5360 to guide security administrators in applying the appropriate data classifications. The information classification scheme has the following categories:

- Sensitive Information - information maintained by state agencies that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency financial transactions and regulatory actions.
- Personal Information - information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request.
 - Notice-triggering personal information - specific items or personal information (name plus Social Security Number, driver's license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. See Civil Code Sections 1798.29 and 1798.3.



- Protected Health Information - individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. State laws require special precautions to protect from unauthorized use, access or disclosure. See Confidentiality of Medical Information Act, Civil Code Section 56 et seq. and the Patients' Access to Health Records Act, Health and Safety Code Sections 123100-123149.5.
- Electronic Health Information - individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers that conduct electronic transactions to ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure. See Health Insurance Portability and Accountability Act, 45 C.F.R. parts 160 and 164.
- Personal Information for Research Purposes - personal information requested by researchers specifically for research purposes. Releases may only be made to the University of California or other non-profit educational institutions and in accordance with the provisions set forth in the law, including the prior review and approval by the Committee for the Protection of Human Subjects (CPHS) of the California Health and Human Services Agency before such information is released. See Civil Code Section 1798.24(t).

8.1.2.3.3 Authorization to Update Data

SFIS uses an enterprise security management solution to ensure that only county staff or collaborating service providers with the proper security, password, and where appropriate, device identification clearance has sufficient authorization to update data. SFIS is configured to manage the access levels of individual IDs through a process of security automation. IDs are created, maintained, and deleted through this process. SFIS abides by role-based security rules that enforce strict access rules based on job function. This process, combined with the individual requirement for IDs and passwords, ensures that only authorized users can change or update information.

8.1.2.3.4 Contractor Access

By combining the rule-based access with ID's, passwords, filtering, and segmentation, only authorized contractor personnel are granted access to specific SFIS resources.



Due to the amount and sensitivity of the information that traverses and is stored on the SFIS network, certain regulatory controls must be observed. Many of these controls can be found in the Federal Information Processing Standards (FIPS). The SFIS project team has implemented security in compliance with appropriate FIPS regulations (FIPS PUB 31, FIPS PUB 41, and FIPS PUB 73), which include:

- Physically securing the network and data center;
- Implementing internal controls;
- Designing security controls into the application itself;
- Ensuring positive identification of those accessing the system;
- Preventing unauthorized access from those persons not defined to the system;
- Preventing unauthorized access to information from those who are defined to the system; and
- Conducting internal audits and proactively monitoring the system to ensure it is functioning in accordance with the security controls stipulated.

8.1.2.3.5 Local Administration

County Coordinators are able to administer user log-on and access levels for their counties. In parallel with the centralized security automation process, local administrators retain the ability to create IDs, change passwords, and grant/revoke access but only for their county's users.

8.1.2.3.6 Individual Log-on Security

Log-on security parameters are enforced at the individual level. Consistent security parameters are specified via standards that dictate what security parameters surround the login process (e.g., login banner, minimum password length).

When a user logs into SFIS, he or she is required to acknowledge his or her specific ID or to have their fingerprints registered in lieu of passwords for that system and to provide the associated password or fingerprint. The ID has the same format across SFIS as dictated through standards and system requirements regardless of end user roles and, unless otherwise determined, no more than one log-on per person is permitted. All user IDs have associated passwords, and at county discretion have their operator fingerprints stored in a special database allowing the user to use a fingerprint in lieu of a password. (The passwords must fall within security parameters as specified by standards, such as minimum length, or alphanumeric required, etc.)



8.1.2.3.7 Automatic Log-out

Automatic timing-out of inactive sessions occurs within a 15 minute interval. This sequence is used at the workstation and laptop level and is not adjustable by the end user. The user needs to use the keyboard or mouse to prevent time-out or reset the interval. A time-out will occur and lock the workstation even if the computer is actively processing information. If a time-out occurs the user is required to enter his or her password to reactivate the session.

8.1.2.3.8 On-Demand Reporting

System, end user, and case activity is audited, and reports concerning activity are processed at the Central Site. The information that is gathered uses a report generation tool to tailor the audit information for the workstation or the individual according to requirements. The information is then made available on an as demanded basis to authorized users of SFIS or SFIS OSI staff. Strong security controls are in place so that only authorized users can view this information.

