

SECTION III
CURRENT SYSTEM

Addendum 4 - 10/05/2007

**RFP OSI 2046
CURRENT SYSTEM**

TABLE OF CONTENTS

A. BACKGROUND AND THE AUTOMATED FINGERPRINT IMAGE REPORTING AND MATCH (AFIRM) SYSTEM	9
B. GENERAL DESCRIPTION OF SFIS	11
SFIS FINGERPRINT IMAGE QUALITY	11
GENERAL DESIGN REQUIREMENTS.....	12
Open Architecture.....	21
Non Proprietary	21
Search Capability	21
Record Synchronization	23
Record Updates.....	24
Data Validation	25
Transaction Trace.....	25
Data Integrity	26
Transaction Logs	26
Collection Requirements	27
All Workstation Requirements	28
Remote Input Workstation Requirements Only	29
Verification and Fraud Investigation Requirements Only	35
System Administration Workstation Requirements Only	35
C. END USER FUNCTIONALITY.....	36
ALL USERS	36
Windows NT Logon	36
CLIENT INPUT WORKSTATION USERS (ONLY) USER FUNCTIONALITY	42
File Clearance Function.....	43
Displaying Results	44
Request for New CIN.....	46
CLIENT INPUT WORKSTATION AND SYSTEM ADMINISTRATION WORKSTATION ONLY	49
Resolution Function.....	49

**RFP OSI 2046
CURRENT SYSTEM**

Scanner Diagnostics.....	52
Replacing Platen on Fingerprint Scanner	55
CLIENT INPUT WORKSTATION, SYSTEM ADMINISTRATION WORKSTATION, AND FRAUD INVESTIGATION WORKSTATION USER FUNCTIONALITY	56
Print Function	56
Inquire Function.....	60
CLIENT INPUT WORKSTATION AND PORTABLE INPUT WORKSTATION (ONLY) USER FUNCTIONALITY.....	69
Stored Transactions	69
Add/Update Function.....	97
Adding Client Photo and Fingerprint Images.....	102
Verifying a Client	114
FRAUD INVESTIGATION WORKSTATION (ONLY) USER FUNCTIONALITY.....	118
Fraud Review Function.....	118
Two Cin Search Function	132
Fraud Restore Function.....	133
SYSTEM ADMINISTRATION WORKSTATION (ONLY) USER FUNCTIONALITY ...	138
Security Function.....	138
Add New User	139
Update User	143
Crystal Reports.....	149
Audit Controls And Security.....	149
Security And Access Control Requirements.....	150
Security Standards	157
Audit Information	157
Contractor Certification.....	157
Password Protection.....	158
Audit Trail and Reports.....	158
Access Control Mechanisms	159
Remote Input Workstation Security	164

**RFP OSI 2046
CURRENT SYSTEM**

LEADER INTERFACE.....	164
Introduction.....	164
Batch System	165
Online System	166
D. COUNTY ENVIRONMENT	168
COUNTY OFFICE EQUIPMENT	168
E. GENERAL COUNTY & CENTRAL SITE HARDWARE DESCRIPTION.....	171
WORKSTATION MAINTENANCE AND REPAIR.....	176
Workstation Operating System.....	176
County & Central Site Software.....	176
County LAN Environment.....	177
PHYSICAL CHARACTERISTICS.....	179
UL Compliant.....	179
FCC Class B Compliant.....	179
CURRENT (AS OF 12/01/2004) COUNTY WORKSTATION LOCATION DETAILS .	180
F. CENTRAL SITE ENVIRONMENT	203
CENTRAL SITE INTERACTION	203
DTS FACILITIES	203
NETWORK ENVIRONMENT.....	204
DTS LAN and WAN Overview	204
SFIS WAN Redesign Project.....	205
Contractor Site Network Charges.....	205
Network Management	206
CENTRAL SITE LAN, HARDWARE AND SOFTWARE.....	207
Database Server.....	207
Workstation Configuration	208
Network Printers.....	211
Motorola, Inc./Biometrics Business Unit Subsystems.....	212
System Expansion.....	219
SFIS TEST AND TRAINING ENVIRONMENT	221

**RFP OSI 2046
CURRENT SYSTEM**

Test Bed System	221
BACKUP AND RECOVERY.....	223
Backup	223
Raw Image Backup	223
Matching Subsystem	224
DIRs Backup.....	224
SFIS Database Backup	225
Spare Backup	225
Application Backup	226
Database Transaction Journal.....	226
Online Data Backup.....	227
Offline Backup	227
Storage of Memory-based Minutiae and Descriptor Data in the Online Database.	228
Off-site Storage	228
Archive Audit Trails.....	228
Additional Tables Archived to Tape	231
System Monitoring.....	232
PRINTRAK AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AFIS).....	237
Accuracy.....	241
G. SYSTEM INSTALLATION.....	243
COUNTY SITE PREPARATION.....	243
Installation Sites	243
Office Relocations and Additions.....	243
FLOOR PLANS	244
Remote Site Floor Plan	244
Central Site Floor Plan	244
Environmental Requirements	246
H. HARDWARE RELIABILITY	249
WORKSTATION RELIABILITY.....	249
Weekly Workstation Reliability.....	249

**RFP OSI 2046
CURRENT SYSTEM**

Workstation Key Components	249
Workstation Reliability Calculation.....	250
Weekly Central Site Reliability.....	250
Central Site Reliability Calculation.....	251
Test Bed System Reliability	252
Test Bed Reliability Calculation	252
I. MAINTENANCE	253
MAINTENANCE AVAILABILITY.....	253
PRINCIPLE PERIOD OF MAINTENANCE TIME-FRAME	254
REMEDIAL MAINTENANCE (UNSCHEDULED).....	254
Remedial Maintenance Response Time Definition	254
Off-line Maintenance Capability.....	255
Maintenance Reports	255
Maintenance of Additional Equipment	259
Equipment Replacement	259
Reliability Improvement Notices	259
CENTRAL SITE MAINTENANCE	259
Hardware and Software Maintenance	259
Preventive Maintenance	259
J. SYSTEM WORKLOAD AND THROUGHPUT	268
DATABASE SIZE.....	268
AVERAGE MONTHLY WORKLOAD.....	268
RESPONSE TIME	268
Simultaneous Entries.....	271
Concurrent Transaction Processing	271
Response Time Requirements	276
K. MANAGEMENT PROCEDURES AND POLICIES	280
CHANGE MANAGEMENT	280
Change Acceptance and Validation Procedures	281
Formal Acceptance and Validation	284

**RFP OSI 2046
CURRENT SYSTEM**

CONFIGURATION MANAGEMENT.....	290
Application Development Environment.....	290
Application Software Configuration Management.....	291
Configuration Management Procedures	300
Managed and Controlled Work Products.....	312
CI Naming Standards	313
Standards	318
Informix Considerations.....	320
Database Standards.....	320
Documentation Standards	321
PROBLEM MANAGEMENT.....	321
Help Desk Ticket	322
Outage Analysis	322
PROJECT POLICIES AND PROCEDURES	324
Administrative Policies, Procedures, and Arrangements	324
Work Standards.....	324
L. DOCUMENTATION AND REPORTS	326
BROCHURES AND OTHER MATERIALS.....	326
Design Publication Materials	326
Provide Publication Materials	327
Languages For Publication Materials	327
Deliver Publication Materials	327
Approach to Public Information Campaign	327
DOCUMENTATION REQUIREMENTS	327
Complete Set of Reference Materials.....	327
Documentation Updates	328
Documentation	328
SFIS GENERATED REPORTS	330
Report Listing	330
Daily Reports.....	331

**RFP OSI 2046
CURRENT SYSTEM**

Weekly Reports	335
Monthly Reports	353
Operator Audit Reports.....	375
M. PERSONNEL	376
STATE APPROVAL OF STAFF.....	376
Contractor Personnel.....	376
AVAILABILITY OF STAFF.....	376
SFIS ORGANIZATION STRUCTURE	376
SFIS – CURRENT CONTRACTOR ORGANIZATION	377
Personnel Requirements	381
Contractor Staff’s Qualifications	384
N. HELP DESK	390
HELP DESK SUPPORT DESCRIPTION SUMMARY	390
Help Desk Level of Effort.....	390
SFIS Help Desk Structure	390
SFIS Help Desk Support Team	391
SFIS Help Desk Approach.....	393
SFIS HELP DESK IMPLEMENTATION	393
SFIS Help Desk Location	393
Toll-Free Telephone Number.....	394
Automated Tools	394
Priority/Severity Handling Process	396
Reporting.....	402
Training	402
SFIS Help Desk Process	405
Request Workflow	409
Information Sources and Reports.....	410
O. TRAINING AND TESTING	412
TRAINING CENTERS	412
CLASS DESCRIPTIONS.....	413

RFP OSI 2046
CURRENT SYSTEM

Client Input Workstation	413
Fraud Investigation Workstation	413
Portable Input Workstation	414
System Administration Workstation	414
Special Issues Workshop	414
Training Database	415
Enrollment Procedures	415

**RFP OSI 2046
CURRENT SYSTEM**

A. BACKGROUND AND THE AUTOMATED FINGERPRINT IMAGE REPORTING AND MATCH (AFIRM) SYSTEM

In October 1993, consistent with the Governor's commitment to improve the integrity of welfare through fraud deterrence, prevention, detection, and overpayment recovery, the California Department of Social Services (CDSS) convened a Strategic Planning Task Force to develop recommendations to improve the integrity of California's welfare system by eliminating fraud, waste, and abuse. Statewide fingerprint imaging was one of a number of items discussed by the Task Force, largely due to the growing prevalence of counterfeit identifications used to establish welfare cases, and the reported success of Los Angeles County's AFIRM system implemented in 1991 to eliminate duplicate aid fraud in the County's General Relief (GR) program. At the direction of the Task Force, in 1994 Los Angeles expanded the system as a pilot to include the Aid to Families with Dependant Children (AFDC) caseload. Subsequently AFIRM was expanded to six (6) other California counties, which included Alameda, Contra Costa, Kern, Merced, Orange, and San Francisco.

Due to the documented success of AFIRM by an independent evaluator, in 1996 the Legislature passed SB 1780 (enacted as Chapter 206, Statutes of 1996), requiring applicants for, and recipients of AFDC, now the California Work Opportunity and Responsibility to Kids (CalWORKs), and Food Stamp Programs (FSP) to be fingerprint imaged as a condition of eligibility. Fingerprint imaging is regarded as both a deterrent to and detector of welfare fraud.

The State of California executed a contract with Electronic Data Systems (EDS) for the design, development, implementation, and operation of the Statewide Fingerprint Imaging System (SFIS). The contract term ran from September 7, 1999 to September 6, 2003, and was extended to September 2005 as provided under the terms of the contract.

SFIS was implemented in three (3) phases between March and June of 2000 in all counties, with the exception of Los Angeles County. Statewide implementation, including Los Angeles, was completed by December 2000. Currently, EDS operates SFIS with oversight provided by the SFIS Project Staff within the OSI. The SFIS Project Staff manage the SFIS contract and provide substantial support for the day-to-day operations of SFIS.

Significant testimonial exists where SFIS was instrumental in detecting and/or deterring fraud:

RFP OSI 2046
CURRENT SYSTEM

- In Sacramento County, the District Attorney reported that a man was successfully prosecuted for receiving more than seventy thousand dollars (\$70K) from multiple cases he set up using five (5) different California drivers' license numbers.
- The Sacramento County District Attorney reported that the Sacramento welfare department discovered six (6) people using forged documents to open fifteen (15) different welfare cases and received over one hundred thousand dollars (\$100K) in aid through SFIS.
- The Sacramento County District Attorney reported that fingerprint imaging detected a Los Angeles County resident who received over twelve thousand dollars (\$12K) in aid by using forged identification documents.
- The Honolulu Star Bulletin reported on June 27, 2003 that: "A former California Man admitted he came to Hawaii to commit welfare fraud because the state does not have safeguards, such as fingerprinting recipients."

The estimated annual savings from the operation of SFIS are approximately sixty-eight million dollars (\$68M) for the CalWORKs program.

As of spring 2004, the SFIS database contained approximately six point two million (6.2M) fingerprint images. The system processes forty-five hundred (4500) to five thousand (5000) fingerprint transactions per day, an average of eighteen point five (18.5) transactions per desktop image-capture workstation. The counties use a total of approximately three hundred and fifty (350) SFIS workstations. In December 2003, only about one percent (1%) of the SFIS fingerprint database contained images with multiple poor quality scores, indicating that the SFIS database images are of good quality.

While the following documentation contains, to the best of the State's knowledge, the best available descriptions of SFIS, the State makes no guarantees, representations or warranties regarding the accuracy or completeness of the descriptions of the systems contained in these documents. The awarded Vendor will be responsible for maintaining and operating the system as it actually exists at the time of system transfer under the Contract resulting from this RFP, and not as it is represented in the documentation.

**RFP OSI 2046
CURRENT SYSTEM**

B. GENERAL DESCRIPTION OF SFIS

SFIS searches for proof of duplicate records (Open Search – one to many match) by matching a client with fingerprints on record for GA/GR (for some counties), and/or CalWORKs and/or FSP (Closed Search – one to one match). The System does not:

- Detect other types of payee fraud, such as unreported income by a recipient that is working and collecting benefits;
- Interface to non-welfare systems such as the Department of Motor Vehicles, Immigration and Naturalization Services, or the Department Of Justice; and
- Provide Eligibility Records Management or Case History Information. SFIS was not intended to replace other systems that are used for Eligibility Records Management or Case History Information.

The SFIS Central Site houses database servers, process-coordinator workstations, and the Motorola, Inc./Biometrics Business Unit (referred to as Motorola/Printrak in this RFP, and formerly known as Printrak International, a Motorola Company) Automated Fingerprint Identification System (AFIS). There are about three hundred (300) SFIS workstations located in county welfare offices statewide used to perform image capture, and another approximately seventy-five (75) workstations supporting various management and administrative tasks, including training. The DTS statewide Wide Area Network (WAN) and dedicated Local Area Networks (LAN) within each county and at the Central Site provide the needed communications infrastructure.

Deleted: Printrak

SFIS FINGERPRINT IMAGE QUALITY

The first in-depth look at SFIS fingerprint image quality occurred in September 2002 immediately before key system enhancements were implemented, and the most recent look was in March 2005. These image quality analyses revealed the following:

- In September 2002 there were over three thousand (3K) fingerprint images in the database where all image quality scores were at the poorest level – in many cases, no image was discernible to the naked eye. In March 2005, none of these images remained.
- In September 2002 about three percent (3%) of the SFIS database had images with grayscale (composed of a series of shades of gray) problems. In March 2005 none of these fingerprint images remained.

**RFP OSI 2046
CURRENT SYSTEM**

- In September 2002 about one percent (1%) of the SFIS database had images with multiple poor quality scores. In March 2005, also about one percent (1%) of the SFIS fingerprint database had images with multiple poor quality scores.

GENERAL DESIGN REQUIREMENTS

The following table summarizes the current SFIS technical design:

SFIS – Current Technical Design Requirements

Technical Requirement	Description
DESIGN REQUIREMENTS	
General Design Requirements	
Open Architecture	Basic design utilizes Open System components
Non Proprietary	No reliance on proprietary components
Workstation Functionality	Collect, store, and transmit finger images, photo images, and demographic data
Identification Fields	Client Index Number (CIN), Process Control Number (PCN), Social Security Number (SSN), Local Identification Number (LIN) and demographic information
Search Capability	System design provides Open and Closed Searching
Search Prioritization	Parameter driven fingerprint searching is possible but unused at this time
Classification Process	No role of workstation operator in classification process
Search Parameter Storage	Record and store all search parameters
SCI Interface	Electronic data interface to (Statewide Client Index (SCI)
System Expansion	Expansion path to at least two (2) times greatest currently anticipated volume
Audit Controls	Appropriate internal controls, quality assurance, indexing, security, and other features
Record Synchronization	Proper linkage of all data elements and images
Record Updates	Online update and inquiry Online match verification Online interface transactions SCI delete transactions
Data Validation	Data validation checks at the character, field, and transaction levels
Transaction Trace	Real time display of transaction status; processing history stored
Backup and Recovery	Backup and recovery capabilities to restore damaged files
Data Integrity	System restart procedures ensuring no loss of data entered

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
Transaction Logs	Transaction logs to assist in data recovery
User Password	Periodic changes to user passwords
Access Levels	User group access categories
Operator Audit Reports	Detailed audit trail reports
Data Collection Requirements	Indices: CIN, SSN, LIN, and PCN Flat, compliant fingerprint images via live scan Digitized color photo image No photo conversion by operator Demographic data fields Control information, including unique system key Character free text comments field
Finger Image Upgrade	Automatically replace poor quality previously captured fingerprint images
Photo Image Recapture	Store most recent photo; photo override
Permission Table	Transaction restrictions by operator, group of operators
Search Queues	Search priority queues Individual transaction priority modification
Queue Status	Queue status inquiry
Priority Queue Authorization	Priority queue authorization restriction
Dynamic Queue Display	Dynamic priority queue display update
Targeted Existing Records Closed Search	Two CIN Closed Search
Targeted Intake Close Search	Intake record against operator - specified record
Open Search Options	Inquire only Open Search Inquire plus store Open Search
RDBMS	Structured Query Language (SQL) - compliant Relational Database Management System (RDBMS) tables
Central Site Design	Digital Image Retrieval Subsystem (DIRS) RDBMS Matching subsystems DTS WAN
Cross Finger Comparison	Closed Search cross finger comparison for Closed Search misses
CIN Interface Update	Interface updates CIN interface update
Search Tracking	Open and Closed Search tracking
Verification Queues	Search verification queue Separate verification queues for search results
Image Exception Report	Unacceptable quality fingerprint image report Exempted fingerprint report "Retake" photo image report

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
Response Time Measurement	Workstation response time measurement
Workstation ID	Unique workstation ID
Welfare Fraud Prevention and Investigation (WFPI) Queue Storage	Six (6) month candidate storage for cases with dispositions
Match Response Printout	Search printout default override "Text only" search printouts "Text plus images" search printouts
Match Response Option	"Text" or Text plus images" report option
Extended Availability	Twenty-four / seven (24/7) operation capability Central Site reliability
Help Features	On-line help
Anti-Virus Software	Anti-virus software installed
Fingerprint Image Requirements	
Image Display	Fingerprint display ten (10) times original size
Image Contrast Controls	Onscreen brightness and contrast controls
Wavelet Scalar Quantized (WSQ) Compression	WSQ Compression
Finger image Safeguards	Prevent altering of data and keep synchronized
Exclusive Property	Photo and fingerprint image data ownership
Photograph Image Requirements	
Photo Resolution	American Association of Motor Vehicle Administrators (AAMVA) Photo digitization standard
JPEG Compression	Photo image JPEG compression
Live Scan Requirements	
ANSI NIST Compliance	ANSI NIST compliance
Flat Impressions	Live scan flat image capture
Consumables	Provide process consumables: White wipes for cleaning scanner platen, yellow wipes for cleaning and moisturizing fingers, Windex™, T-10 screwdriver, scanner platen, eye dropper, Corn Huskers Lotion™, Diagnostic Grid, DocuPrint 4508 Cartridges, HP Laserjet C8061X, photo light bulb, bulb replacement screwdriver, Zip Disk, DAT Tape, and Optical Platter.
Live Scan Operational Requirements	Consistent repeat test target scanning results Warm up period and continuous operations
Live Scan Quality Control Testing	Automatic input workstation live scan testing
Interface Requirements To The SCI Database	

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
Interface Specifications Document	OSI Provided
Interface Responsibilities	SFIS-side interface programming; provide network equipment
File Clearance/Photo Display	Display photos of persons returned from file clearance candidates
Image Server Capability	Perform as an image server on DTS network
Verification and Fraud Investigation Workstations	
Side-by-Side Display	Side-by-side split screen display of photo images Side-by-side split screen display of fingerprint images
Fraud Investigation / Verification Workstations	Display images side-by-side Add, delete, and modify minutiae points Print out the side-by-side marked prints A nineteen (19) inch high resolution monitor Cursor motion by mouse or positioning keys Operator controllable fingerprint image enlargement up to ten (10) times original size Print images side-by-side with or without fingerprint characteristics
Verification Workstation Display	Clear and readable side-by-side display with zoom capability
Minutiae Display	Mark minutiae common to each of the two (2) side-by-side images
Minutiae Encoding	Add, delete, modify minutiae characteristics
Re-launch Search Record	Change the minutiae points Resubmit an Open Search Submit a Closed Search against another record
Fraud Investigation / Verification Workstations Printer	Verification and Fraud Investigation Workstation printer
Multi-Function Workstation	
Configuration	Performs the functions of Remote Input, Fraud Investigation, and System Administration Workstation
Printer	Multi-function Workstation Printer
SPECIFIC REMOTE INPUT WORKSTATION REQUIREMENTS	
Functionality	
Fully Functional	Capability to input, collect, store, transmit, access and display information
Image Printing	Capable of printing fingerprint images Capable of printing photo images

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
Field Edits	Field edits on client and control information entered by operator
Menu Selection	Menu driven system
Live Scan Capture	Live scan fingerprint and camera photo capture
Video Display	Video display of captured fingerprint images
Fingerprint Image Quality Check	Fingerprint image quality check Quality check when network is down
Pre Transmission Image/Demographics Update	Reentry of demographics prior to transmission Reentry of finger images prior to transmission Reentry of photo image prior to transmission
Post Transmission Image/Demographics Update	Demographic data update after transmission Image update after transmission
Photo Image Capture	Single key stroke to freeze the photo and store into local memory
Client Information Display	During data entry client information must appear on the screen
Central Site Interaction	Adding a new client for search, match, and filing Updating a record and researching Inquiring on a client record Receiving a Match/No Match confirmation Inquiring on fingerprint image with dual display Inquiring on photo image with dual display Printout of full or partial client record Confirmation based on side-by-side image display
Search Status	Display search transaction activity
Workstation Operating System	Industry standard OS with available off the shelf application software packages
Image Transmission	Extract minutiae and transmit minutiae and compressed images to the Central Site
Download Demographic Data	Download data from SCI interface
Remote Input Workstations	Hard Disk Capacity High Resolution Monitor Removable Media High Capacity Digital Recording Device RDBMS Installed
Workstation Display Characteristics	
Monitor Resolution	High-resolution digital color image display
Image Display	ANSI/NIST display characteristics
Workstation Printer (Portable Input does not have a printer)	Printout of any Image Displayed on Screen Capable of Full Gray Scale Printout Side-by-Side Capable of Full Binary Printout Side-by-Side Resolution of five hundred (500) pixels per inch

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
	Fingerprint Images ten (10) times Original Size Photographs with Sufficient Resolution
Photograph Image Side By Side Display	Display photo at least five (5) inch by five (5) inch side-by-side
Adjustable Contrast	Onscreen controls for brightness and contrast
Physical Characteristics	
UL Compliant	UL Certified
FCC Class B Compliant	Pre-wired FCC class B certified workstations
Off-Line Transaction Capability and Storage	
Stored Records	Store up to one thousand (1K) complete transactions on remote workstation
Portable Input Workstations	
Portable Input Workstation	Portable remote option
Remote Workstation Security	
Operator Security	Closed Search operator logon
Connection to the DTS Network	
LAN Configuration	LAN connectivity via Ethernet or token ring
Printer Requirements	
Workstation Printer (Portable Input Workstation does not have printer)	One (1) high-resolution printer per workstation except for Portable Input Workstations
Remote Printer Resolution	Printer capable of printing photo and fingerprint images
Bar Code Scanner Requirement (Los Angeles County Only)	
Client Input and Multifunction Workstation-attached Bar Code Scanner	Scanner capable of close range scanning of various data used by Los Angeles County
SPECIFIC CENTRAL SITE REQUIREMENTS	
Central Site Functionality	
Priority Queues	Prioritize transactions within system queues; no loss of data in the event of processor malfunction
Central Site Operations Functionality	Primary operations menu driven with clear instructions and messages to the user Stand-alone maintenance and monitoring utilities
Dynamic Fingerprint Quality Threshold	Quality threshold adjustable system-wide from the system console and broadcast immediately over the network

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
System Interfaces	Provide all interfaces to connect system components
Match Responses	Guarantee a match response for all transactions accepted by the Central Site
Workstation Error Notification	Display of the current system-wide status of all attached workstations
Central Site Error Notification	Provide a message to remote workstations when Central Site is not fully operational
Workstation Network Monitoring	Workstations can monitor the "heartbeat" of the Central Site over the network
Operational Downtime	Limit operational downtime during a physical relocation or computer room shutdown In-process transactions in system queues to be restartable
End-to-End Downtime	Shutdown and restart within twenty (20) minutes
Update Access	Each record to be updated by only one (1) workstation at a time
Printer Requirements	High speed Central Site printer
Central Site Test Bed System	
Test Bed System	Fully functional Test Bed system located at the Central Site facility
DATABASE CAPACITY	
Database Volume	Designed to accommodate fourteen point six million (14.6M) record volume
Purge and Restore	Off-load denied/discontinued or purged client records onto high capacity storage media; restore records within twenty-four (24) hours
WORKLOAD and RESPONSE TIME REQUIREMENTS	
Workload Requirements	
Daily Transactions	Process daily (Normal) search transactions between the hours of 7 a.m. and 7 p.m. (Pacific Time) Monday through Friday, except State holidays
Proposed Workstation Total	Number and type of workstations required to handle daily transaction volume
Response Time	Complete all Priority transactions within fifteen (15) minutes Complete all Normal transactions by 7 a.m. (Pacific Time) the next day Complete all Conversion search transactions by 7 a.m. (Pacific Time) one week later (7 consecutive days)
Simultaneous Entries	Capable of responding to simultaneous entries
Concurrent Transaction Processing	Concurrent types of transactions

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
Response Time Requirements	
Retrieval Response Time	Retrieve fingerprint images within five (5) seconds (excluding network time) Retrieve photo within five (5) seconds
Closed Search Response Time	Closed Search response within fifteen (15) minutes
Verification Operators	Number of verification/validation operators
SYSTEM ACCURACY REQUIREMENTS	
Print-to-Print Search Accuracy Requirements	
Two (2) Finger Open Search Accuracy	Two (2) Finger Open Search accuracy: ninety-seven point five percent (97.5 %) when in database; eighty percent (80%) when not in database
Single Finger Open Search Accuracy	One (1) Finger Open Search accuracy: ninety-five percent (95%) when in database; fifty percent (50%) when not in database
Two (2) Finger Closed Search Accuracy Requirement	Two (2) Finger Closed Search accuracy: ninety-nine point nine percent (99.9%) when in database; ninety-nine point nine percent (99.9%) when not in database
Single-Finger Closed Search Accuracy Requirement	One (1) Finger Open Search accuracy: ninety-nine percent (99%) when in database; ninety-nine percent (99%) when not in database
System Accuracy Test Requirements	
Two (2) Finger Open Accuracy	Two (2) Finger Open Search accuracy rate
Single Finger Open Search Accuracy	One (1) Finger Open Search accuracy rate
Two (2) Finger Closed Search Accuracy	Two (2) Finger Closed Search accuracy rate
Single Finger Closed Accuracy	One (1) Finger Closed Search accuracy rate
System Accuracy Testing	System Accuracy test completed after each phase and on request by the State
Test Data	System Accuracy test data will consist of at least six thousand (6K) sets of two (2) Finger records collected from specified workstations
Test Results	Examine all "no-hit" results
Test Record Storage	Store all search test set images to a high-capacity storage medium at the remote workstation to be used for future testing
Batch Launch of Test Searches	Batch launch previously stored test transactions for subsequent System Accuracy tests
Search Data Returned	Return specified items from each test search

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
System Accuracy Testing Hours	Subsequent System Accuracy tests conducted during non-operational hours
USE OF THE STATE'S DTS COMMUNICATION NETWORK	Use of DTS communication network
BACK UP and RECOVERY REQUIREMENTS	
Backup and Recovery Plan	Backup & Recovery Plan to restore the system to fully operational within two (2) hours
Disaster Recovery Plan	Disaster Recovery Plan to restore the system from complete system destruction
Transaction Logs	Detailed transaction logs that report errors; non interrupting report generation and log review
Database Journal	Journalled RDBMS transactions that can be stored on-line or on a high-capacity storage medium
Operating System Logs	Log operating-system-generated hardware and software error reports journalled to magnetic tape
On-Line Transaction Recovery and Data Backup	On-line mirror copies of image and minutiae databases, and transaction queues Queued transactions automatically restart after system restart Continue acquisition during system downtime
Off-Line Transaction Recovery and Data Backup	Off-line backup: Backup to high capacity off-line storage media; optical disks and backup tapes stored off-site Restoration: restore from corresponding backup volume or by copying the data from the backup tape and applying journalized transactions. Recovery: recreate all data and minutiae Offline minutiae database reorganization within two (2) days (during non business hours)
Training for Backup and Recovery	Train operators to backup and restore
Minutiae Data Recovery	Recover minutiae data without re-reading fingerprints
Transactions in process	Automatically restart transactions in progress on a system restart
Off-Site and Restoration of System Software	Provide application and system software to State for off-site storage
SYSTEM INSTALLATION	
Site Preparation	Site installation, included in implementation
Floor Plans	
Central Site Floor Plan	Included
Remote Site Floor Plan	Included
Square Footage Requirements Identification	Current Contractor listed square footage requirements

**RFP OSI 2046
CURRENT SYSTEM**

Technical Requirement	Description
Environmental Requirements	Comply with federal, State laws, and local regulations
Installation Sites	
Remote Workstation Sites	Multiple remote county sites
Remote Site Workstations	Workstations at remote sites
Central Site	Central Site at the DTS location
Remote Workstation Installation Options	Multiple remote workstation installation scenarios
Installation Standards	Installations in accordance with applicable laws, codes, ordinances, and industry standards and conform to existing electrical system and wiring of referenced sites
System Re-Configurability	Schedule to minimize system downtime for system maintenance
Data Storage Across Physical Storage Devices	Capability of spreading system database and index files across physical storage devices

Open Architecture

The system was designed in accordance with the industry trend toward open architecture solutions. In addition, the Motorola, Inc./Biometrics Business Unit (referred to as Motorola/Printrak in this RFP, and formerly known as Printrak International, a Motorola Company) matching subsystem's basic design follows the principles of an open systems design.

Deleted: Printrak

Non Proprietary

The SFIS design is flexible, and does not rely on a single vendor, supplier, or product in such a way that a change or upgrade would result in a significant loss of investment or degradation to system performance to the degree possible with the specialized system requirements involved. The requirement for Motorola/Printrak hardware and software, the current AFIS provider is an exception to this.

Deleted: Printrak

Search Capability

SFIS provides both Open and Closed Search capabilities. In an Open Search, the fingerprint data and demographic information for the client to be searched are forwarded to the Central Site for comparison against the fingerprint database. In a Closed Search, fingerprint data is processed and compared against a fingerprint retrieved from the Central Site fingerprint database. Open and Closed Searches are discussed in detail in the paragraphs describing the Central Site.

**RFP OSI 2046
CURRENT SYSTEM**

Search Delimiters

PARAMETER DRIVEN SEARCHES

For the purposes of expediting match/no-match reporting and reducing the business hour transaction-processing load, SFIS allows for the capability of executing parameter driven fingerprint image searches. Parameters are available in the matching subsystem but SFIS does not require the use of parameters for fingerprint image searches.

SEARCH PARAMETER

SFIS does not make use of either sex or data that can be derived from the fingerprint images to narrow the search.

CLASSIFICATION DATA

Data derived from the fingerprint image, such as classification, has not been used as a database delimiter, and therefore has not been used to determine database access. The elimination of classification as a filter also reduces the need for "fingerprint experts" to operate the system.

CLASSIFICATION PROCESS

The Remote Input Workstation (Client Input, Portable, and Multifunction Workstation) operator does not need to determine and/or assign fingerprint image data. Remote Input Workstation software [the Advance Fingerprint Processor (AFP)] measures print quality and extracts fingerprint minutiae without operator intervention.

SEARCH PARAMETER STORAGE

SFIS does not utilize parameters during the search process. Should the design be modified to utilize search parameters, these search parameters would be compiled, stored, and made available for audit trail purposes and system reports in the same manner as the existing system tracks parameters. The search parameter would be stored, associated with the appropriate PCN, on the Informix database in the log table.

RFP OSI 2046
CURRENT SYSTEM

CROSS-GENDER SEARCH

SFIS does not use sex as a delimiter, eliminating the need to perform CROSS GENDER searching. However, should the State decide to do so, SFIS has the capability to automatically search all records of one (1) sex against records of the other sex for all records input during a given day. CROSS-GENDER searching would occur at a time that would not conflict with the normal workflow of the system. All records input on any given day would be CROSS-GENDER searched by 7 a.m. of the next business day. If the CROSS-GENDER search operation results in a Match, the system would automatically change the sex of the retained record to "Unknown."

Record Synchronization

SFIS ensures that all data elements of each client record i.e., the two (2) fingerprint images, the photo, and the client biographical and control data are properly linked. The existing system currently tracks all database table rows and image files associated with a client through the use of an internally generated system key to ensure that any change in operator-entered information such as CIN, LIN or SSN does not result in any loss of linkage to database table rows and files associated with the record.

Client fingerprint minutiae, finger images, photo images, control information, and demographics will all be marked as they are created with a unique internally generated key (Process Control Number (PCN)) to permanently link all data elements. The PCN is created at the workstation and all files are marked as they are created. The PCN is recorded both in the data files when created and on the database tables as the information is transmitted to the Central Site. All PCNs are stored in an index table cross-referenced to their associated CINs for ease and speed of access.

The PCN is stored in the header of all image files including the fingerprint minutiae files, finger image files, and photo image file. These image file headers, containing the PCN, cannot be accessed or altered without the use of an application program. Viewing and editing of these image files is not possible without coding an application program to retrieve the files. Any application program would also need to be aware of the file structure to locate the PCN within the header of the image and then modify that PCN. Without an application program, the PCN within the images may not be altered.

RFP OSI 2046
CURRENT SYSTEM

Record Updates

SFIS provides the capability to perform on-line adds, updates, inquiries, and match verifications. These transactions are processed by the workstation through the use of a key identifier. Currently the system provides for interface transactions to the Statewide Client Index (SCI) for File Clearance.

RFP OSI 2046 CURRENT SYSTEM

Data Validation

SFIS performs data validation checks at the character, field, and transaction levels. The existing system performs multiple validation checks including check digit verification, valid data type, verification of entries across fields for discrepancy and allowed combinations, and availability of a particular transaction based on the current state of a record, among others. Error Fields are highlighted and error messages are displayed to instruct the workstation operator on correcting invalid entries.

Transaction Trace

The existing system provides the ability to trace a transaction from the point of inception to final disposition. A processing history is also available through the log table stored in the Informix relational database. Current or final overall processing time, queues entered, time that the transaction was entered and was removed from each queue, etc. are also included in the database. The current state of any operator-initiated transaction (an example of which follows) is available on-line for a real time display of the transaction state. The display screen is updated dynamically as changes in the status occur. The data is also available for use in State-defined reports.

Current State of Operator-Initiated Transaction Example:

For a Closed Search, the following processing stages are identified:

- Waiting for Closed Search.
- Closed Search Matching.
- Waiting for Closed Search Verification.
- Closed Search Verification.
- Matching Complete.

The following Open Search processing stages are identified:

- Waiting for Matching.
- Matching.
- Waiting for Verification.
- Verification.
- Matching Complete.

RFP OSI 2046 CURRENT SYSTEM

The Start Date, Start Time, Finish Date, and Finish Time are also stored for each queue so that system performance can be monitored.

Data Integrity

SFIS provides System restart procedures that ensure no loss of data entered. Should a system problem occur, use of the previous day's backup database and transaction log files are used to maintain data integrity. Integrity is ensured through the stringent requirements to process transaction log records in the order they were written. In the event of a hardware failure, the backup database is able to begin processing with full data integrity rapidly.

Additionally, SFIS protects matching work in progress by retaining the entire queue in the system, stored on magnetic disks. Automatic re-initiation from a point of interruption guarantees data integrity. Transaction information is maintained by the system through completion. These protective measures enable the system to:

- Back up to the last current match in the queue;
- Restore all prior queues of search results, and
- Re-initiate matching.

The Informix database and associated logs retain any transactions in the input and output queue(s) at the time of a system failure. The search in progress at the time of failure is restarted to ensure that search requests are always recovered, and data integrity is maintained.

Transaction Logs

Detailed transaction logs, which include all demographic data, finger images, photo images, and control data, are continuously maintained to prevent loss of data. The transaction logging utilities of the database are used to ensure that all transactions are logged as they occur and in the proper format to allow reconstruction of the database should it ever become necessary.

RFP OSI 2046 CURRENT SYSTEM

Collection Requirements

SFIS tracks the following information:

- Client Index Numbers (CINs), Social Security Numbers (SSNs), and Local Identification Numbers (LINs) for each record are indexed for fast retrieval. Each record is referenced by a unique internally generated-system key and each transaction is referenced by a Process Control Number (PCN) that is indexed for fast retrieval of records. Each record will contain a list of PCNs associated with the client indexed for fast retrieval of records based on a PCN search.
- A flat (not rolled, not nail-to-nail) fingerprint image of each index finger. The print definition meets the current ANSI/NIST - CSL 1-1993 standards for a high-resolution image. All fingerprint images are entered via a direct read of untreated and reasonably clean fingers.
- A color photo image of the applicant/client is captured by equipment connected to the workstation.
- The captured color photos are automatically digitized, with no requirement for special conversion operations by the operator.
- Client record and control information (name, DOB, sex, etc.) input by keyboard. The record currently contains in excess of thirty (30) fields.
- Automatically generated additional control information (date, time, workstation, id, etc.) is stored upon completion of the transaction by the operator. This information is used to construct a system-wide record identifier (PCN).
- A "free text" field is attached to each client record entered in the existing system by the fraud investigators and operators. The "free text" field is capable of being updated at any time.

Targeted Existing Records Closed Search

The existing system performs a Closed Search comparison of the input record and the record on file associated with the same CIN. The existing system is also able to perform this same Closed Search functionality on any two (2) records in the SFIS database that are specified by the workstation operator. The results of this match request is returned to the requesting workstation for display and printed on the printer assigned to the workstation submitting the request. Additional information may be found in the User Guides.

All Workstation Requirements

User Friendly

The workstation's user interface is designed to be easy to learn and use.

Image Printing

The existing system prints photo and fingerprint images in gray scale and allows the printing of all fingerprint images in binary.

Menu Selection

The existing system provides for all transactions to be selectable via either keyboard stroke or PC mouse selection based on the operator's preference. All menus and functions are selectable via PC mouse click. The workstation provided is an industry standard PC workstation and SFIS software conforms to Windows standards.

Error Logs

The system provides error logs and system status information in response to system operator requests. This information provides intelligible assistance in the diagnosis of problems. Each workstation maintains an SFIS application status log including error messages to assist in the diagnosis of problems.

A system console screen is available to obtain status and error information. This information includes browsing the operating system log file, including errors, browsing the RDBMS log file, including errors, checking queue status, checking network connection status, and checking database status.

The RDBMS used by the system contains many error logs and system status information which can be used in the diagnosis of problems and ongoing system maintenance, some of the utilities which are used to access this information include the following:

- Online.log: An Informix log, logs how many of the routines the fingerprint passed. The log tracks daily operational information that the system generates i.e., beginning and ending checkpoints, Informix errors, login error, and the like.
- Oncheck: Check specified disk structures for inconsistencies.

RFP OSI 2046 CURRENT SYSTEM

- Repair index structures found to contain inconsistencies.
- Display information about the disk structure.
- Onlog: Display Logical-Log contents to track a specific transaction or to see what changes have been made to a specific table space.
- Onstat: Provides statistics about the system status of the RDBMS at the instant that the command is executed including but not limited to the display of shared-memory structures and message log content.
- Dbaccess: Allows an operator to run queries against the database records.

Remote Input Workstation Requirements Only

A Remote Input Workstation is a workstation that is used to collect client finger images. Each Remote Input Workstation is configured as a fully functional SFIS workstation with the capability to input, collect, store, transmit, access and display fingerprint images and other associated client and control information. The Remote Input Workstation includes the following workstations:

- Multifunction;
- Client Input; and
- Portable Input.

Field Edits

The existing system performs multiple edits on individual fields and the relationships between fields for valid entries. When a field edit has determined an incorrect entry, the field is highlighted and a descriptive message is displayed indicating corrective actions to be taken by the operator.

Upon entering the client demographics area of the screen, all fields are populated with client information from either the SFIS database or the SCI Database. The operator may view and/or update the case demographic information.

RFP OSI 2046 CURRENT SYSTEM

As the operator adds or updates demographic information, the system performs on-line data validation checks at the character and field level, to ensure only valid information is added to the SFIS database tables. The operator moves from field to field by pressing the Tab key or using the mouse. If data is entered in error, SFIS displays a Data Entry Error message box indicating the problem or suggesting corrective action, and highlights the data field that contains errors. The operator acknowledges the errors by selecting the OK button in the Data Entry Error message box, and correcting the highlighted items. Please refer to the Client Input Workstation User Guide, and Portable Input User Guide for in-depth descriptions of this functionality.

Video Display

The live scan finger image provides a video display of captured fingerprint images to ensure that the fingerprint image is acceptable prior to storage of the image into local memory. Prior to storage of the image into local memory, the live scan finger image is displayed on the video monitor, without noticeable scrolling of the image. To aid in the positioning of the finger image, a "cross-hair" has been placed on the image display window. This "cross-hair" assists the operator in centering the image in the capture area.

Pre Transmission Image/Demographics Update

The fingerprint operator is able to reenter all data and images prior to indicating that the transaction is complete. The operator simply needs to retype any of the demographic fields to be changed. Demographic edits are performed on the re-entered data. The photo may be retaken before transmission. Finger images may only be updated before transmitting by clearing the entire transaction and starting the imaging process again. All fingerprint image quality check procedures are performed each time an image is captured including the left to right fingerprint comparison.

Post Transmission Image/Demographics Update

SFIS allows the workstation operator to reenter images and modify the demographics of any client record data previously stored in SFIS.

Client Information Display

During the data entry process, the client record and the Add/Update screen appears on the display for the operator to perform data entry.

Right to Left Search

Once both fingerprint images are captured, SFIS compares the right image to the left image to ensure two (2) different fingerprint images were captured. This one-to-one match is automatically performed at the Remote Input Workstation and is transparent to the operator. If the comparison results in a match, SFIS notifies the operator by displaying a Capture Error message window.