8.1.2.3.9 Application Level Security

SFIS implements security at the application level based upon the user's role. Every system user (including external users) is assigned a role or roles. The application limits a particular user's access to menus, windows, functions, and data based upon the role(s) assigned to that user.

One of the most important roles is the capability to change the roles for other users. Only appropriate State SFIS staff, contractor staff, and County Coordinators (for their county only) and administrative staff are permitted access to the role assignment function. Once operating the function, County Coordinators have data access only for the particular users for which they have responsibility.

8.1.3. Security Design Overview

The design of the SFIS firewall environment adheres to the following policy statements that ensure a secure architecture is implemented:

- All security measures take into account the portion of the TCP/IP protocol that is used in any particular environment.
- The networking environment is grouped into network classifications—local trusted, and remote internal trusted. Since SFIS operates on a private network operated by the State, no public access to the SFIS application or its databases is possible. Remote connections to SFIS fall under the remote internal trusted classification.
- Each network classification is separated into distinct network domains (i.e., a specific project LAN segment is a single distinct network domain).
- Each network domain resides on its own LAN segment.
- Communication between network classifications is controlled by a centrally managed firewall.



- Only the centralized security team located in Sacramento manages remote access and similar critical network access points.

8.1.4. Security Components

8.1.4.1. Firewall Gateway

The primary roles of the Firewall are access control, authentication, auditing and logging, and alarming. In addition, the firewall conforms to the security philosophy by adhering to the failsafe stance, implementing default deny, and providing simple management.

The firewall is a gateway that permits workstations at county offices to only connect to the private network supporting SFIS, while ensuring that SFIS resources are not put at risk.

8.1.4.2. Authentication Database

The authentication database is an integral part of SFIS' overall security policy enforcement. The authentication database server provides a centralized repository of user's names, passwords, access levels, and in some cases user fingerprints. This simplifies management and design for the overall architecture.

8.1.4.3. Routers

Networking gateway architectures call for a router on most interfaces of the firewall. These routers perform different roles depending on which interface of the firewall they are attached.

The screening router, owned by the contractor, performs a variety of security tasks. The screening router denies typical attacks caused by malicious manipulation of IP options flags in the IP header, such as source routing and fragmentation attacks. The screening router also prevents attempts at IP spoofing, including both external users spoofing internal addresses as well as internal users spoofing external addresses. In addition, it blocks ICMP packets. Finally, the screening router mirrors the firewall rulesets to provide defense in depth.

8.1.4.4. Network Management Station

This component primarily acts as a network monitoring/management station, but it also performs security roles. It has several security products that perform real time and scheduled security tasks. Below is a list of functions along with the security technology needed to perform them:

- Security automation. This ensures that the IDs are created/modified/deleted in a timely manner; it also ensures that only those persons that need access to SFIS have that access. This software also provides efficient removal of access for terminated or transferred employees.
- Anti-virus technology. A COTS package is used for virus reporting and virus string update distribution.



- Network node management. HP OpenView, and CA Unicenter are used to monitor the status of devices.

8.1.5. Program Integrity

Program integrity security involves provisions for preventing fiscal abuse of the SFIS system. The system is able to identify the source of any addition, change, or deletion to case files. This feature, combined with expanded reporting capabilities at the local, office, and program level, provides supervisory and management personnel with a mechanism for analyzing case actions at the individual worker level.

8.1.6. Audit and Control

Audit and control considerations are especially important since SFIS has implemented an on-line, user interactive system that may be accessed by a large number of geographically dispersed staff with diverse skill levels and responsibilities. The audit and control requirements for the SFIS are described below in terms of data control, error correction, and audit trails.

8.1.7. Security Assessment

When a new SFIS contract is awarded, the Contractor will prepare a detailed description annually of SFIS security as specified below.

- For Security Administration, define, discuss, document, and recommend the use of:
 - Audit and accountability trails in the system;
 - System integrity controls and reports; and
 - System reports of errors, failures, attempted violations.
- Prepare summary listings of sensitive function and data showing the levels of protection that are present, and recommended changes to security if not already part of SFIS (e.g., physical site protection, terminal locks, encryption for transmission and/or data storage). All recommendations shall be consistent with ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management.
- Describe interfaces or dependencies on other software and discuss security aspects.
- Classify data elements to level of sensitivity.
- Describe any security breaches or incidents that occurred during the previous year and protective measures taken.