The message displayed in the Capture Error message window instructs the operator to restart the capture process. The operator is then instructed to recapture both fingerprint images. If the second set of images do not match, the images previously captured are replaced by those captured the second time.

Because the right to left Closed Search procedures are installed and operated on each Remote Input Workstation, this function is operational regardless of whether or not either the communications network or the Central Site is operational.

Finger Image Upgrade

When the operator selects the Capture button on the *Add/Update* screen of the Remote Input Workstation, a capture session begins. Multiple images are taken of the fingerprint at different pressure levels. Once the maximum number of capture seconds (as defined in the .ini file, currently set to three (3) seconds) has passed, the message area on the *Add/Update* screen is replaced by a process meter. While the process meter is displayed, the system sorts the results placing the best *x* images (*x* equals the number of capture attempts defined in the .ini file) at the top of the list to be processed. These images are then put through a more extensive Motorola/Printrak quality check. Once each of the images has been processed, the data is again sorted. The first sort criterion is the Fast Image Quality (FIQ) value. In the event that multiple images have the same FIQ value, the Contextual Enhancement Processor (CEP) and Check Image Quality (CIQ) values are used to break the tie. If the top image based on the secondary sort is of acceptable quality, the process will continue and prompt the operator to either capture the next finger or to transmit the images. If the top image is deemed unacceptable, the application displays an error message.

Deleted: Printrak

RFP OSI 2046 CURRENT SYSTEM

The operator acknowledges the message and the application prompts the operator to attempt to capture the fingerprints again. This can happen up to three (3) times before the software either chooses the best of the poor quality images, or determines that the prints are unacceptable. If a print is deemed of unacceptable quality, no image is saved and the client will not have the given fingerprint on file. SFIS displays an error message.

In the event that a client has two (2) unacceptable quality images, the client's fingerprints cannot be used in the matching process. SFIS logs all replacement transactions and provides the capability to report all replacement transactions. All replaced fingerprint images are written to off-line storage.

SFIS automatically replaces finger images with a higher quality image if a match is detected during the search process. Upon capture, all fingerprint images receive a set of quality scores from the Motorola/Printrak AFIS. These scores include the following:

Deleted: Printrak

- Contextual Enhancement Processor (CEP): CEP has four (4) possible values: zero (0) or Bad, fifty-five (55) or Poor, eighty (80) or Fair, and ninety-five (95) or Good.
- Check Image Quality (CIQ): There are five (5) image quality routines the print is run through. The CIQ number represents how many of Motorola/Printrak's quality measurement routines the fingerprint passed.
- Number of minutiae points: Less than forty (40) is considered poor quality.
- Grayscale Dynamic Range: Dynamic range value is the difference between the maximum distinct shades of gray and the minimum distinct shades of gray. Grayscale ranges less than one hundred (100) are considered poor quality.
- Gray Scale Values: This is the number of distinct shades of gray that are found in a given image. Less than seventy (70) grayscale values is considered poor quality.

Deleted: Printrak

Quality is automatically measured at the workstation, and the quality ratings for saved images are stored in the fingerprint database. If a match is detected, and if the search image has a higher quality rating than the file image, then the file image is replaced by the search image.

RFP OSI 2046 CURRENT SYSTEM

When the fingerprint images in the database record are from the converted AFIRM database, SFIS automatically replaces the AFIRM fingerprint images with the search record fingerprint images.

Fingerprint Image Quality Check

Upon capturing a fingerprint image, the Remote Input Workstation automatically determines if the image passes Motorola/Printrak's quality determination procedures. The Remote Input Workstation then informs the operator whether or not fingerprint images meet the system criterion for acceptability.

Deleted: Printrak

This image quality check is performed before the fingerprint image capture process is completed; if necessary, the operator is asked to recapture substandard images. If the image is not acceptable the workstation will display a Poor Quality Fingerprint Image message box, requesting the poor quality fingerprint image be recaptured and providing suggestions for improvement. The operator acknowledges the message and restarts the capture process for that fingerprint image.

Individual print quality indicators are stored with each record, allowing substitution of higher quality print images should they become available. For example, if the original print in the database (the file print) had a CIQ score of three (3), and a newly entered print (the search print) had a CIQ score of zero (0), then the original, better-quality print would be retained in the database. However, if the file print had a CIQ score of three (3) and the search print has a CIQ score of four (4), then the search print would replace the file print.

Because the quality-check procedures are installed and operated on each remote workstation, quality check is operational regardless of whether or not either the communications network or the Central Site is operational. Historically, one-half of one percent (0.5%) of all images entered into all input workstations connected to SFIS may be marked as "unusable."

RFP OSI 2046 CURRENT SYSTEM

The quality-check software used in SFIS has an adjustable threshold. Currently, the system rejects less than one-half of one percent (0.5%) of the fingerprint images; however this threshold may be adjusted by the current Contractor by written approval of the State. SFIS' incorporation of EXPERT Matching allows the threshold on the quality check to be changed to meet the current requirement and still achieve the required accuracy.

Photo Image Capture

During data entry at the SFIS Remote Input Workstation, a client color photograph is taken. When the operator is ready to capture the photo of the client, a single-key stroke by the operator freezes the image and stores it into local memory. Please refer to the Client Input and Portable Input Workstation User Guides, and the SDD for in-depth descriptions and screen captures of this process.

Photo Image Recapture

SFIS is capable of photo capture/recapture. The operator is able to capture a photo prior to SFIS Open or Closed Search requests. The capture of a photo is not required in transactions such as a match between two (2) existing client records on the database. If the matching/verification process results in a match, the most recent photo replaces the older photo on file.

The operator may select the Retake button to specify that a photo should be retaken at a later date or immediately. In the case of desiring to retake it later, this information is used to generate a report to be acted on by the county. Please refer to the Client Input Workstation User Guide, and the Portable Input Workstation User Guide for in-depth descriptions of this process.

**RFP OSI 2046
CURRENT SYSTEM**

Verification and Fraud Investigation Requirements Only

Side-by-Side Display

SFIS provides a side-by-side split-screen display of the following:

- The photo image of the search record (Applicant) and each candidate (File) photo image for comparison by the operator (all photo images displayed on-screen are in twenty-four (24) bit color).
- The fingerprint images of the search record (Applicant) and each candidate (File) fingerprint images for comparison by the operator (fingerprint images displayed on-screen are in either eight (8) bit gray scale images or skeleton images at the option of the user).

The system displays the applicable alphanumeric data screen for each candidate photo and/or fingerprint image when the images are viewed alongside the photo and/or fingerprint images of the record.

System Administration Workstation Requirements Only

Search Status

The transaction status of all transactions is displayable on all SFIS workstations subject to the user's access permission level. For an in-depth description of the Queues Function, please refer to the System Administration Workstation User Guide.

**RFP OSI 2046
CURRENT SYSTEM**

C. END USER FUNCTIONALITY

SFIS users have access to many different functions, which are determined by their User IDs, security levels, and the equipment attached to their workstations (The exact same application is loaded on every remotely located workstation.). The following paragraphs describe the different types of functionality used by the different types of users, which include the following: Client Input, Portable Input, Fraud Investigation, System Administration, and Project Management Workstation. (Functions used by a Multifunction user have not been specifically described, since these functions fit into one (1) of the other described user types. The Multifunction Workstation has the same equipment as the Client Input Workstation and differs in name only. The Multifunction Workstation is used in counties where the workstation is shared by its users. For example, if a Fraud Investigator uses the same workstation as the Client Input Worker; it is a Multifunction Workstation.) Additional references to these functions are included in the SFIS User Guides.

ALL USERS

Since all workstations contain the same application, workstation functionality is available at any workstation and is therefore driven by the user Logon ID and by the equipment attached to the workstation. For example, if a Fraud Investigator (D Level) logs onto a workstation referred to by the project as a "System Administration Workstation (SAW)," the investigator will access all of the Fraud Investigative functionalities, however a scanner may be attached to the workstation. If a Client Input Operator (A-C Levels) logs on to a workstation referred to by the project as a, "Fraud Investigation Workstation (FIW)," the operator will have access to all of the Client Input Workstation (CIW) screens, however they will not be able to take fingerprints unless the FIW has a scanner attached to it.

All SFIS users utilize the following functions:

Windows NT Logon

The user must logon to the workstation at the beginning of each capture session and/or each time it has been left inactive for fifteen (15) minutes. The users follow the following steps to logon:

- Windows NT will display the message: "Press Ctrl + Alt + Delete to Log on", as shown below.

RFP OSI 2046 CURRENT SYSTEM



Exhibit: Begin Logon Message

- The user will press the Ctrl, Alt, and Delete keys simultaneously.
- The logon information screen is displayed with “xxxx” pre-filled in the User Name field.
- The user will type xxxx in the Password field and press the Enter key. The Windows NT password is case sensitive and should always be lower case. Make sure the Caps Lock key is off. For security reasons, the password will appear as asterisks on the screen, as shown below.



Exhibit: Begin Logon Message

- The desktop will appear with the Start button in the lower left-hand corner of the screen.

Logon Function

Every authorized user of SFIS must have the security level necessary to gain access to the appropriate SFIS application. The SFIS application is initiated when the user selects the Start button located in the lower left-hand corner of the desktop. After selecting SFIS, but before logon, a message appears if the computer's internal date is older than the current SFIS release date. This could mean that the workstation's internal clock is not working and the battery needs replacing. The user is instructed to call the SFIS Help Desk.

RFP OSI 2046 CURRENT SYSTEM

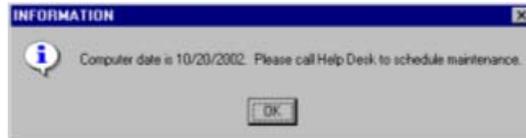


Exhibit: Computer Date Message

The SFIS Logon screen appears ready for logon by the user. Remote Input Workstation users log on to SFIS by entering a unique user ID and password or by capturing one (1) fingerprint image (fingerprint image Logon is not possible on Portable Input or Fraud Investigation Workstations).

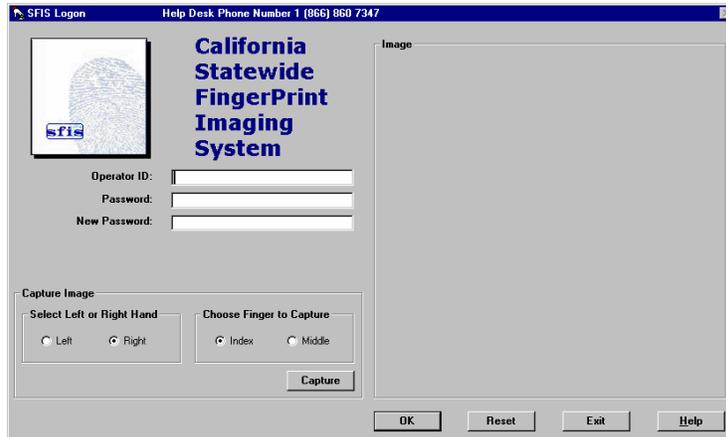


Exhibit: Logon Screen

All users are required to change their default password the first time they log on to the system. Password access is also required for Stored Transaction processing. Stored Transaction processing is defined as Portable Input Workstation or Multifunction/Client Input Workstation processing during Wide Area Network unavailability. Fraud Investigation and System Administration Workstation users also log on via user ID and password. However, System Administration Workstation users may use fingerprint logon, if they have a scanner attached to their workstation.

RFP OSI 2046
CURRENT SYSTEM

When the SFIS Logon screen appears, the operator ID field is active. The user begins the logon process by entering his/her user ID in the operator ID field and password in the Password field or capturing his/her fingerprint image. SFIS validates the user ID and determines whether to provide access to the system based on the password entered in the Password field or based on the fingerprint image captured in the capture area of the SFIS Logon screen. User ID, password, and password enabled or fingerprint enabled setup are assigned by a System Administrator through the Security screen function as described in the paragraphs that follow entitled, "Security Function."

For those users who will log on via fingerprint image, SFIS defaults to the right index finger. The Right radio button and the Index radio button will already be selected. The user may change to the left hand and the middle finger by selecting the appropriate radio buttons. For example, if the user decides to capture his/her left middle finger, he/she selects the Left field radio button, and selects the Middle radio button. SFIS then activates the Capture button.

SFIS informs the user that the capture process has begun by sounding a beep and displays the "Have finger ready for capture" message. The user selects the Capture button and SFIS displays the "Please wait for beep before placing finger on scanner" message. SFIS then beeps once and a "Place finger on scanner now" message appears. The user places the selected finger on the fingerprint scanner and waits for the scanning process to complete. SFIS performs a quality check on the fingerprint image to determine if an acceptable image was captured. If the fingerprint image is acceptable, minutiae points are extracted and used during the matching process. The Logon screen with the User ID and fingerprint image is displayed.

SFIS compares the user's fingerprint image captured at the time of logon with the fingerprint image on file for that User ID. If the comparison results in a match, the user has successfully logged on to the system, and the SFIS Bulletin Board window is displayed. If the comparison does not result in a match, the user is denied access to SFIS. If the user wishes to cancel the capture process, he/she selects the Exit button. If the user selects the Reset button, SFIS removes all data from the fields and the image capture area of the Logon screen and allows the user to restart the logon process. The Help button will take the user to the indexed help application.

RFP OSI 2046 CURRENT SYSTEM

For those users who log on to SFIS via password, the logon process begins by entering the user ID in the Operator ID field and his/her personal password in the Password field on the SFIS Logon screen. The user then selects the OK button or presses the <Enter> key. SFIS places an asterisk (*) for each character the user types in the Password field. The asterisks allow the user to determine how many characters were entered while keeping the password secure. The password is compared to the password on file for that user. If the password entered is not correct, the user will have two (2) more attempts to enter the correct password before the User ID is suspended. In order for the user to gain SFIS access again, an appropriately authorized county user must unlock the User ID.

If the Password or New Password fields contain invalid characters (valid characters are A-Z, a-z, and zero (0) - nine (9)), or invalid length (less than seven (7) or greater than eight (8) characters), or contain only characters (must have at least one (1) numeral), an appropriate message is displayed.

The first time a user logs onto the system using their password, SFIS prompts the user to change their password. The user is also prompted to change his/her password three (3) days prior to its expiration. At this point, the user enters a new password in the *New Password* field. The system displays a message if the user enters the same password as one (1) of the past five (5) previously used passwords, or if they use three (3) characters in common with the previous passwords. For more information on password security, refer to the paragraphs that discuss, "Security." The Password Verification window appears.



Exhibit: Password Verification Window

At any time during the logon process, the user may elect to exit the SFIS Logon screen by clicking the Exit button. The SFIS application terminates, and the user is returned to the Windows NT Logon screen.

RFP OSI 2046 CURRENT SYSTEM

Security information is added to SFIS through the Security function, as detailed in the paragraphs describing the, "Security Function." Using the Security function, a user ID is assigned and the user's fingerprint images are captured and a password assigned. Other security features such as User ID approval and assignment of additional user tasks by the State System Administrator and County Coordinators are described in the paragraphs that describe the, "Security Function."

Online Help

SFIS provides a Help Function that is accessible from every screen. The user selects Help from the toolbar to display the online Help. The information found within the Online Help closely parallels the step-by-step descriptions found in the SFIS User Guides.

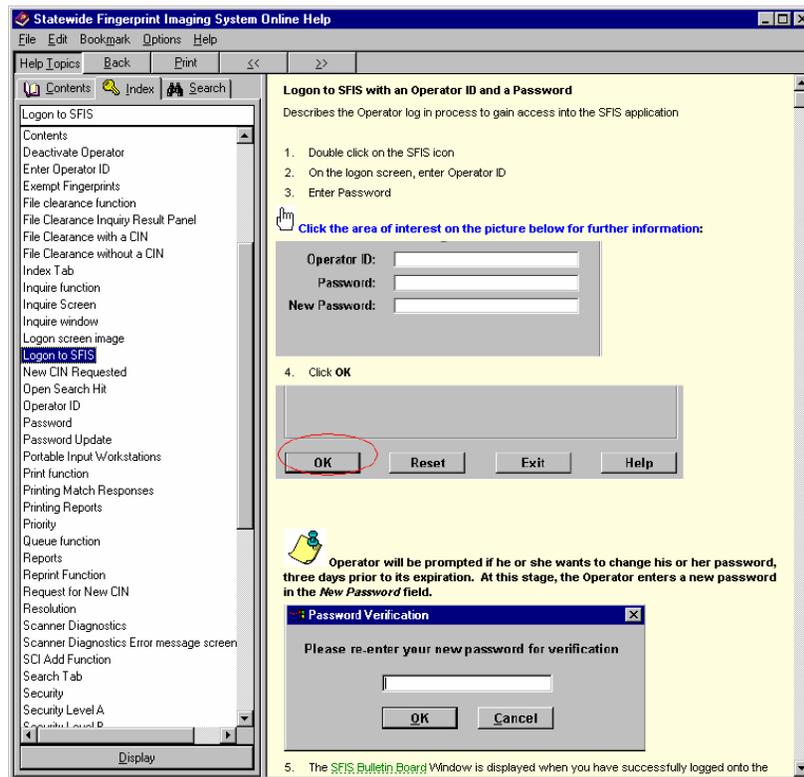


Exhibit: Online Help Index Window

RFP OSI 2046 CURRENT SYSTEM

There are several different ways the SFIS user can find Help topic information. When the user first enters the online Help, the Help Index window appears with all of the main SFIS help topics listed alphabetically by title. To quickly find an entry in the index, the user can type the beginning of the first word of the topic (or the entire first word of the topic) in the data entry field at the top of the index. The index will then automatically go to the first matching entry it finds. The user can then double-click on the desired topic, and more detailed information is displayed in the main window.

Another way to find topic information is by using the Contents tab. The Contents tab displays five (5) main SFIS topics, or books. The user can "open" the book by clicking on the plus (+) sign. More topics or chapters within the book are then displayed. The Contents topics are basically an online version of the User Guides.

The user can also use the Search tab to find a topic. After selecting the Search tab, the user enters search criteria (a word or partial word) into the data entry field. The Search function searches and then returns any topics containing the search criteria.

To return to the previous topic viewed, the user can press the *Back* button. To scroll through a given set of topics, the user can use the scroll buttons (<< >>) to scroll back and forth. To print a topic, the user presses the *Print* button. The topic is formatted for printing and prints at the user's default printer.

SFIS users can obtain additional help on every screen in the application by placing the mouse pointer over an area, waiting for it to turn into a hand, and pressing the left mouse button. A Help dialog box will appear.

CLIENT INPUT WORKSTATION USERS (ONLY) USER FUNCTIONALITY

The Client Input Workstation users are typically the only users that utilize the following functions:

**RFP OSI 2046
CURRENT SYSTEM**

File Clearance Function

The users from counties are able to execute a File Clearance transaction to search for the client CIN on the SCI database (This function is deactivated in Los Angeles County). The users are also able to request a CIN if it does not exist on the SCI database. The use of File Clearance is a county option. However, all counties use File Clearance functionality when processing Stored Transactions.

The users access the File Clearance function by selecting the File Clearance icon on the SFIS toolbar or File Clearance from the drop-down Function menu. The File Clearance window is displayed to allow users to enter the search criteria needed to query the SCI database.

The screenshot shows a software window titled "File Clearance" with a sub-header "SCI File Clearance". At the top left, there is a checkbox labeled "Available CIN" which is currently unchecked. To its right is a red dot and the text "Optional Fields". Below this is a section titled "Search Fields" containing several input fields: "CIN:" (empty), "Last Name:" (highlighted in red), "First Name:" (highlighted in red), "Middle Name:" (highlighted in red), "Appellation:" (highlighted in red), "SSN:" (containing "--"), and "Alien Number:" (highlighted in red). Below the search fields is a section titled "Clearance Filters" containing: "DOB:" (containing "00/00/0000"), "CA Drivers License:" (highlighted in red), "Range:" (with a dropdown arrow), and "Gender:" with radio buttons for "Female" and "Male". At the bottom of the window are four buttons: "OK", "Clear", "Print Scrn", and "Cancel".

Exhibit: SCI File Clearance

RFP OSI 2046 CURRENT SYSTEM

The user can use the CIN to perform a File Clearance. The user checks the Available CIN box, causing the CIN field to be the only available data entry field on the screen. Once the user has entered the correct information in the appropriate field and presses the OK button, the search is sent to SCI.

The user may also inquire on the client using one (1) or a combination of the following fields: SSN, Alien Number, First Name, or Last Name, simply by entering the information in the appropriate data fields on the File Clearance window. To enter information into these data fields, the Available CIN box must not be checked. Additional clearance filters may be added to further narrow the search on SCI. These filters are shown on the lower part of the screen in the area labeled Clearance Filters.

The information entered by the user is validated to ensure the user is inquiring using valid information. If an error is detected, the system displays an error dialog box and highlights the invalid entry, to request the data be corrected before the File Clearance can be performed. The File Clearance window also contains a Cancel button that allows the user to exit out of the File Clearance function. Once the user has entered the correct information in the appropriate fields, and presses the OK button, the search is sent to SCI.

Displaying Results

SCI will search its database for the closest match based on the search criteria entered in the File Clearance window. If the CIN is used as the search criteria, SCI will return one (1) record if the CIN is found, no records if the CIN is not found, and zero (0), one (1), or multiple candidates (up to twenty-five (25)) if search criteria other than CIN are entered.

RFP OSI 2046 CURRENT SYSTEM

CIN	SSN	LIN	Last Name	First Name	Date of Birth
74048991H	540-00-0010	90-55-126425-1-08	BEAN	GREENLY	11/17/1960

Exhibit: SCI Inquire Function Screen

If more than twenty-five (25) records exist, SFIS displays an error message.



Exhibit: SCI File Clearance Error Message

The client data retrieved from SCI and the photo image from SFIS are displayed for the first record in the inquiry results panel. Each record in the inquiry results panel is displayed by CIN. Other columns include SSN, LIN, Last and First Name, and Date of Birth.

The user may view another record in the inquiry results panel by highlighting the record in the panel with the mouse pointer. The SCI Inquire screen is populated with the client data and photo, if available, for the selected record. The user views each record in the inquiry results panel until the correct record is found, or until he/she reaches the end of the list.

If a matching record is found from the inquiry results panel, the user clicks on the Add/Update button. The client information of the selected record is populated on the Add/Update screen and the user is able to modify the client information online.

RFP OSI 2046 CURRENT SYSTEM

If the desired client is not in the inquiry results panel, the user may press the Cancel button to exit the screen and return to the File Clearance function to try the search with new or additional search criteria. If the desired client is not in the inquiry results panel, and no new or additional information is available, a new CIN may be requested for the client by selecting the Request New CIN button. Requesting a new CIN should only be used once all potential search criteria for SCI have been exhausted.

Request for New CIN

If none of the results in the inquiry results panel match the SFIS client, the user is able to request a new CIN by pressing the Request New CIN button. As previously mentioned, when a new CIN is requested, it should be used to track the client throughout any other systems such as SAWS or MEDS. The Request New CIN button is available on the SCI Inquire screen for those instances when SCI returned candidates, but none are determined to be the client. This button “forces” SCI to issue a new CIN by bringing up the SCI Add screen.

If no record returns from SCI during a File Clearance transaction, a message window is displayed for the user to request a new CIN by selecting Yes or No.

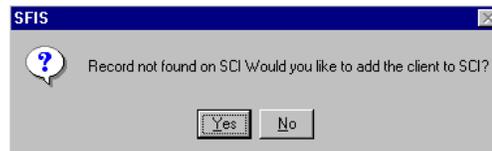


Exhibit: CIN Request Message

If the user chooses No, another File Clearance may be conducted with different search criteria to attempt to locate the correct candidate.

If the user chooses to add a new CIN for the client, the SCI Add screen appears.

**RFP OSI 2046
CURRENT SYSTEM**

The screenshot shows a window titled "SCI Add" with a close button in the top right corner. Below the title bar, the text "SCI Add" is centered. To the right of this text is a green dot followed by the text "Optional Fields". Below this is a section titled "Client Information" enclosed in a light gray border. Inside this section are several input fields: "Last Name:" with an empty text box; "First Name:" with an empty text box; "Middle Name:" with a green highlighted text box; "Appellation:" with a green highlighted text box; "DOB:" with a text box containing "00/00/0000"; "SSN:" with a green highlighted text box containing "- -"; "Alien Number:" with a green highlighted text box; "Drivers License:" with a green highlighted text box; "Mother's Maiden Name:" with a green highlighted text box; and "Birthplace:" with a green highlighted text box. To the right of these fields is a "Gender" section with two radio buttons: "Female" and "Male". At the bottom of the window are four buttons: "Add", "Clear", "Print Scrn", and "Cancel".

Exhibit: SCI Add Screen

The SCI Add screen is displayed requesting the user to enter the demographic information for the client. Data elements that are requested by SCI to assign a new CIN include:

- Local Identification Number (LIN);
- Social Security Number (SSN);
- Alien Number (if any);
- Name;
- Date of Birth;
- Gender;
- Mother's Maiden Name;
- Birthplace; and
- Drivers License Number (if any).

RFP OSI 2046
CURRENT SYSTEM

The information entered is edited to ensure the information is valid. After completing the data entry, the user clicks on the Add button to send the request to SCI. The Cancel button is also available if the user decides to cancel the request. Once the user sends the information, SCI will assign a new CIN for the requested client and return the CIN to the SFIS workstation. A message with the new CIN is displayed on the screen. The user clicks on the OK button, or presses <Enter> to close the window and enter the Add/Update screen.

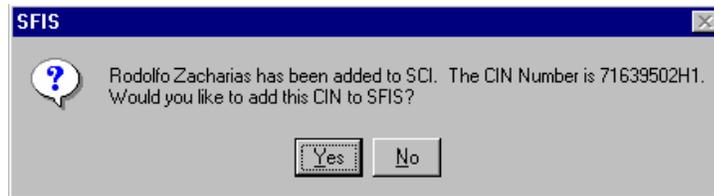


Exhibit: CIN Return Message Window

Refer the following paragraphs, "Add/Update Function," for a description of the Add/Update process.

**RFP OSI 2046
CURRENT SYSTEM**

**CLIENT INPUT WORKSTATION AND SYSTEM ADMINISTRATION
WORKSTATION ONLY**

The Client Input Workstation and System Administration Workstation are used to access the following functions:

Resolution Function

Security Level B, C, or E is needed to be able to access the Resolution Function, but authorization may be granted to a Security Level A user through special customization (See Security Function description). Open Search Match responses and Closed Search No Match responses (unexpected results) returned to the workstation are also placed on a Resolution Queue for the county. The purpose of the Resolution Function is to enter the results of research of Unexpected Results (Open Search Match responses or Closed Search No Match responses). The Resolution function is accessed by selecting the Resolution icon from the toolbar or by selecting Resolution from the drop-down Function menu.

The screenshot shows a window titled "Resolution Function". At the top, there is a table header with the following columns: Appl Last Name, Appl First Name, Appl DOB, Appl CIN, Ind, Appl EW, File Last Name, File First Name, File DOB, File CIN, and Date. The table body is currently empty. Below the table, there are two main sections: "Resolution Options" and "Comments to Investigator".

Resolution Options:

- Administrative Situation
- Reason Code:
- Cleared By:
- Possible Fraud

Comments to Investigator:

At the bottom of the window, there are five buttons: OK, Print Screen, Cancel, Apply, and Print.

Exhibit: Resolution Queue Screen

RFP OSI 2046 CURRENT SYSTEM

For each Open Search Match or Closed Search No Match Response on the queue, the following fields are displayed:

- Applicant Last Name;
- Applicant First Name;
- Applicant DOB;
- Applicant CIN;
- One-to-One Indicator (whether it is an Open Search or Closed Search);
- Case Eligibility Worker (if more than one (1) worker number was entered, only one (1) Worker Number will be shown in the precedence order of CalWORKs, Food Stamps, and GA/GR);
- File Last Name;
- File First Name;
- File DOB;
- File CIN (Open Search Match only); and
- Date Matched.

Below the rows displayed on the queue is an area to record the results of the county's research.

To record the county results, the user highlights the row in the queue area, causing the lower part of the screen to activate. The user then chooses a Resolution Option to complete the resolution process:

Administrative Situation (Code: AS) – The County determined that the Open Search Match or Closed Search No Match is not a potential fraud situation. For example, the client was previously on aid in another county, but that aid was terminated when the client moved to the current county.

Possible Fraud (Code: PF) – The County determined that the case may be a possible fraud situation and should be researched by a Fraud Investigator.

The user chooses either Administrative Situation or Possible Fraud by clicking the correct radio button. If the user chooses Administrative Situation, the Reason Code is entered via a drop-down selection box. The drop-down selection box will include the text for the reason code entered by the County Coordinator.

RFP OSI 2046 CURRENT SYSTEM

A worker number is also entered into the Case Cleared By field to indicate the county staff member who determined that the Match Response was an Administrative Situation.

Comments directed to the Fraud Investigator may also be added in the Comments field in the lower part of the screen. Records marked as an Administrative Situation are placed on the administrative section of the Fraud Investigator's queue and those marked Possible Fraud are placed on the possible fraud section of the Fraud Investigator's queue. Any rows on the resolution queue that are not marked as Administrative Situation or Possible Fraud remain on the Fraud Investigator's queue as pending Resolution.

Once the user has finished marking the resolution determination, he/she clicks the OK button to update the record and exit. Or, the user can select the Apply button if they want to continue resolving more responses. After the resolution is complete, a confirmation message box appears.

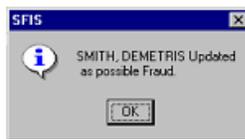


Exhibit: Resolution Confirmation Message Box – Possible Fraud

SFIS then moves the record to the appropriate section of the Fraud Investigator's queue and it is removed from the Resolution queue.

The State System Administrator has the capability to view all county pending resolution records while the county personnel will only be able to view and resolve pending resolution specific to their county.

RFP OSI 2046 CURRENT SYSTEM

Scanner Diagnostics

The purpose of Scanner Diagnostics is to ensure that the scanner is functioning properly. A malfunctioning scanner may slow the operator down, requiring a client's finger images to be captured three (3) times for every client. Weekly diagnostics should be conducted using the Scanner Diagnostic test to confirm that the fingerprint scanner is operating within factory specifications.

Scanner Diagnostics' Test Instructions

1. Clean the scanner platen with the Windex and white wipes provided by the SFIS Help Desk.
2. From the Function drop-down menu, select Scanner Diagnostics.
3. Capture a blank image by selecting the Start button and then the Capture button on the Scanner Diagnostics screen.

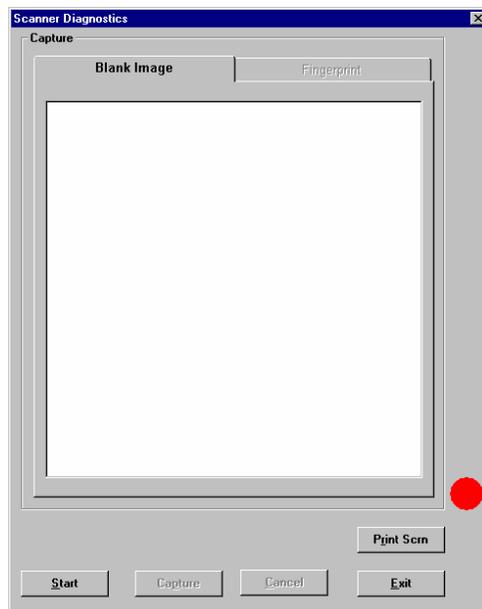


Exhibit: Blank Image Capture

RFP OSI 2046 CURRENT SYSTEM

4. If the Blank Image test passes, the Fingerprint tab is enabled. Select the Start button, place a clean finger in the center of the platen and select the Capture button.

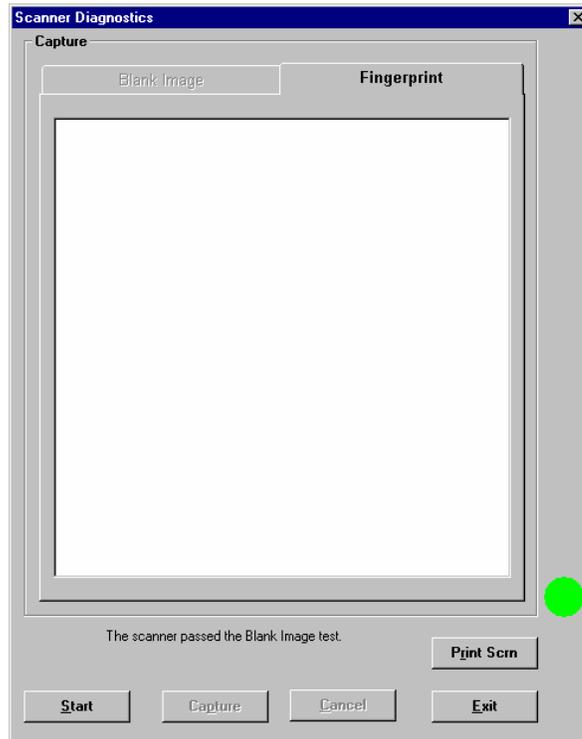


Exhibit: Fingerprint Image Capture

5. If the scanner passes the Blank Image diagnostic test, a green ball is displayed in the lower right hand corner of the Scanner Diagnostics window and text at the bottom of the screen appears stating: "The scanner passed the Blank Image test."
6. To print the Scanner Diagnostics window, select the Print Scrn button.
7. If both of the tests pass, select the Exit button and the test window will close.
8. If either or both of the tests fail, select the Exit button, and the message: "Are you sure you are finished with scanner diagnostic?" appears.

**RFP OSI 2046
CURRENT SYSTEM**



Exhibit: Scanner Diagnostics Exit Confirmation Box

9. If the Blank Image test fails, SFIS will prompt the operator to ensure that the scanner platen is clean and clear and to retest the Blank Image.

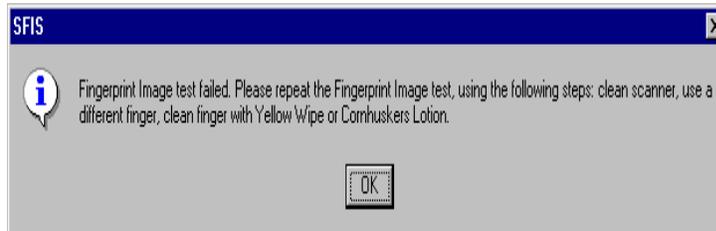


Exhibit: Failed Message – Scanner Diagnostics

10. If the Blank Image test fails three times, the operator will be instructed to contact the SFIS Help Desk to receive technical assistance.
11. If the Fingerprint test fails, SFIS will prompt the operator to ensure that the fingerprint is clean and centered and to retest the Fingerprint.
12. If the Fingerprint test fails three times, the operator will be instructed to contact the SFIS Help Desk to receive technical assistance.

RFP OSI 2046
CURRENT SYSTEM

Replacing Platen on Fingerprint Scanner

The platen on the Fingerprint Scanner is easily damaged and subject to wear, so care should be taken when using or transporting the Fingerprint Scanner. The platen will need to be replaced periodically. The SFIS Help Desk supplies replacement platens to the county upon request. The platen is designed for easy replacement:

1. Disconnect the power cable from the back of the Fingerprint Scanner.
2. Using the T10 Hex-Wrench, remove the screw on the front of the Fingerprint Scanner by rotating it counter clockwise.
3. Lift the black metal cover to gain access to the platen.
4. Lift the platen and carefully replace it with a new platen.
5. Reposition the black metal cover and tighten the screw by rotating it clockwise.
6. Reconnect the power cable to the back of the Fingerprint Scanner.

**RFP OSI 2046
CURRENT SYSTEM**

**CLIENT INPUT WORKSTATION, SYSTEM ADMINISTRATION WORKSTATION,
AND FRAUD INVESTIGATION WORKSTATION USER FUNCTIONALITY**

The following functions are only used by the Client Input, System Administration, and Fraud Investigation Workstations:

Print Function

The Print function allows users to print or reprint Match Responses and batch cycle generated reports. Every SFIS workstation (except the Portable Input Workstation) is equipped with a high-resolution laser printer.

The users access the Print function by selecting the Print icon on the SFIS toolbar, or by selecting Print from the drop-down Function menu.

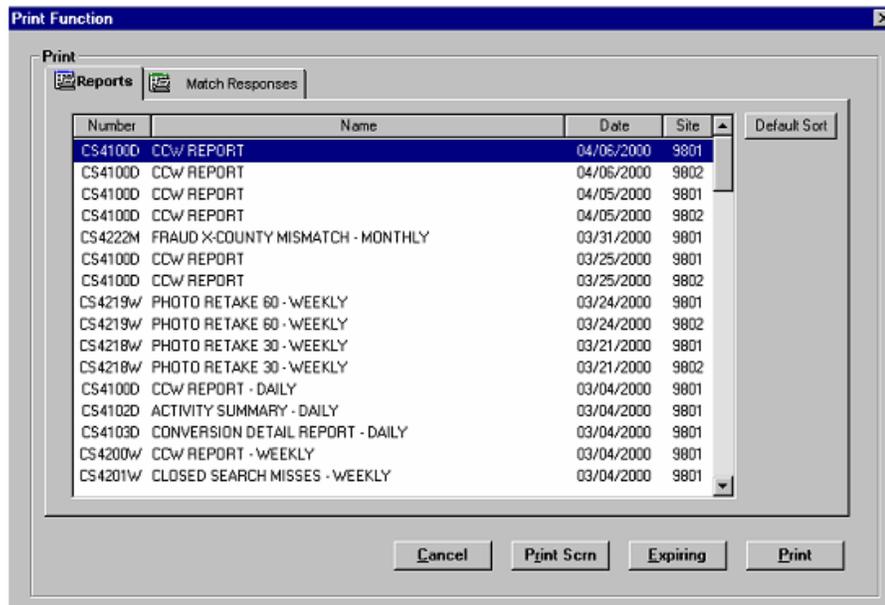


Exhibit: Print Function Screen

The user may click on the Cancel button on the bottom of the Print Function screen to exit at any time.

The Print screen displays two (2) tabs: The Reports tab and the Match Responses tab. Each of these tabs is described in the following subsections.

RFP OSI 2046 CURRENT SYSTEM

Printing Reports

The Reports tab is the active tab upon entry into the Print Function screen. If the user sees the report they desire on the Report tab list, they may highlight the desired report and click on the Print button. If the user is unable to locate the desired report he/she may click the Expiring button, which is also located on the toolbar, enter the requested report and date information, then print. The selected report is retrieved from the database, transmitted to the workstation, and printed on the local laser printer. Reports remain on the Report tab list as follows:

- Daily Reports – Remain on the list until the next daily report for the next business week is generated, i.e. the Monday report is on the list until the Monday report for the following week is generated.
- Weekly Reports – Remain on the list for four (4) weeks from the day on which it was generated.
- Monthly Reports – Remain on the list until creation of the next monthly report.
- Annual Reports – Remain on the list until creation of the next annual report.

If the desired report is no longer on the Report tab list, but is still maintained in the database, the user may obtain a printout of the report by pressing the Expiring button on the Report tab. Reports are retained on the database as follows:

- Daily Reports – Available through the end of the month following the month in which the report was created, i.e. June daily reports are available until the end of July.
- Weekly Reports – Available through the end of the month following the month in which the report was created, i.e. weekly reports created in June are available until the end of July.
- Monthly Reports – Available for twenty (20) months from the creation month.
- Annual Reports – Available for five (5) years from the creation date.

RFP OSI 2046 CURRENT SYSTEM

The Report Reprint window appears with the Report Date, Report Number, and Report Name fields filled in. The user may change these fields to select a different report to be reprinted. To print the selected report, the user clicks the OK button. The Cancel button cancels the print request transaction.

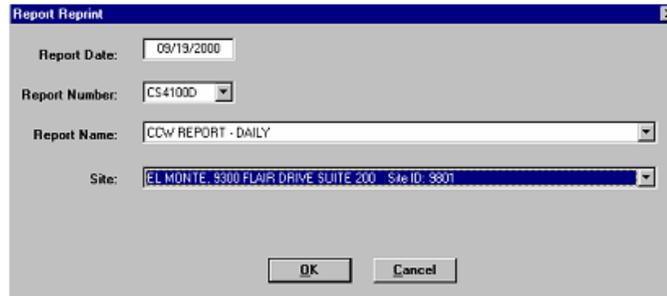


Exhibit: Report Reprint Window

The validity of the report date is checked against the SFIS database. If the date is not valid, that is, no such report was generated on this date, an error message window is displayed. If both the Report Number or Report Name and Report Date are valid, the report for the specified date will be reprinted on the laser printer associated with the user's workstation.

Reports are displayed on the Report list and reprint is allowed at the site level for enabled security levels A, B, and C. Security level D (Fraud Investigator) and E (County Coordinator) have access to all county reports. Security level F (CDSS) has access to State reports designated for routing to the California Department of Social Services (CDSS). Security level G (State System Administrator) has access to reports at a statewide level. The Max Range Report Date field is for specifying the date range of reports to be printed and is granted only to security level G users.

Printing Match Responses

Match Responses are the print out results/responses that the county receives from SFIS when an Open or Closed Search is conducted. Upon entry into the Print Function screen, the user may select the Match Responses tab.

**RFP OSI 2046
CURRENT SYSTEM**

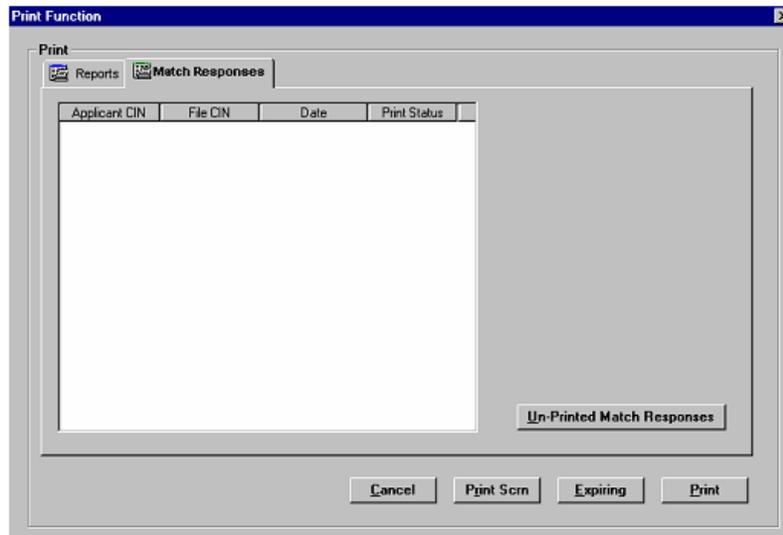


Exhibit: Match Responses Tab

If the user sees the Match Response they desire on the Match Response tab list, they may highlight the desired response and click on the Print button.