8.1.8. Encryption

At present, client data is secured on remote Client Input, Multifunction and Portable workstations using PKZIP, NIST AES-128 standard (described in Federal Information Processing Standards Publication 197).

Now that the new SFIS contract has been awarded, the Contractor will implement improved data encryption technology to protect all remote workstations used by SFIS users, and backup media such as tape. The encryption solution(s) will conform to the NIST AES-256 standard. The following will be protected by encryption:

- Data on ALL remote workstations.
- Data on all backup media such as tape.

8.1.8.1. **Data Control**

The SFIS contains a sufficient number of controls to maintain the integrity of the data and information involved. These controls fall into three types.

- Preventive Controls: Controls designed to prevent errors and unauthorized events from occurring.
- Detective Controls: Controls designed to identify errors and unauthorized transactions that have occurred in the system.
- Corrective Controls: Controls designed to ensure the problems identified by the detective control are corrected.

These controls are in production at all appropriate points of processing.

8.1.8.2. **Error Correction**

With an on-line, interactive system, error correction procedures are not as critical as they might be in a system of a different design. Since on-line editing forces immediate correction of data entry errors, error correction procedures in an interactive environment primarily relate to manual procedures, which are outside the control of SFIS. Automated on-line policy enforcement edits require immediate correction, which prevents many input errors.

8.1.8.3. **Audit Trail**

Audit trails are incorporated in the system to allow information on source input to be traced through the processing stages to the point where the information is finally recorded. The ability to trace data from the final place of recording back to the source of input also exists. These audit trails consist of listings, transaction reports, update reports, transaction logs, and error logs. The audit trails make it possible to reverse the effects of a transaction on the SFIS database.



8.2. PHYSICAL SECURITY PROCEDURES

It is important that effective physical security measures be implemented and maintained at all processing sites. SFIS restricts perimeter access to the Central Site through a coded access card type system; as well as, accountability control to record access attempts of unauthorized users and cancellation of unauthorized or fraudulent access cards. Physical security includes additional features designed to safeguard all mainframe-processing sites through the use of a Closed-Circuit Television (CCTV) system, fire suppression system, smoke detectors, and electrical alarms monitored by security personnel for key processing areas. LAN servers are physically protected from non-authorized access and located at the Central Site with most of the same security features. Physical security at the Central Site is provided by OTech. Physical security at county sites is the responsibility of the counties with State SFIS staff having oversight responsibility.

The SFIS are in the planning stage of moving the SFIS Central Site to the Franchise Tax Board (FTB) Location. At this time the FTB will be responsible for the physical security of the Central Site. The new Central Site will have the following physical security features:

- The facility will be equipped with a Uninterruptible Power Supply (UPS) that allows SFIS to be shutdown with no loss or corruption of SFIS data if the primary power source is lost.
- The area surrounding the building containing the computer room will be lit and free of obstructions that would block surveillance via CCTV cameras and patrols.
- There will not be a sign advertising that the facility has a computer room.
- There will be CCTV cameras outside the building housing the computer room monitoring parking lots and neighboring property.
- Computer rooms will not have windows to the outside.
- Loading docks and all doors on the outside of the building housing the computer room will have some automatic authentication method (such as a badge reader).
- Computer room access: There will be an automatic authentication method at the entrance to the room (such as a badge reader). Access will be restricted to those who need to maintain the servers or infrastructure of the room.
- The computer room will be monitored by CCTV cameras.
- Visitors will be escorted by the person whom they are visiting at all times. Visitors will not be allowed access to the computer room without written approval from Contractor management. All visitors who enter the computer room will sign Non Disclosure Agreements.



8.3. BACKUP AND RECOVERY

It is critical that procedures and facilities be in place to ensure that, in the event of major problems at any processor site(s), a mechanism exists to reconstruct the system and the affected databases. Adequate backup and recovery mechanisms are incorporated at all processor levels that meet the requirements of the overall SFIS disaster recovery plan. The SFIS application is a lower priority application with a maximum acceptable outage in excess of one month. Since SFIS has Stored Transaction capability, network failure, software error, or operational error where one or several days processing is invalid should not occur.