The selected Match Response will be retrieved from the database, transmitted to the workstation, and printed on the local laser printer. The Match Response will contain the demographic information and photos that were transmitted with the Open or Closed Search. If another search is completed on the same CIN, a new Match Response will be created. The new Match Response will contain the demographic information and photos from that specific search. If the first Match Response is reprinted, it will print the demographic information and photo that was transmitted with the original search; it will not be updated with the demographic information or photo from the new search.

RFP OSI 2046 CURRENT SYSTEM

Match Responses remain on the Match Response tab list for two (2) days following completion of the matching process. If the desired response is no longer on the Match Responses tab list, the response is still maintained in the database until sixty-one (61) days have elapsed. During this period, the user may obtain a printout of the Match Response by clicking the Expiring button. This is only true if the CIN is not used as the applicant CIN in any other search transaction. Security level G users can use the Expiring option to request a Match Response that includes fingerprints.

The user enters the CIN in the CIN field for the Match Response desired. The user then clicks the OK button to have the most current Match Response printed.

If a Match Response for the entered CIN is not available on the database, that is, sixty-one (61) days or more have elapsed, an error message will be displayed in red on the Match Response Reprint screen. Pressing the Clear button to allow entry of another CIN in the CIN field may then clear the Match Response Reprint window. The user may also exit the Match Response Reprint window at any time by clicking the Cancel button.

The user may elect to print all Match Responses that have not been printed by clicking the Un-Printed Match Responses button.

Inquire Function

The Inquire Function is used to view client demographic information and the client photo image, if available. Client information, the status of fingerprint images, and photo image for any client in the SFIS database may be viewed. (Images cannot be captured from the Inquire screen.)

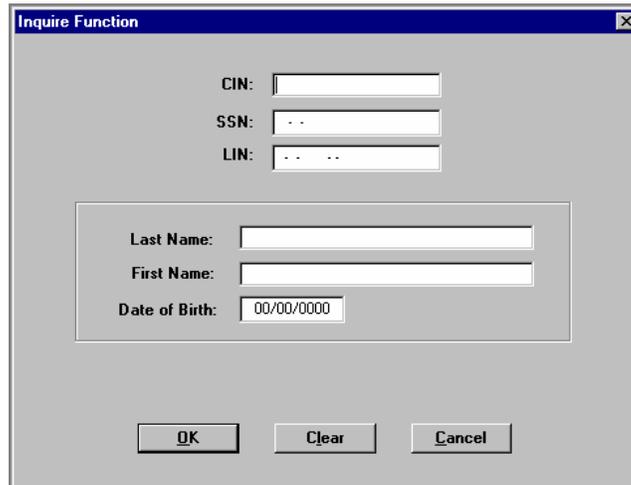
Client Input and System Administration Workstation View of Inquire

Users access the Inquire function by selecting the Inquire icon on the toolbar or selecting Inquire from the drop-down Function menu. The Inquire function enables SFIS users to view client demographic information, the status of fingerprint images, and photos for any active client on the SFIS database, if available. Active clients are those that have not been deactivated by the State System Administrator. Users may inquire on SFIS clients using any one (1), or a combination of the following:

RFP OSI 2046 CURRENT SYSTEM

- CIN;
- Social Security Number (SSN);
- Local Identification Number (LIN); and
- First and Last Name and Date of Birth.

To begin the Inquire function, the user clicks on the Inquire icon, or selects Inquire from the drop-down Function menu.



The screenshot shows a dialog box titled "Inquire Function". It contains the following fields and controls:

- CIN: [Text Input Field]
- SSN: [Text Input Field with mask: - -]
- LIN: [Text Input Field with mask: - - -]
- Last Name: [Text Input Field]
- First Name: [Text Input Field]
- Date of Birth: [Text Input Field with mask: 00/00/0000]
- Buttons: OK, Clear, Cancel

Exhibit: Inquire Function Window

The Inquire Function window contains six (6) fields: CIN, SSN, LIN, First Name, Last Name, and Date of Birth. The user may inquire using any single item or combination from CIN, SSN, or LIN, simply by entering the information in the appropriate data field and clicking on the OK button, or pressing <Enter>. Inquiries using first and last name and date of birth must begin by entering all three (3) data elements and clicking the OK button, or pressing <Enter>.

The information entered by the user is edited online to ensure the user is inquiring on valid data, such as the Date of Birth containing a valid date. The system displays an error dialog box, and highlights the invalid entry, to request that the data be corrected before the inquiry can be performed.

RFP OSI 2046 CURRENT SYSTEM

The Inquire Function window also contains a Cancel button that allows the user to exit out of the Inquire Function. Once the user has entered the correct information in the appropriate field(s) and pressed the OK button, the Inquire Function window disappears, and the Inquire Display screen appears.

For those cases where the demographic information and photograph image reside on the SFIS database, the Inquire Display screen fields are populated with the information retrieved from the database, and the photo image is displayed. If a photo image is not on file with SFIS, only the demographic information is displayed. The fingerprint image status is also displayed in the demographics area of the screen.

The Inquire Display screen displays the record or records returned from the inquiry in the queue area at the bottom of the screen. The record displayed is known to SFIS, with demographic information and photograph image retrieved from the SFIS database.

The screenshot shows the 'SCI Inquire Function' window. It is divided into several sections:

- Case Information:** A form with fields for CIN (748499TH), SSN (540-00-0010), LIN (98-55-1266425-1-08), EW Number (2235), Program Type (GR/GA), Last Name (BEAN), First Name (GREENLY), Date of Birth (11/17/1960), Gender (MALE), Photo Image (CAPTURED), Left Image (CAPTURED), and Right Image (CAPTURED).
- Case Photo:** A large gray area with the text 'Photo' centered, indicating a missing image.
- Comments:** A text area for user notes.
- Table:** A table with columns: CIN, SSN, LIN, Last Name, First Name, Date of Birth. It contains one row: 748499TH, 540-00-0010, BEAN, GREENLY, 11/17/1960.
- Buttons:** Display, Add/Update, Request New CIN, Print Scrn, and Cancel.

Exhibit: Inquire Display Screen with Client Information

If the inquire was performed using a CIN only, one (1) result will be listed. The information returned can be displayed in more detail in the Case Information section of the screen. To view the associated photo image (if available), click on the Display button.

RFP OSI 2046 CURRENT SYSTEM

If the inquire was performed with data elements other than CIN, multiple records may be returned in the inquiry results area of the screen. To view the image associated with a CIN, highlight the desired CIN, and click on the Display button.

To access another record in the list, highlight the row in the inquiry results panel, then click on the Display button or double click on the row. More detailed information related to the highlighted CIN is displayed in the Case Information area of the window. The associated photo, if available, is displayed. If the displayed record has multiple SSNs or LINs, the user may view all information by clicking on the arrow associated with the SSN or LIN field. This action will cause a drop down list to appear with the other SSNs or LINs shown.

The user views each record in the inquiry results panel until satisfied with the search results. If the client in question is found in the inquiry results panel, the user may go directly to the Add/Update function, to update or verify the existing fingerprint images, photo, and demographic information. To access the Add/Update function, the user presses the Add/Update button. Or, if another query is desired, the user selects the Cancel button. Inquire may then be selected from the Function drop-down menu or by clicking on the Inquire button on the toolbar.

If the CIN is not known to the SFIS database, the message "Record Not Found" instructing the user to inquire with a different value appears.

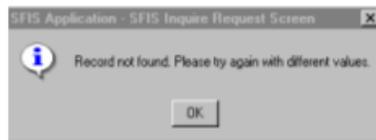


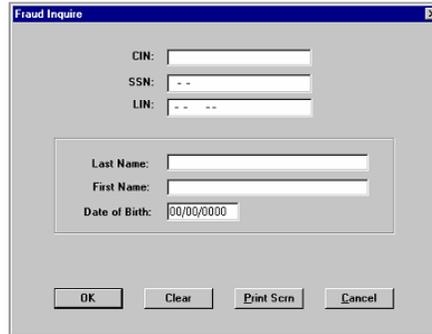
Exhibit: CIN Not in SFIS Message Window

The user selects the OK button to acknowledge and remove the message window from the screen. The user may then verify that a correct value was entered. If yes, then the user would contact their County Coordinator. If no, the user would correct the information and inquire again. To exit the Inquire function, the user clicks on the Cancel button.

RFP OSI 2046 CURRENT SYSTEM

Fraud Investigation Workstation View of Inquire

The Fraud Investigators also have the ability to request the images of any active CIN in the database, by submitting a request on the Fraud Inquire window. Selecting the Fraud Inquire button on the toolbar or from the drop-down Function menu accesses the Fraud Inquire window.



Fraud Inquire

CIN:

SSN: --

LIN: -- --

Last Name:

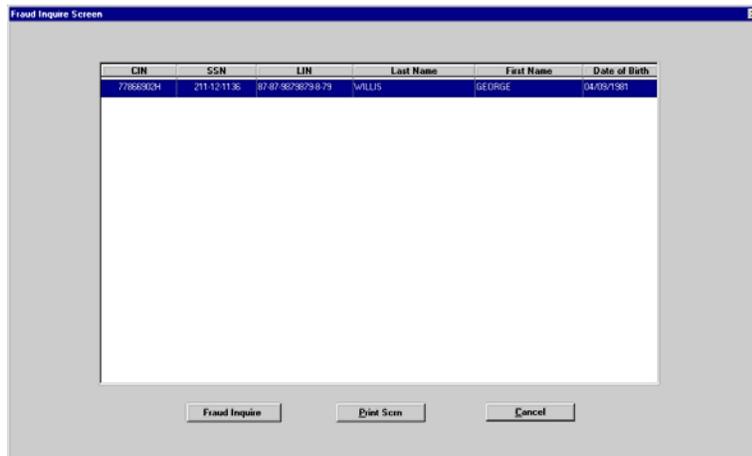
First Name:

Date of Birth: 00/00/0000

OK Clear Print Scrn Cancel

Exhibit: Fraud Inquire Window

The Fraud Investigator may inquire using CIN, SSN, or LIN individually. Additionally, an inquiry may be made using the combination of Last Name, First Name, and Date of Birth. The results of all inquiries are returned in a queue.



Fraud Inquire Screen

CIN	SSN	LIN	Last Name	First Name	Date of Birth
7286904	011121136	87879879879	WILLIS	GEORGE	04/03/1981

Fraud Inquire Print Scrn Cancel

Exhibit: Fraud Inquire Screen

RFP OSI 2046 CURRENT SYSTEM

The Fraud Investigator chooses an appropriate result from the Fraud Inquire screen by highlighting the row and clicking on the Fraud Inquire button. A message occurs if a record is selected that already resides on their Fraud Inquire List.

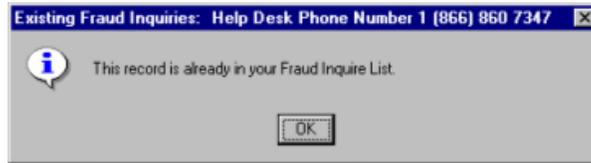


Exhibit: Existing Fraud Inquire Message

Given the record is not already on the Fraud Investigator's Fraud Inquire List, two scenarios can then occur. If the images for this CIN have not previously been requested by any user, a new record is created. This is the most likely scenario. However, if records exist that were previously requested by another Fraud Investigator, the Existing Fraud Inquiries window appears as explained below.



Exhibit: Existing Fraud Inquiries Window

The Existing Fraud Inquiries window allows the Fraud Investigator to see a list of any existing fraud inquiry requests, when they were requested, and who requested them. The list is sorted by CIN and Request Date with the most current date listed first. If the current Fraud Investigator has previously requested a copy of the record it will be listed at the top. The list may contain groups or multiples of records containing the same capture date. In this case the only record that can be selected is the top record of the group (the one containing the CIN).

RFP OSI 2046 CURRENT SYSTEM

The Fraud Investigator has the option of selecting one or more of the existing requests in the list, or requesting the most current images using the New Record button. To select an existing request, the Fraud Investigator highlights a record in the left side list and then clicks the Add (>) button to move the record to the right side list. To undo a selection, the record in the right side list is highlighted and the Remove (<) button is clicked. The New Record button is disabled whenever the Add button is clicked. When the Remove button is clicked and it is the last record on the right side, the New Record button is again enabled. If a record is selected containing the current Fraud Investigator's ID in the Operator column, the message "This record is already in your Fraud Inquire List" is displayed.

To cancel at any time, the Cancel button is pressed to close the window and exit. If records have already been selected and the Cancel button is pressed, a message is displayed.



Exhibit: Existing Fraud Inquiries Cancel Message

When all of the desired records have been moved to the right side list, the Fraud Investigator clicks on the OK button.

If the Fraud Investigator wants the most recent images instead of choosing any existing records in the list, the New Record button is pressed to create a new entry. If there is already a record in the list with a current capture date, a copy is just made of that record. This prevents unnecessary duplication of information in the Matched table.

Once the OK button is pressed, a message is displayed confirming that the request was processed.



Exhibit: Fraud Inquire Request Message

RFP OSI 2046 CURRENT SYSTEM

After the record is created at the initial Fraud Inquire screen or by using the Existing Fraud Inquiries window, the CIN is sent to the SFIS Central Site for retrieval upon request, and placed in the Fraud Investigation area of the database.

To display the records retrieved through the Fraud Inquire process, the Fraud Investigator selects the Fraud Inquire List radio button from the Queues area of the main Fraud Review screen and then clicks the OK button.

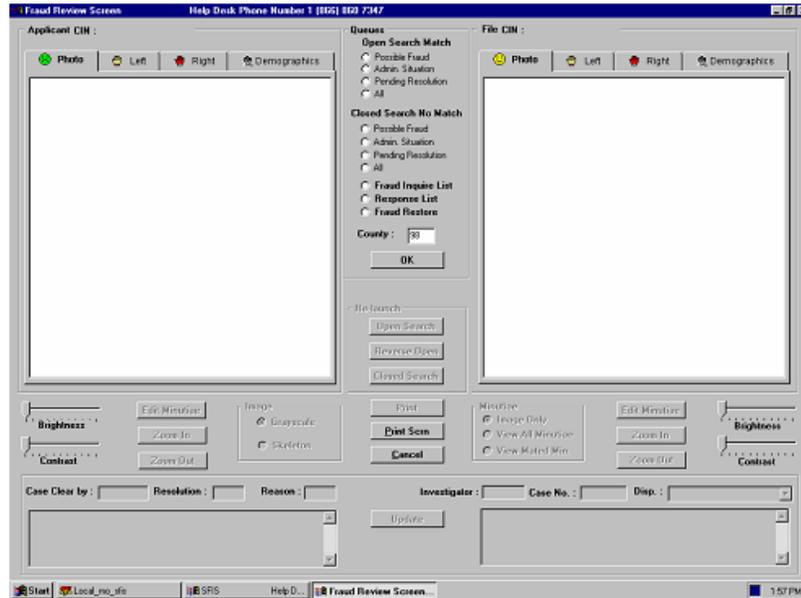
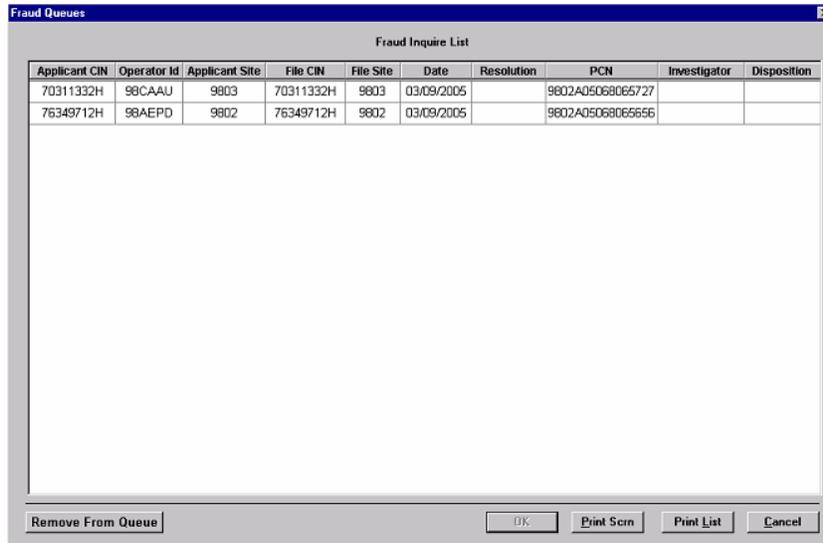


Exhibit: Fraud Review Screen

The Fraud Inquire List is then displayed. The Fraud Inquire List only displays Fraud Inquire records that the current Fraud Investigator has requested. Therefore, if the user wants a record that does not currently appear in their queue, they must perform the Fraud Inquire steps described above to view the record.

**RFP OSI 2046
CURRENT SYSTEM**



Fraud Inquire List

Applicant CIN	Operator Id	Applicant Site	File CIN	File Site	Date	Resolution	PCN	Investigator	Disposition
70311332H	98CAAU	9803	70311332H	9803	03/09/2005		9802A05068065727		
76349712H	98AEPD	9802	76349712H	9802	03/09/2005		9802A05068065656		

Remove From Queue OK Print Scrn Print List Cancel

Exhibit: Fraud Inquire List Screen

To display a record's images on the Fraud Review screen, the Fraud Investigator selects a CIN from the Fraud Inquire List and presses the OK button. The photo and fingerprint images are then displayed in the Applicant and File areas of the Fraud Review screen. The Remove from Queue button is used to manually remove records from the list when they are no longer needed. This removal applies only to the current Fraud Investigator's queue. If other investigators have requested a copy of the record it will still appear on their respective list.

**RFP OSI 2046
CURRENT SYSTEM**

***CLIENT INPUT WORKSTATION AND PORTABLE INPUT WORKSTATION
(ONLY) USER FUNCTIONALITY***

The Client Input and Portable Input Workstation users are the only users that utilize the following functions:

Stored Transactions

The purpose of Stored Transactions is to allow counties to image clients when the SFIS network is not available. Stored Transactions are used for the following reasons:

- The Client Input Workstation.
 - The network is experiencing problems and SFIS Help Desk instructs the county to use Stored Transactions or it is a State Holiday that the county does not observe.
- The Portable Input Workstation.
 - The County wishes to image clients at a remote site or at a home visit.

The transactions are saved to the workstation's hard drive and must be uploaded to the network for processing.

Client Input Workstations

When the SFIS network is unavailable, Client Input Workstations must operate in Stored Transactions' mode. The transactions are saved to the workstation's hard drive. Stored Transaction records on the Client Input Workstation must be uploaded within seven calendar days after they are created.

Use one of the below described methods to enter into Stored Transactions' mode:

Connection Method One – Used When Experiencing Network Problems:

1. When the Transmit button is selected from the Add/Update screen, and the network fails, a Database Error message is displayed to alert the operator.

RFP OSI 2046 CURRENT SYSTEM

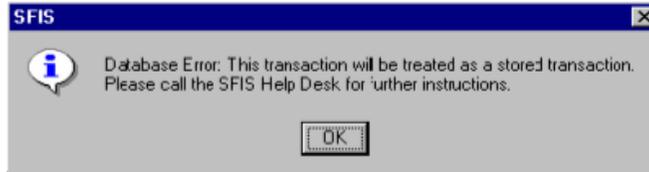


Exhibit: Database Error Message

2. The Database Error message instructs the operator to call the Help Desk. Select the **OK** button. The Help Desk operator will attempt to resolve the problem in a timely manner. If for any reason, the connectivity or central site problem is expected to continue for an extended period of time, the Help Desk operator will instruct the Client Input Workstation operator to continue processing in Stored Transactions' mode.
3. To capture images in Stored Transactions' mode, log completely out of SFIS.
4. To log into Stored Transactions' mode, use a new Windows NT user ID of **sfis_stored** and the new password of **sfis_stored**. (REMINDER: The ID and password are case sensitive. Do **NOT** activate the **Caps Lock** key on the keyboard.)
5. The Domain Controller/Logon message will appear explaining the absence of network connectivity. Select the **OK** button on the Domain Controller window (see below).



Exhibit: Domain Controller Window

6. At the SFIS Logon screen, use the same ID and password that is used in production.
7. Continue adding records in Stored Transactions mode.

RFP OSI 2046 CURRENT SYSTEM

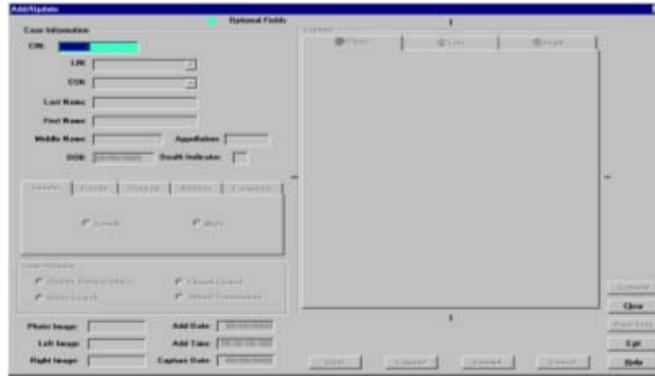


Exhibit: Stored Transaction Add/Update Screen

****Note:**

- Operators that log on to the system with ID and password will continue to do so.
- Operators that log on to the system with ID and fingerprints must now use ID and password logon. (The password was created when the operator first updated the default password, which expires and is updated every 90 days.)
- Passwords cannot be reset over the network while in Stored Transactions' mode. If an operator gets suspended, SFIS will allow the operator to continue using the Add/Update function in limited capacity, not allowing records to be copied from the hard drive to a zip disk.

Connection Method Two – Network Not Available (A State Holiday, for example):

1. To log into Stored Transactions' mode, use a new Windows NT user ID of **sfis_stored** and the new password of **sfis_stored**. (REMINDER: The ID and password are case sensitive. Do **NOT** activate the **Caps Lock** key on the keyboard.)
2. The Domain Controller/Logon Message will appear explaining the absence of network connectivity. Select the OK button on the Domain Controller window (see below).

RFP OSI 2046 CURRENT SYSTEM



Exhibit: Domain Controller Window

3. At the SFIS Logon screen, use the same ID and password that is used in production.
4. Continue adding records in Stored Transactions' mode.

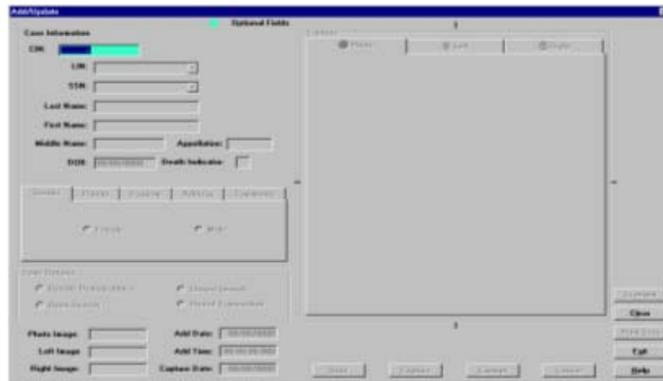


Exhibit: Stored Transaction Add/Update Screen

****Note:**

- o Operators that log on to the system with ID and password will continue to do so.
- o Operators that log on to the system with ID and fingerprints must now use ID and password logon. (The password was created when the operator first updated the default password, which expires and is updated every 90 days.)
- o Passwords cannot be reset over the network while in Stored Transactions' mode. If an operator gets suspended, SFIS will allow the operator to continue using the Add/Update function in

RFP OSI 2046 CURRENT SYSTEM

limited capacity, not allowing records to be copied from the hard drive to a zip disk.

Confirming that you are operating in Stored Transactions' Mode

If unsure about operating status, the following is a list of indicators to assist in verifying that the Stored Transactions' Mode is operational:

- Fingerprint Logon is not enabled
- The Bulletin Board will **NOT** appear after logon
- The Function menu only has three options to choose from (Printing is not available, for example)
- The Add/Update CIN field is green, indicating that a CIN is not needed for processing
- The Successful Transmission message states that the record has been added to Stored Transactions

Stored Transaction Functionality

Stored Transactions' mode functionality is limited to transactions that do not require network connectivity:

- Add/Update
- Copying transactions to a Zip Disk
- Scanner Diagnostics
- Help

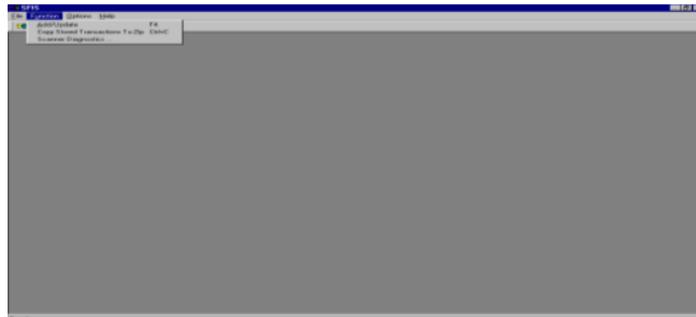


Exhibit: Stored Transaction's Function Menu

RFP OSI 2046 CURRENT SYSTEM

Add/Update Function in Stored Transactions

The Add/Update function in Stored Transactions is different than Add/Update with network connectivity because it does not require the following fields to be completed (All green fields are optional and all white fields must be completed.):

- o CIN

The CIN is not required because some counties may not be able to access a CIN without the SFIS network. To bypass the *CIN* field, press the **tab** key.

- o Priority

A priority for the Match Responses does not need to be selected since no print outs will be generated during Stored Transactions.

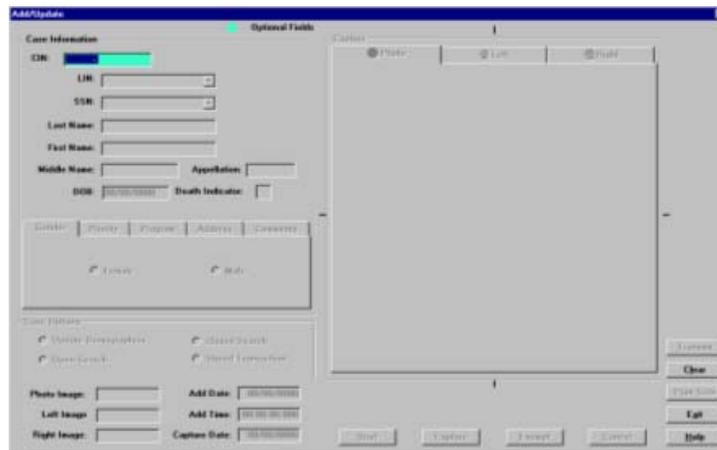


Exhibit: Stored Transaction Add/Update Screen

When the record is transmitted in Stored Transactions, the following message appears in the bottom left-hand corner:

“First Name Last Name Has Been Successfully Added in Stored Transaction Mode.”

RFP OSI 2046 CURRENT SYSTEM

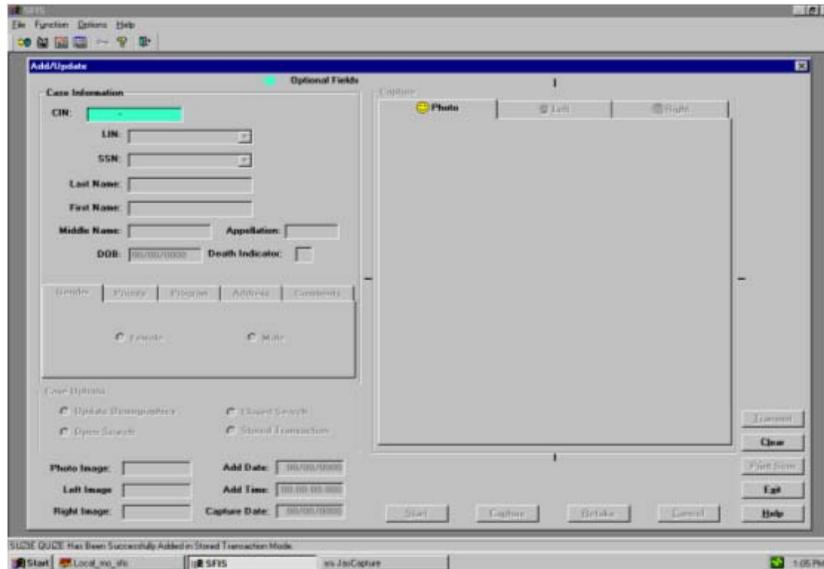


Exhibit: Successful Transmission Message

Re-Establishing Network Connectivity

1. If the operator is logged into Stored Transactions, they must log out. The operator may now follow their usual logon procedures and the network connectivity will be re-established. If it is the day after a State Holiday, the operator should also now follow their usual logon procedures and the network connectivity will be re-established. (If the SQL message appears when the operator is attempting to logon, select the **OK** button and attempt to logon again.)

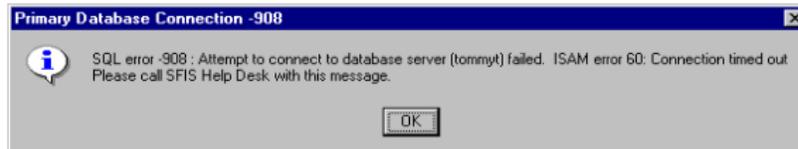


Exhibit: Time Out Message – SQL 908

RFP OSI 2046 CURRENT SYSTEM

Portable Input Workstation

Portable Input Workstations are not connected to the central database and, therefore, have to process in Stored Transactions' mode. At the end of each day, the stored transactions are downloaded onto a Zip Disk and transferred to the Client Input Workstation.

1. To transfer the files, the Zip Disk with the stored transactions from the Portable Input Workstation must be placed into the Zip drive on the Client Input Workstation.
2. Initiate upload processing by choosing the **Copy Stored Transaction From Zip Function** from the drop-down **FUNCTION** menu.

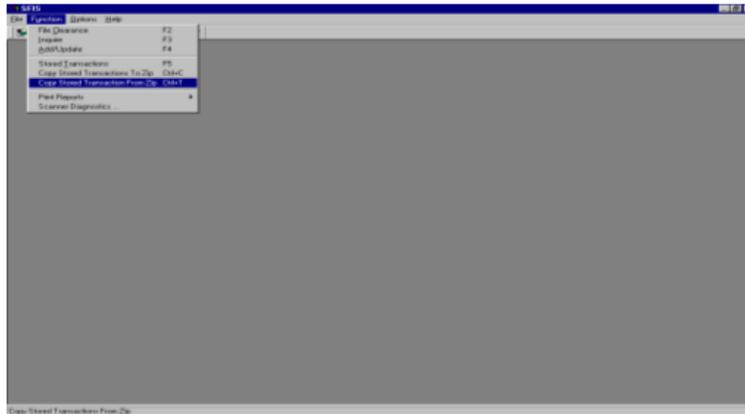
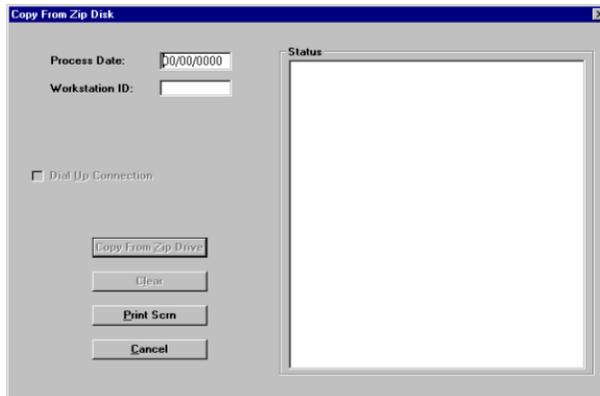


Exhibit: Copy Stored Transactions From Zip

3. Copy from Zip Disk window appears.

RFP OSI 2046 CURRENT SYSTEM

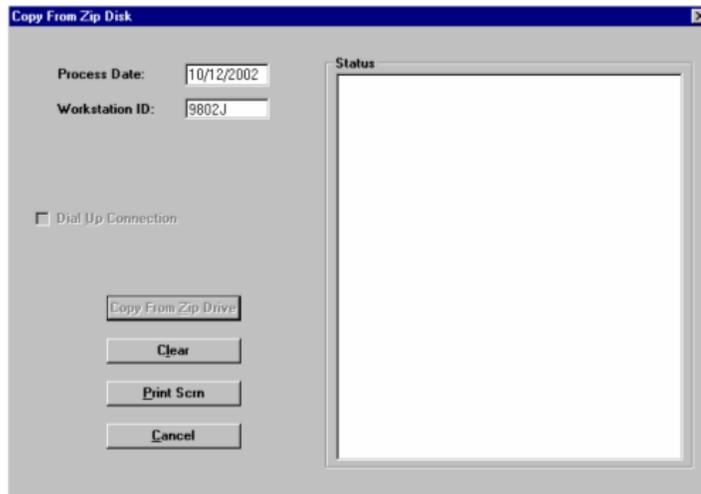


The screenshot shows a window titled "Copy From Zip Disk". It contains the following elements:

- Process Date:** A text box containing "00/00/0000".
- Workstation ID:** An empty text box.
- Dial Up Connection**
- Copy From Zip Drive** button
- Clear** button
- Print Scrn** button
- Cancel** button
- Status:** A large empty rectangular area on the right side of the window.

Exhibit: Copy From Zip Disk Window

4. Type the date that the images were captured in the Process Date field.
5. Type the Workstation ID that the Portable Input operator provided in Workstation ID field. (The format should be five characters long and start with a number. If the operator provides the number: P1202J, leave off the first alpha character: 1202J.)



The screenshot shows the same "Copy From Zip Disk" window, but with the following changes:

- Process Date:** The text box now contains "10/12/2002".
- Workstation ID:** The text box now contains "9802J".
- All other elements (checkbox, buttons, and status area) remain the same as in the previous screenshot.

Exhibit: Process Date and Workstation ID Field

RFP OSI 2046 CURRENT SYSTEM

6. Press the Tab key. The Copy From Zip Drive button enables. Select the Copy From Zip Drive button.

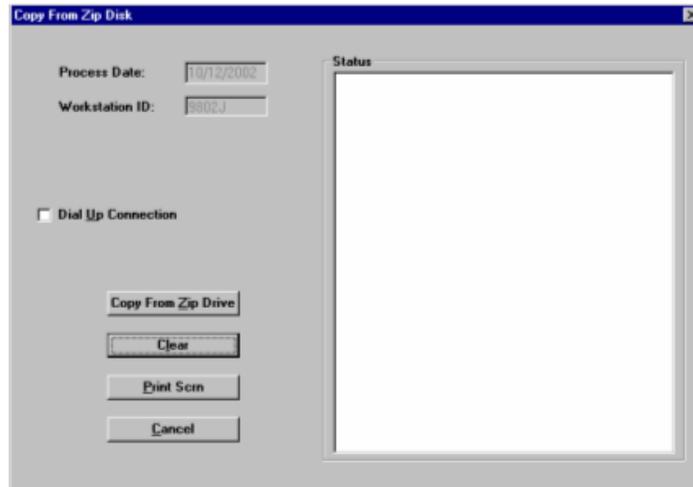


Exhibit: Copy From Zip Drive Button

7. Processing completed message appears. If records from different dates need to be copied, select the Yes button and repeat the above listed steps. If no further records need to be copied, select the No button.

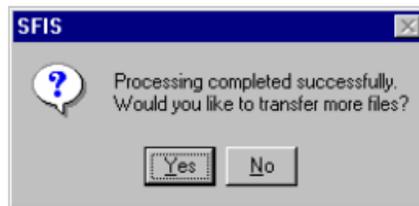


Exhibit: Processing Completed Successfully Message

Processing Stored Transactions

1. Prior to processing transactions, the Client Input Workstation must have network connectivity.
2. Upon successful logon, a message appears to remind the operator that Stored Transaction records are saved on the hard drive and that they need to be processed.

**RFP OSI 2046
CURRENT SYSTEM**

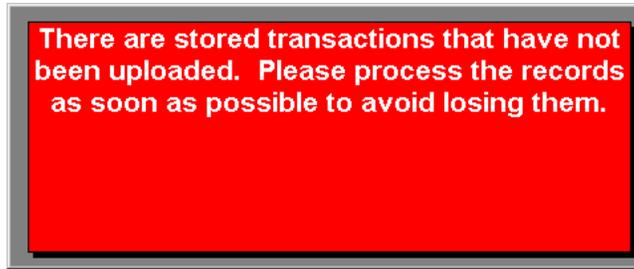


Exhibit: Upload Reminder Message

3. To initiate upload processing, select Stored Transactions from the FUNCTION menu.

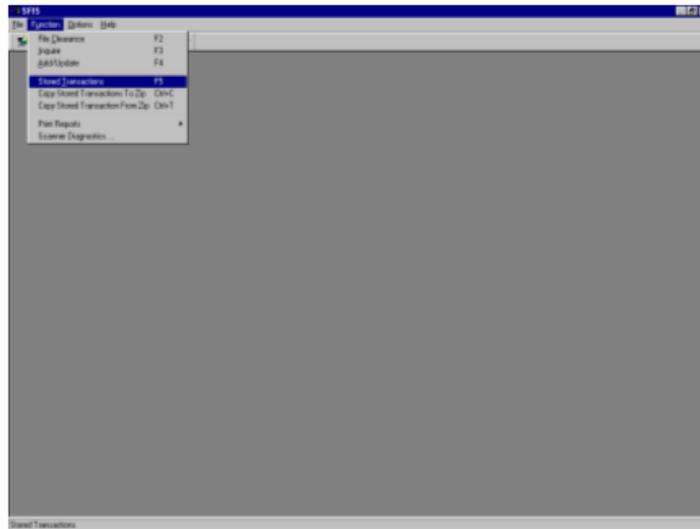


Exhibit: Stored Transactions Function

4. Each transaction captured in Stored Transaction mode must be processed through File Clearance. A queue is available to the operator to work through each stored transaction on the Client Input Workstation. The Stored Transaction File Clearance Screen is shown below.

**RFP OSI 2046
CURRENT SYSTEM**



Exhibit: Stored Transaction File Clearance Screen

5. Records that have not been uploaded will be visible in the queue. To load the records into the queue, select the Find and Load Stored Transactions button.
6. The Available Files/Files to Load window appears.

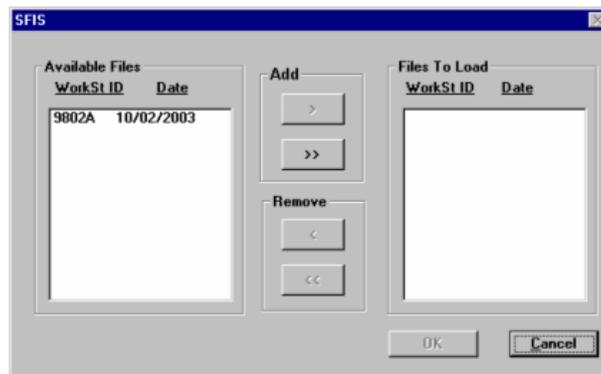


Exhibit: Available Files/Files to Load Window

**RFP OSI 2046
CURRENT SYSTEM**

7. Select the Workstation ID and Dates that need to be processed.

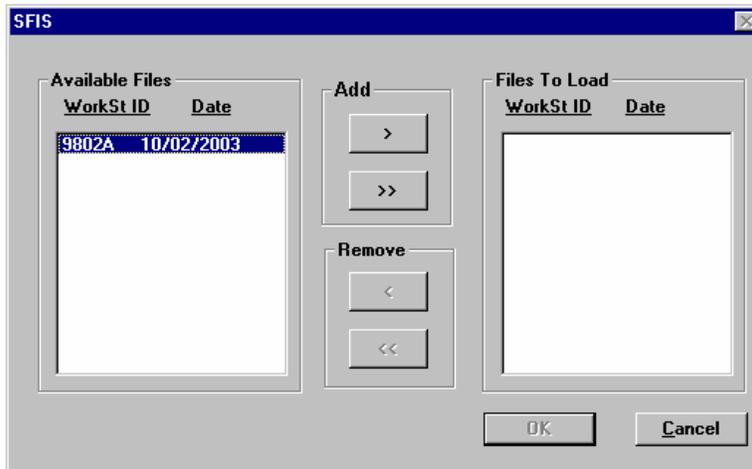


Exhibit: Available Files Queue

8. Select the Add (>) button to move the record (or records >>) to the Files to Load queue.

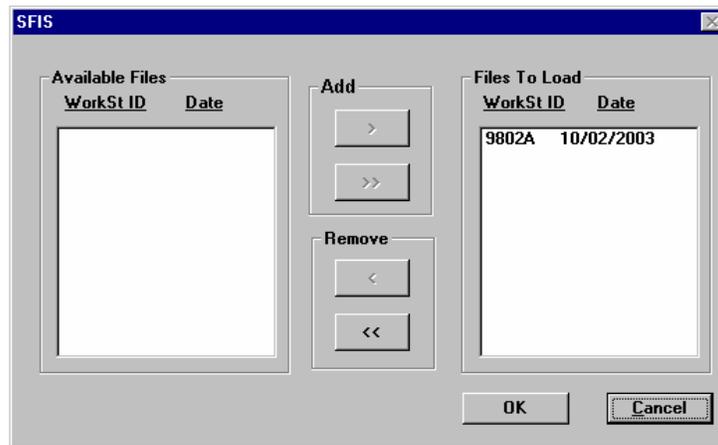


Exhibit: Files to Load Queue

9. Select the OK button to continue and Stored Transaction File Clearance screen will appear containing the newly loaded records.

RFP OSI 2046 CURRENT SYSTEM

10. Select the record desired for upload and the photo of the applicant will appear. If the Print Stored Transactions button is selected, the list of records present in the Stored Transactions File Clearance queue will be sent to the printer.



Exhibit: Desired Record Selected for Upload

11. To upload the record, select the OK button and file clearance will begin. (Please refer to the File Clearance section in the Client Input Workstation user guide for a complete explanation of the File Clearance function.)
12. If available, the client data retrieved from SCI and the photo image from SFIS is displayed in the SCI Inquire Function screen. If a CIN is not located in SCI, the operator will be given the opportunity to create a new CIN in SCI using the information contained in the SFIS file or the opportunity to decline the creation of a new CIN. If declined, the record will appear in the View Errors queue. If a new CIN is created, the Add/Update screen will appear with the new CIN in the CIN field.