Two major problem situations, which are addressed by safeguard procedures, include:

- A major disaster where the computer installation and resident software is destroyed or damaged. The contractor provides a comprehensive disaster recovery plan for the current SFIS. When a new SFIS contract is awarded, the contractor will not only produce the plan but additionally will be responsible for updating the plan at least once a year, and will also be responsible for annually testing the plan. The plan will conform to the State Administrative Manual (SAM, Section 4843-4845) and the Statewide Information Management Manual (SIMM, Sections 5 & 140), and be formally accepted by the State SFIS Project Manager. The contractor will produce a written report of the test.
- A system-wide outage.

The State has designated SFIS as a non-critical system, and therefore, extensive disaster recovery capabilities are not required. Since SFIS has the capability to process stored transactions on remote workstations, SFIS operations can continue uninterrupted for an extended period of time

The concepts and procedures outlined in this plan will be utilized in the event of, but are not limited to, the following situations: flood, fire, earthquake, explosion, building collapse, communication failure, power interruption, or other emergency in which the operation of the SFIS Central Site is interrupted.



9. TRAINING PLAN

9.1. PURPOSE

The purpose of this plan is to plan the effective, systematic training of the SFIS users and the SFIS Project Staff. The plan documents the current learning program, learning obstacles and attempts to identify learning needs of the SFIS users and SFIS Project Staff (current and potential new staff). The plan also recommends learning, implementation, evaluation and measurement strategies for meeting the learning needs of the Counties and SFIS Project Staff. The SFIS Training Plan should be used as a reference and as a source of inspiration for training, not limiting the project from new and ongoing ideas. The plan does not cover specialized county training that may be needed when system enhancements occur.

Based upon the Needs Assessment and SFIS Project Staff input, recommendations for the effective training of SFIS to end-users were developed.

The SFIS Training Plan is a required document and has been in production use for several years. We have provided a current version of the document including the revision history as an attachment. A summary of these documents has been provided in the body of the IAPD for your convenience. The complete SFIS Training Plan is ATTACHMENT III.

9.2. COUNTY TRAINING

The learning goal of all SFIS Training is to ensure that SFIS' users fully understand the purpose of SFIS, and to ensure that end users are able to understand the program integrity issues surrounding SFIS, and to properly operate their SFIS workstation to its full capacity.

The goal is met using Classroom Training, Website Material, State Led Customized Training, and Targeted County Training.

9.3. STAFF TRAINING

The SFIS Project Staff is comprised of individuals who are State employees, those who are employed through the PMO/QA contractor, and those who are employed by the primary contractor for SFIS M&O.

A needs assessment was conducted in order to determine that the current SFIS Project Staff was sufficiently trained for their specific job functions. The Training Coordinator spoke with the departmental supervisors and employees and concluded that the current level of knowledge and skills are sufficient. It was determined that recommendations included in the SFIS Training Plan would benefit the project for the training of new SFIS Project Staff or current staff who may transition into different positions.

To review the complete SFIS Training Plan, see ATTACHMENT III – Training Plan.



10. TRANSITION-IN SCHEDULE

	Duration	Start	Finish
Stakeholder Meeting Managers Notification	1 Days	2/11/10	2/11/10
APD Approval	3 Months	3/1/10	5/31/10
SFIS IHSS Project Oversight Users Group	On-Going	3/1/10	
Gather Requirements			
Site Assessments for Workstation/Network Installs	3 Months	3/1/10	5/31/10
Gather Requirements from Case Workers	3 Months	3/1/10	5/31/10
Gather Requirements from Fraud Investigators	3 Months	3/1/10	5/31/10
Initiate Change Order with Prime Vendor	5 Days	6/1/10	6/8/10
SFIS Handheld Solution			
Install Network	3 Months	6/1/10	8/31/10
Purchase Equipment	6 Months	6/1/10	11/31/10
Develop Application	6 Months	6/1/10	11/31/10
Training Rollout	3 Months	9/1/10	11/31/10