RFP OSI 2046 CURRENT SYSTEM

CIN	SSN	LIN	Last Name	First Name
77250624	323-25-4393	98-32-3456789-708	JACOBS	SETH

Exhibit: SCI Inquire Function Screen

13. If the correct CIN/record is found in the SFIS Inquire Function window, select the Add/Update button.
14. By selecting the Add/Update button, the SFIS Inquire Function window closes and the Add/Update screen is displayed. The client information for the selected record is populated on the Add/Update screen and may be edited before transmission.
15. If the desired client entered into Stored Transactions is not on the SFIS Inquire Function window, selecting the Client Not Found button places the client into an error queue.
16. If the desired client is not on the SFIS Inquire Function window and county procedure permits, a new CIN may be requested for the client by selecting the Add with New CIN button. (If possible, verify that there are no spelling errors or typos in the client information that could cause the client not to be found on the SFIS Inquire Function window.) Selecting this button will open the Add/Update screen, which will automatically populate with the demographic information and photo image from Stored Transactions.
17. At the Add/Update screen, enter the client information for Gender, Priority and Program. Complete the Case Option field for an Open

RFP OSI 2046 CURRENT SYSTEM

Search or Closed Search, then select Transmit. A new CIN will be added to SFIS from SCI.

18. To edit the record before processing, select the Edit Record button.

Optional Fields

CIN: Edit CIN

LIN:

SSN:

Last Name:

First Name:

Middle Name:

Appellation:

DOB:

Gender	Program	Address	Comments
<input checked="" type="radio"/> Female			
<input type="radio"/> Male			

Capture Date: Edit Capture Date/Time

Capture Time:

Exhibit: Edit Stored Transaction Record Window

19. All fields may be edited before processing. Select the OK button when editing is completed and the Edit Stored Transaction Record window will close.

20. To edit the CIN field or the Capture Date/Time field, a supervisor fingerprint override is required.

RFP OSI 2046
CURRENT SYSTEM

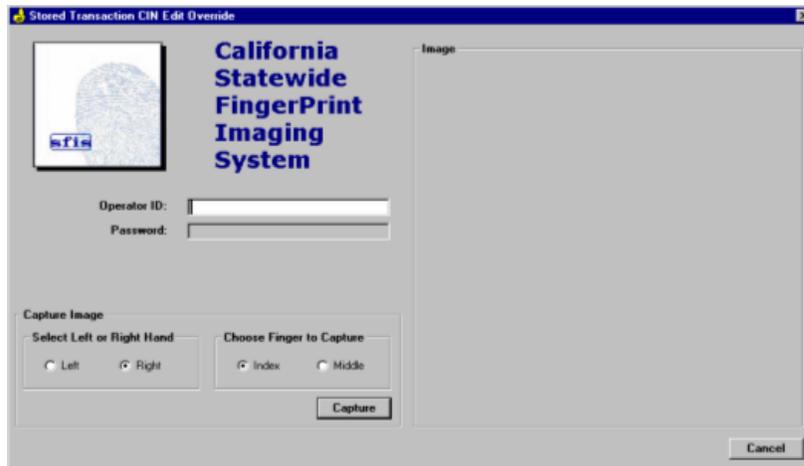


Exhibit: Stored Transaction CIN Edit Override Window

21. If an error occurred during the loading process or if the operator cancelled the upload process during file clearance, the record is moved to the View Error queue. To view the records, select the View Errors button, located on the Stored Transactions File Clearance screen. The View Errors queue is illustrated below. To remove a record from the View Errors queue for editing or processing, select the record and select the Reset Error button. If resetting the record is not desired, call the Help Desk for assistance.

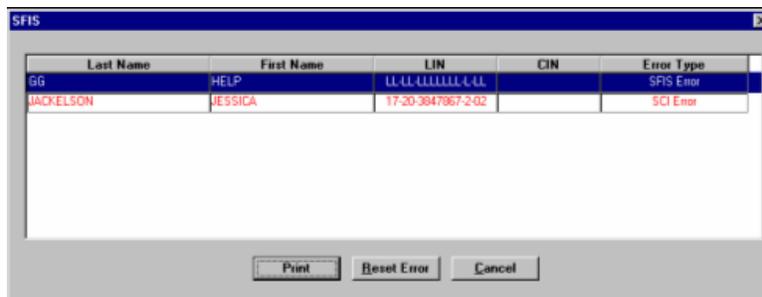


Exhibit: View Errors Window

22. Print the error log by selecting the Print button or close the window by selecting the Cancel button.

**RFP OSI 2046
CURRENT SYSTEM**

23. If error records are not present, the “No errors found.” message will appear. Select the OK button to close the message.



Exhibit: No Error Found Message

Portable Input Workstation

Portable Input Workstations are not connected to the central database and, therefore, have to process in Stored Transactions' mode. At the end of each day, the stored transactions are downloaded onto a Zip Disk and transferred to the Client Input Workstation.

1. To transfer the files, the Zip Disk with the stored transactions from the Portable Input Workstation must be placed into the Zip drive on the Client Input Workstation.
2. Initiate upload processing by choosing the Copy Stored Transaction From Zip Function from the drop-down Function menu.

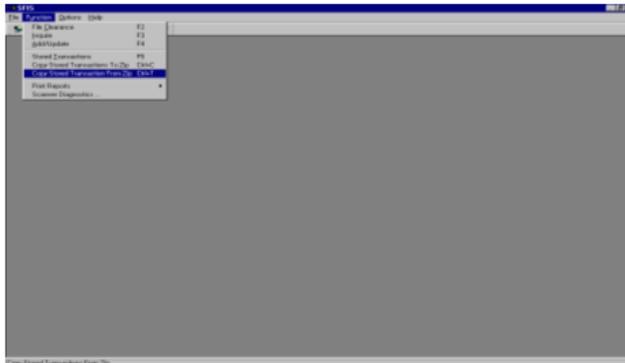


Exhibit: Copy Stored Transactions From Zip

3. Copy from Zip Disk window appears.

**RFP OSI 2046
CURRENT SYSTEM**

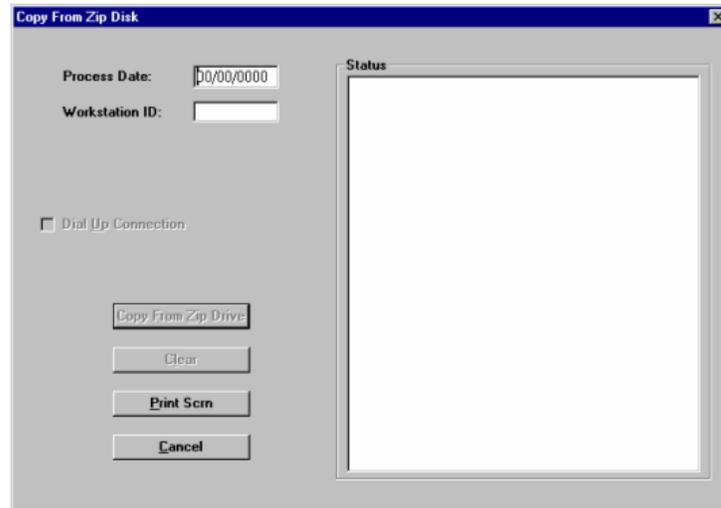


Exhibit: Copy From Zip Disk Window

4. Type the date that the images were captured in the Process Date field.
5. Type the Workstation ID that the Portable Input operator provided in Workstation ID field. (The format should be five characters long and start with a number. If the operator provides the number: P1202J, leave off the first alpha character: 1202J.)

**RFP OSI 2046
CURRENT SYSTEM**

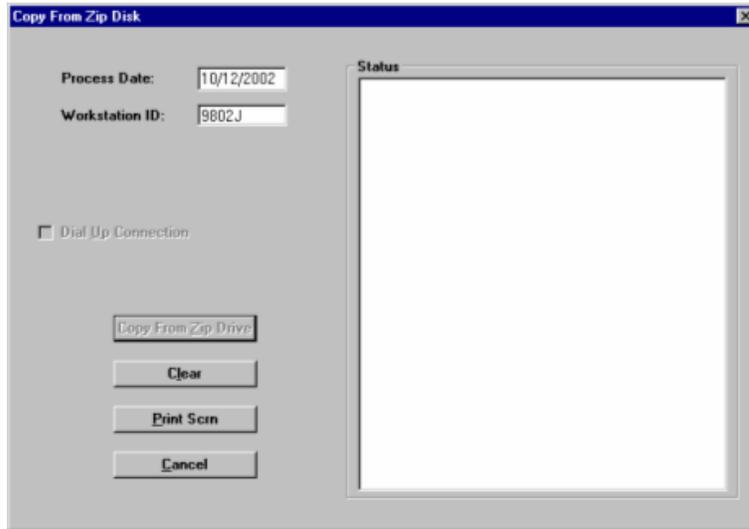


Exhibit: Process Date and Workstation ID Field

6. Press the Tab key. The Copy From Zip Drive button enables. Click on the Copy From Zip Drive button.

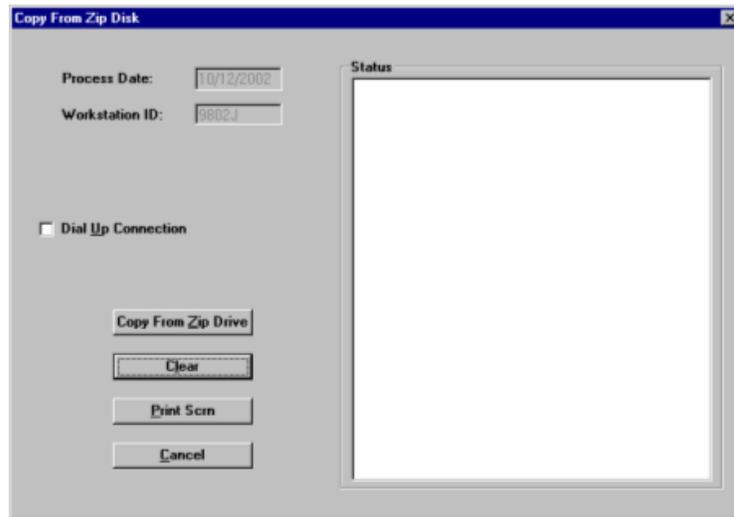


Exhibit: Copy From Zip Drive Button

RFP OSI 2046
CURRENT SYSTEM

7. Processing completed message appears. If records from different dates need to be copied, click on the Yes button and repeat the above listed steps. If no further records need to be copied, click on the No button.

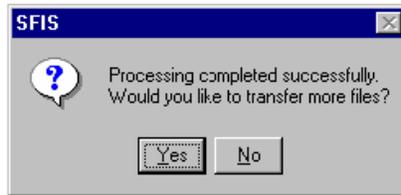


Exhibit: Processing Completed Successfully Message

RFP OSI 2046 CURRENT SYSTEM

Processing Stored Transactions

1. Prior to processing transactions, the Client Input Workstation must have network connectivity.
2. Initiate upload processing by choosing the Stored Transactions function from the toolbar or drop-down menu.

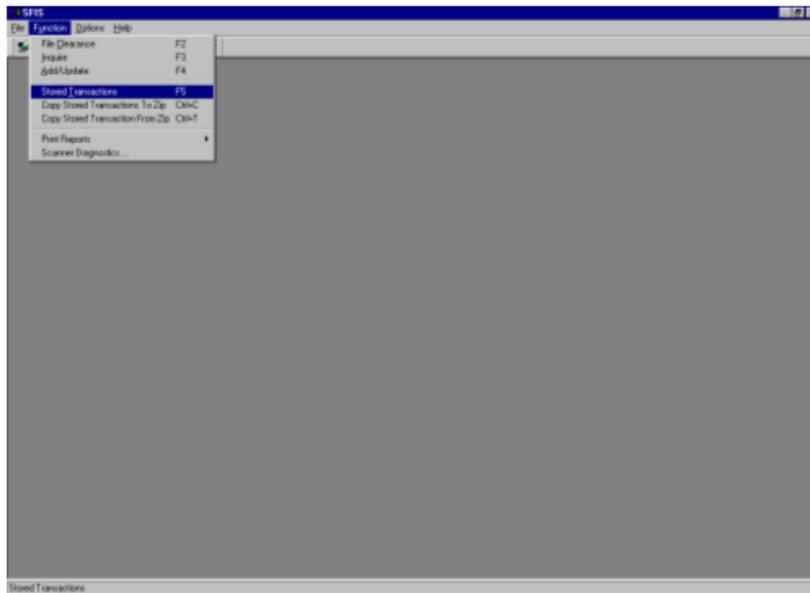


Exhibit: Stored Transactions Function

3. Each transaction captured in Stored Transaction mode must be processed through File Clearance. A queue is available to the operator to work through each stored transaction on the Client Input Workstation. The Stored Transaction File Clearance Screen is shown below.

**RFP OSI 2046
CURRENT SYSTEM**

Stored Transaction File Clearance

Process Date: 00/00/0000

Workstation ID:

Load Stored Transactions View Errors

Last Name	First Name	LIN	CIN
-----------	------------	-----	-----

Photo

Print Stored Transactions

OK

Clear

Print Scrn

Exit

Exhibit: Stored Transaction File Clearance Screen

4. The Process Date field must be populated with the date that the images were captured.
5. The Workstation ID field must be populated with the number that appears on the sticker attached to the SFIS Monitor (lower right hand corner). The number should begin with an alpha character such as "P," "M," or "C" followed by four numbers (county number and site number) and end with an alpha character. When entering this number, leave off the first alpha character as seen in the below screen capture (For example, if the number is M9802A, enter 9802A.)

RFP OSI 2046
CURRENT SYSTEM

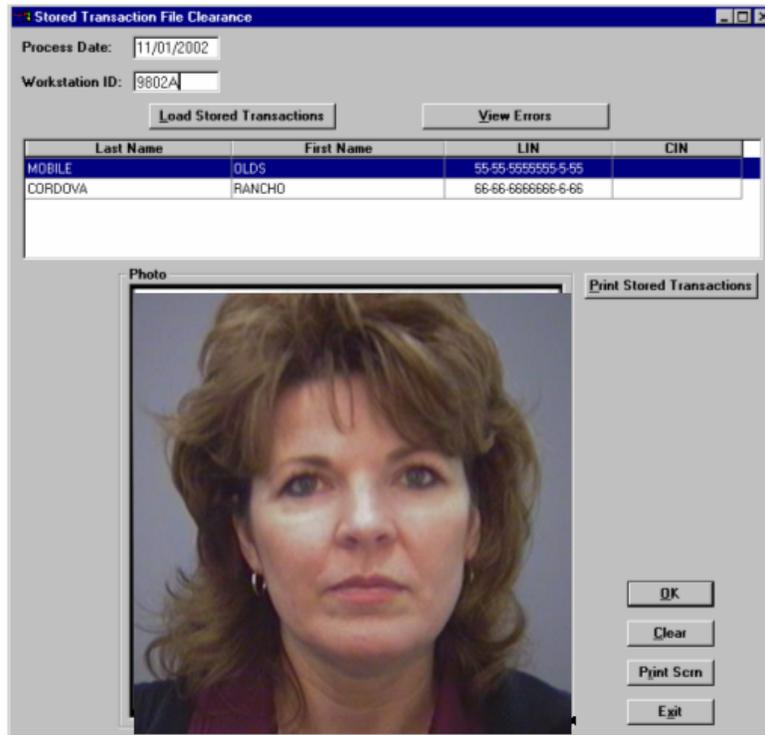


Exhibit: Stored Transaction File Clearance Window

6. Click on the Load Stored Transactions button and the queue displays the Last Name, First Name, LIN, and CIN of each client to be processed for a particular Workstation ID and process date. (See screen capture below.)

Formatted: Indent: Left: 1.5",
Numbered + Level: 1 + Numbering
Style: 1, 2, 3, ... + Start at: 1 +
Alignment: Left + Aligned at: 1.75"
+ Tab after: 2" + Indent at: 2",
Tabs: Not at 2"

RFP OSI 2046
CURRENT SYSTEM



Exhibit: Stored Transaction File Clearance Window

7. Any errors that occurred during the loading process can be seen by clicking on the View Errors button. The View Errors window is illustrated below. Call the help desk if any errors appear here.

**RFP OSI 2046
CURRENT SYSTEM**

Last Name	First Name	LIN	CIN	Error Type
JAS	RONALD	34-51-5215887-7-11		SCI Error
LORENS	RAUL	34-85-2145663-3-32		SCI Error

Exhibit: View Errors Window

8. Print the error log by clicking on the Print button or close the window by clicking on the Cancel button.
9. If no errors entered the error log, the "No errors found." Message will appear. Click on the OK button.



Exhibit: No Error Found Message

10. To print the Stored Transaction File Clearance screen, click on the Print Scrn button.
11. To process a successfully loaded transaction, select a row from the Stored Transaction File Clearance queue by highlighting it with a mouse click.
12. The photo image captured for that client during the stored transaction processing is displayed. Once highlighted, click on the OK button and the Stored Transaction File Clearance Screen performs a File Clearance function with SCI using the data entered during the stored transaction.

RFP OSI 2046 CURRENT SYSTEM

13. When SCI responds to the File Clearance request, the processing proceeds with the display of the SCI Inquire Function screen, as illustrated below.

CIN	SSN	LIN	Last Name	First Name	Date of Birth
7796004	323-25-4393	98-32 3456789-7-88	JACOBS	SETH	01/01/1970

Exhibit: SCI Inquire Function Screen

14. The client data retrieved from SCI and the photo image from SFIS, if available, is displayed for the first record in the Inquire Results panel.
15. View another record in the Inquire Results panel by highlighting the record in the panel.
16. The SCI Inquire Screen is populated with the client data and photo image, if available, for the selected record.
17. View each record in the Inquire Results panel until the correct record is found or until the end of the list is reached.
18. If a matching record is found in the Inquire Results panel, click on the Add/Update button.
19. By clicking on the Add/Update button, the SCI Inquire Screen disappears and the Add/Update screen is displayed. The client information for the selected record is populated on the Add/Update screen and may be modified on-line.

RFP OSI 2046 CURRENT SYSTEM

20. If the desired client entered into Stored Transactions is not on the Inquire Results panel, clicking on the Client Not Found button places the client into an error queue. If within seven (7) days, the Client Not Found button was clicked in error, call the Help Desk to retrieve the client from the error queue.

CIN	SSN	LFN	Last Name	First Name	Date of Birth	
100196P	---	---	SINDALEZ	SAMUEL	16/7/1967	Client Not Found
149020H	---	---	SINDALEZ	SAMUEL	16/7/1967	
732020H	---	---	SINDALEZ	SAMUEL	16/7/1967	
762020H	---	---	SINDALEZ	SAMUEL	16/7/1967	

Exhibit: Inquire Results Screen

21. If the desired client is not on the Inquire Results panel and no new or additional information is available, a new CIN may be requested for the client by clicking on the Add with New CIN button. (If possible, verify that there are no spelling errors or typos in the client information that could cause the client not to be found on the Inquire Results panel.) Clicking on this button will bring you to the Add/Update screen, which will automatically populate with the demographic information and photo image from Stored Transactions.
22. Once at the Add/Update screen, enter the client information for Gender, Priority and Program. Complete the Case Option field for an Open Search, then click on Transmit. A new CIN will be added to SFIS from SCI.

RFP OSI 2046 CURRENT SYSTEM

Add/Update Function

The Add/Update Function is used to:

- Add new clients including fingerprint and photo images to the SFIS database, creating a link to the SCI database, and completing an Open Search.
- Verify a client's fingerprint images against the fingerprint images stored for the same client CIN in the SFIS database completing a Closed Search.

Update demographic information in both SFIS and SCI related to clients on the SFIS database.

*NOTE: the Add/Update function on the Portable workstation does not interact with the SCI database. Therefore, the SCI links are not established until the records have been processed.

The user may be presented with the Add/Update screen through a number of process flows including:

- **CIN is Known** – Obtaining a CIN from the referral paperwork or from another automated system.
- **CIN is Found on SFIS** – Selecting a client from the Inquire Screen and pressing the *Add/Update* button.
- **CIN is Found on SCI** – Selecting a client from the SCI Inquire Screen and pressing the *Add/Update* button.
- **New CIN Requested** – Requesting a new CIN on the SCI Add screen or on the SCI Inquire screen during Stored Transaction processing.

Each of these processes is highlighted in the following subsections. Following these subsections, the Add/Update process is described and is the same process regardless of the way in which the user reached the Add/Update screen.

CIN is Known

In this situation, the CIN for the client is known through some means other than the SFIS workstation. The CIN may be present on referral paperwork, it may have been researched on the Medi-Cal Eligibility Data System (MEDS), it may have been generated through Statewide Automated Welfare System (SAWS), etc. The user may choose the

RFP OSI 2046 CURRENT SYSTEM

Add/Update icon on the toolbar and enter the Add/Update screen directly. The Add/Update screen will be blank awaiting entry of the CIN by the user.

A check digit is used to validate the data entered and ensure no typos occurred. The typical use of a check digit would be for the data entry person to calculate the check digit manually for a new add, and then the system would verify it. For any given set of digits, only one (1) check digit is valid. The check digit in SFIS is the result of a mathematical algorithm, and is calculated based on the nine (9) characters of the CIN. However, there is a potential problem because the SFIS user is not required to manually calculate and enter the check digit. This requirement was removed from SFIS at the request of the State in order to make data entry easier, but opened up the possibility of allowing miskeyed data. If the user does not enter the check digit, SFIS will calculate it for them, which in essence renders it partially ineffective. This is particularly true of a new Add when the nine (9) digits entered are miskeyed. The system will calculate the check digit based on misinformation, and generate a CIN that may belong to an existing client. However, if the complete CIN is entered, the system will reject it when an invalid check digit is keyed.

CIN is Found on SFIS

The CIN may have been located by inquiring on SFIS through the Inquire function. The client would have been selected from the Inquiry Results panel of the Inquire Screen (SFIS). Once the row containing the correct client is highlighted, pressing the Add/Update button accesses the Add/Update screen. The Inquire Screen disappears and the Add/Update screen appears with the demographic information pre-filled and the photo displayed, if available.

CIN is Found on SCI

The CIN may have been located by inquiring on SCI through the File Clearance function. The client would have been selected from the inquiry results panel of the SCI Inquire screen. Once the row containing the correct client is highlighted, pressing the Add/Update button accesses the Add/Update screen. The SCI Inquire screen disappears and the Add/Update screen appears with the demographic information pre-filled and the photo displayed, if available.

RFP OSI 2046
CURRENT SYSTEM

New CIN Requested (for Counties not operating SAWS)

The correct client may not have been found on SFIS using the Inquire function or SCI using the File Clearance function. In this case, the File Clearance function would have allowed the user to request a new CIN be assigned to the client. Once the new CIN was returned from SCI, the CIN Return message window would have appeared indicating the new CIN. By pressing Yes on the CIN Return message box, the user would be taken to the Add/Update screen with the demographic information entered during the File Clearance function pre-filled.

During Stored Transaction processing, a new CIN may be requested for the client. SCI will assign a new CIN for the requested client and return the CIN to the SFIS workstation on the Add/Update screen with all the information, including images, pre-filled.

Add/Update Screen

This section describes the process once the Add/Update screen has been displayed, regardless of what flow caused the screen to be displayed. The Add/Update screen is used to do the following:

- Update Demographic Information – The Add/Update screen is used to update a client's demographic information such as date of birth, etc.
- Add Photo and Fingerprint Images to a CIN – The Add/Update screen is used to add photo and fingerprint images to a case for the first time resulting in an Open Search against the database. (Open Search is a fingerprint matching process where the newly added fingerprints are matched against all the other fingerprints in the database to determine if the client is known to the system by another CIN.)

RFP OSI 2046
CURRENT SYSTEM

- Verifies a Client's Fingerprints Against Those Stored for a CIN – The Add/Update screen is used to update photo and fingerprint images and launch a Closed Search. (Closed Search is a fingerprint matching process where the client's fingerprints are matched against the fingerprints already on file for a particular CIN.) Images are only updated on the CIN in the database if the Closed Search results in a match. For example, SFIS verifies that the client's fingerprint images match those already on file for the particular CIN. If the Closed Search results in a match, the photo on file is replaced with the incoming (most current) photo. However, fingerprint images are only updated if they are of better quality than those already on file or are replacing fingerprint images converted from the Automated Fingerprint Imaging Reporting and Match (AFIRM) system.

Once the Add/Update screen is displayed, the fields may be blank (user has a CIN from another source) or pre-filled (user obtained CIN via the SFIS workstation through SFIS or SCI). Data to be entered, or in the case of pre-filled data, updated for each client consists of:

- CIN, SSN, and LIN (full fourteen (14) digit), if available (if pre-filled, the SSN displayed is the most current entered into SCI).
- Digitized color client photo.
- Demographic information, including name, date of birth, and gender.
- Free text comments entered by users.

RFP OSI 2046 CURRENT SYSTEM

Exhibit: Add/Update Screen

The following subsections describe the process to update demographics, add photo and fingerprint images to a CIN, or verify a client against fingerprint images currently on file for a particular CIN.

Update Demographics

- **From SFIS Inquire** – The user may have performed an SFIS Inquire, chosen a client, and pressed the Add/Update button. When the Add/Update button is pressed from the Inquire screen, SFIS performs a File Clearance using the chosen CIN, and reports all SCI information on the Add/Update screen. The information displayed may then be updated by the user. If the user wants to update demographic information only, he/she presses the Update Demographics button. Once all updates have been completed, the user presses the Transmit button, and the updated information is stored in the SFIS database and transmitted to SCI for update.

RFP OSI 2046 CURRENT SYSTEM

- **From File Clearance** – The user may have performed a File Clearance, chosen a client, and pressed the Add/Update button or requested a new CIN. In this situation, the SCI information retrieved or entered during the File Clearance is displayed and may be updated by the user. If the user updates demographic information and presses the Update Demographics radio button, the updated information is stored in the SFIS database and transmitted to SCI for update.
- **Starting with CIN** – The user may have entered this screen directly from the toolbar, having obtained the CIN from another location. The user enters the CIN in the CIN field and presses the <Tab> key. The SFIS workstation submits a request to the SCI database for the demographic information on the CIN entered. If the CIN is known to the SCI database, the Add/Update screen is populated with the client demographic information, along with the photo image from the SFIS database, if available. If the CIN is not known to SCI, an error message is displayed. If the client demographic data is available from SCI, the user clicks on the Update Demographics button to update the client demographic data. A message box is displayed with the question “Are you sure you want to update the demographics of this case?” The user clicks on the Yes button and updates the demographic data. Once all updates have been completed, the user clicks on the Transmit button. The updated information is stored in the SFIS database and returns it to SCI for update.

Adding Client Photo and Fingerprint Images

There are three (3) locations from which the user may start the process of adding a new client or updating a client without fingerprint images.

- **From SFIS Inquire** – The user may have performed an SFIS Inquire, chosen a client, and pressed the Add/Update button. When the Add/Update button is pressed from the Inquire screen, SFIS performs a File Clearance using the chosen CIN, and reports all SCI information on the Add/Update screen. The information displayed can be updated by the user. The process continues at the Adding Photo Images subsection below.

RFP OSI 2046 CURRENT SYSTEM

- From File Clearance – The user may have performed a File Clearance, chosen a client, and pressed the Add/Update button or requested a new CIN. In this situation, the SCI information retrieved or entered during the File Clearance is displayed and may be updated by the user. The process continues at the Adding Photo Images subsection below.
- Starting with CIN – The user may have entered this screen directly from the toolbar, having obtained the CIN from another location. The user enters the CIN in the CIN field and presses the <Tab> key. The SFIS workstation submits a request to the SCI database for the demographic information on the CIN entered. If the CIN is known to the SCI database, the Add/Update screen is populated with the client demographic information, along with the photo image from the SFIS database, if available. If the CIN is not known to SCI, an error message is displayed. If the client demographic data is available from SCI, the user may update the client demographic data. The process continues at the Adding Photo Images subsection below.

Adding Photo Images

The user may add and/or update the client demographic information on the Add/Update screen. SFIS also checks to see if the CIN is known to the SFIS database in order to retrieve a photo, if available. For new clients, the CIN would not be known to the SFIS database. Clients with a CIN known to SFIS, but who do not have fingerprint or photo images on file, would also fall into this processing area of adding images to the client record.

If the CIN is known to SFIS and fingerprint and photo images have been captured, the client would be processed as a Closed Search, which is described in the Updating Images subsection.

A CIN may have multiple SSNs or LINs on file. The user may view multiple SSNs or LINs for that CIN using the drop-down indicator on these data fields.

As the user adds or updates demographic information, the system performs online data validation checks at the character and field level to ensure only valid information is added to the SFIS database tables. The user moves from field to field by pressing the <Tab> key. If data is entered in error, SFIS displays a Data Entry Error message window.

RFP OSI 2046 CURRENT SYSTEM

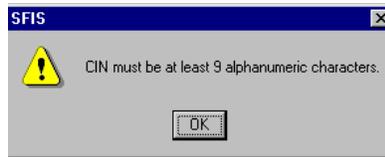


Exhibit: Data Entry Error Message Window

SFIS displays the Data Entry Error message window and highlights the data fields that contain the errors. The user acknowledges the errors by clicking *OK* in the Data Entry Error message window and correcting the highlighted items.

Next to the *DOB* field is a *Death Indicator* field. This field may not be updated and is used to display the death indicator status from SCI.

In the area below the *DOB* and *Death Indicator* fields is a series of tabs that may be selected:

- **Gender** – (Required) Allows selection of the client's gender, either Male or Female.
- **Priority** – (Required) Allows selection of a priority for match processing: Normal, Priority, or Conversion. Normal is the default choice.
 - **Normal** – Match request submitted with a response required by 7 a.m. the next business day.
 - **Priority** – Match request submitted with a response required in fifteen (15) minutes.
 - **Conversion** – Match request submitted with a response required by 7 a.m., seven (7) business days following submission.
- **Program** – (Required) Allows selection of the program(s) that the client is participating in; GA/GR, CalWORKs, and/or Food Stamps. Any program that is selected may have a four (4) character worker number entered corresponding to the program selected.
- **Address** – (Optional) Allows addition of the client's address information.
- **Comments** – (Optional) Allows addition of comments and annotations into the SFIS database to be stored with the client record.

RFP OSI 2046 CURRENT SYSTEM

Once each required tab is filled out, the user chooses a *Case Option*. When adding images for the first time to a CIN, the *Open Search* option is the only one (1) available. Once a *Case Option* is chosen, SFIS activates the Photo tab on the screen. The user continues the Add/Update function by capturing the client's photo image.

To capture a photo image the user first clicks the *Start* button. The capture area becomes active, and the photo camera image is displayed on the workstation screen. There is a slight delay after pressing the *Start* button before the *Capture* button is activated. This was designed to prevent the use of the *Capture* button until the *Start* processing has fully completed.

The user centers the client's facial image in the capture window by adjusting the camera, and presses the *Capture* button. SFIS indicates the photo was captured by displaying the word "Captured" in the *Photo Image* demographic field. The case photo captured by the user is automatically digitized and stored with all other case information for that CIN. The Exhibit below shows an example of a photo image after all capture processing, including fingerprints, has been completed.

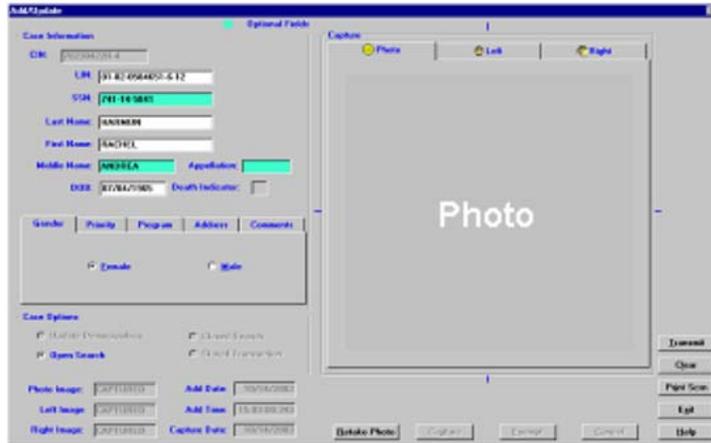


Exhibit: Add/Update Screen with Client Photo

Note that after capturing the fingerprint images, the user may recapture the photo image until an acceptable image is obtained, as explained in the Retaking Photo Images subsection below.

RFP OSI 2046 CURRENT SYSTEM

After the photo is captured, SFIS automatically activates the Left fingerprint tab for the user to begin capturing the client's fingerprints images. The processes for capturing the left and right fingerprint images are the same. The user determines if the left index fingerprint image is to be captured or exempted.

Exempting Fingerprints

If the left index finger is determined to be temporarily exempt or missing, the user clicks the *Exempt* button and SFIS displays the Fingerprint Exempt window.



Exhibit: Selection of an Exemption for Left Finger

The window offers two (2) options, Temporary Left and Alternate Finger Selection. The user selects the Temporary Left option if the client's finger is injured or bandaged and may be recaptured at a later date.

The user selects the Alternate Finger Selection option only if the client's index finger is missing. SFIS then begins the process of requesting alternate fingers in the following mandatory sequence: index, thumb, middle, ring, little. Should the user indicate that all fingers are missing, SFIS will generate a permanent exemption. If the Alternate Finger Selection is chosen (by an operator that does not have authorization to bypass override screens), the Alternate Finger Override window appears.

RFP OSI 2046
CURRENT SYSTEM



Exhibit: Alternate Finger Override Window

A security level B or higher user must approve the use of an alternate fingerprint by entering their user ID in the user ID field on the Alternate Finger Override window. Once the user ID and fingerprint have been correctly entered to allow the capture of an alternate finger, the Alternate Finger Selection window is displayed with the thumb as the active selection.



Exhibit: Alternate Finger Selection Window

The user chooses Yes or No to indicate whether the thumb is available for fingerprint capture. If the user chooses No for the thumb, SFIS prompts the user to verify that the thumb is not available.

**RFP OSI 2046
CURRENT SYSTEM**

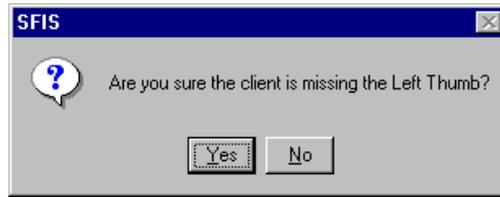


Exhibit: Alternate Finger Selector

This process continues for each finger in order of thumb, middle, ring, and finally the little finger. If none of the fingers on the left hand are available for capture, the client will receive a permanent exemption.

Adding Fingerprints

To initiate the fingerprint capture process, the user presses the *Start* button. Once the *Start* button is pressed, the *Exempt* button becomes disabled. This is to prevent the user from exempting fingerprints prematurely (before three (3) attempts have been made to capture a valid image). After pressing *Start*, the video *Capture* window becomes active. At this time there will be lines (crosshairs) on all four (4) sides of the live window that run almost to the center of the window. These lines signify where the core of the fingerprint should be placed. To help with the centering process, directional (Up, Down, Left, and Right) indicators are also provided on each side of the live window. Additionally, fingerprint capture instructions will be displayed in place of the demographic information. The instructions are: "Clean scanner with white wipe," "Clean finger with yellow wipe," "Center core," "Press finger lightly on scanner," "Press Capture," "Press finger harder on scanner (vary pressure during capture)," and "Remove finger when status bar appears." A message also appears above the *Start*, *Capture*, *Exempt*, and *Cancel* buttons to make sure the finger is centered before pressing *Capture*.

RFP OSI 2046 CURRENT SYSTEM

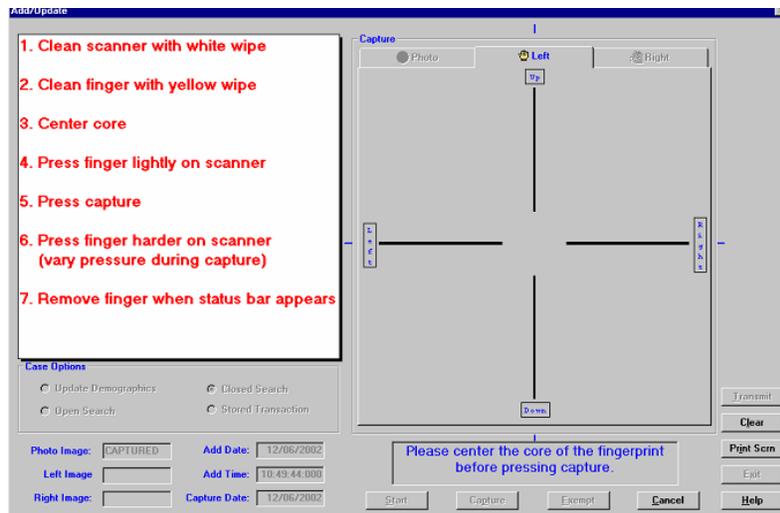


Exhibit: Add/Update Screen with Crosshairs and Capture Messages

These instructions will go away once x seconds (x equals maximum capture time as defined in the .ini file) worth of images have been captured or the *Cancel* button is pressed. The only available option at this point is the *Cancel* button. To get the *Capture* button to become live, the user needs to have the client press their finger onto the fingerprint scanner platen, making sure to center the core of the fingerprint in the open area of the crosshairs. At this point, the software will sense the presence of a finger and will enable the *Capture* button.

RFP OSI 2046 CURRENT SYSTEM

Once the maximum number of capture seconds (as defined in the .ini file) has passed, the message area will be replaced by a process meter. While the process meter is displayed, the system will sort the results placing the best x images (x equals the number of capture attempts defined in the .ini file) at the top of the list to be processed. These images are then put through a more extensive Motorola/Printrak quality check. Once each of the images has been processed, the data is again sorted. The first sort criterion is the Check Image Quality (CIQ) value. In the event that multiple images have the same CIQ value, the Contextual Enhancement Processor (CEP) and Fast Image Quality (FIQ) values are used to break the tie. If the top image based on the secondary sort is of acceptable quality, the process will continue and prompt the user to either capture the next finger or transmit the images. If the top image is deemed unacceptable, the application displays an error message.

Deleted: Printrak

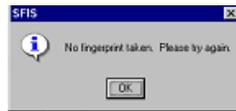


Exhibit: Add/Update Capture Error Message

The user acknowledges the message by pressing the *OK* button, and the application will prompt the user to attempt to capture the fingerprints again. This can happen up to three (3) times before the software either chooses the best of the bad quality, or decides the prints are unacceptable. If a print is deemed unacceptable quality, no image is saved and the client will not have the given finger on file.

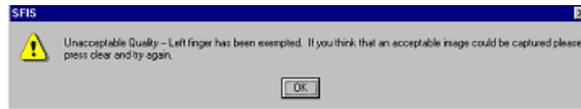


Exhibit: Unacceptable Quality - Exempt Message

In the event that a client has two (2) unacceptable quality images, the client cannot be used in the matching process. When the capture process is over, the process meter is hidden. The Exhibit below shows an example of a left fingerprint image after all capture processing has been completed.

RFP OSI 2046 CURRENT SYSTEM



Exhibit: Add/Update Screen with Left Fingerprint Image

Once an acceptable quality left fingerprint image is captured, the system automatically selects the Right fingerprint tab in order to repeat the capture process for the right hand. The *Exempt* button becomes enabled once again to allow exemption of the right hand before starting the capture process. If an exemption is necessary, the user follows the exemption process as detailed in the Exempting Fingerprints subsection. The Exhibit below shows an example of a right fingerprint image after all capture processing has been completed.



Exhibit: Add/Update Screen after Right Fingerprint Image Capture

RFP OSI 2046 CURRENT SYSTEM

After both fingerprint images are captured, SFIS compares the right image to the left image to ensure two (2) different fingerprint images were captured. This one-to-one or Closed Search is performed at the Client Input Workstation. If the comparison results in a match, SFIS notifies the user by displaying a Capture Error message window.



Exhibit: Capture Error Message Window

The message displayed in the Capture Error message window instructs the user to restart the capture process. The user acknowledges the error message by selecting *OK*, and the Capture Error message window disappears. The user recaptures both fingerprint images, paying close attention to which finger the client places on the fingerprint scanner. The fingerprints captured the second time, assuming they do not again match each other, replace the images previously captured.

Once the left and right fingerprint images are captured, SFIS automatically returns to the Photo tab.

Retaking Photo Images

To recapture an unacceptable photo, the user clicks on the *Retake Photo* button. The Retake Message window appears asking, "When do you wish to capture the photo?" There are three (3) options, *Take Now*, *Take Later*, or *Cancel*.

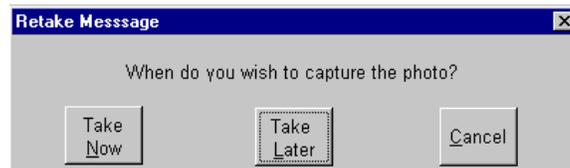


Exhibit: Retake Message Window

RFP OSI 2046 CURRENT SYSTEM

Cancel is used to cancel any retake actions and return to the Add/Update screen. The Take Now option closes the Retake Message window, and returns to the Add/Update screen's Photo tab to recapture the photo. If the user determines that an acceptable photo is not possible at this time (that is, if the client's face is bandaged or the camera is malfunctioning), the Take Later button is selected. After pressing the Take Later button, the Reschedule Client Message window appears stating "This client will be documented for reschedule on Photo Retake report #CS4218W."

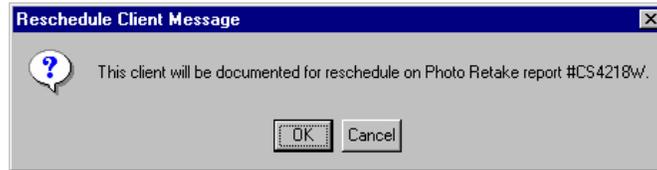


Exhibit: Reschedule Client Message Window

The user selects the *OK* button to complete the photo reschedule and return to the Add/Update screen. SFIS displays "Retake" in the *Photo Image* field. Or, if the user wants to cancel at this point, the *Cancel* button is pressed, the client is not rescheduled, and the user is returned to the Retake Message window. It is important to note that some kind of photo, regardless of quality, must be taken in order to enter the client into the system. A client cannot be entered into the system using only fingerprints.

Open Search

Once all images are successfully captured, and all demographic information is entered correctly, the search request is then submitted by clicking the *Transmit* button. To end the transaction without transmitting to the Central Site, the user clicks on the *Exit* button to abort the Add/Update function or clicks on the *Clear* button to reset the data on the screen.

The Open Search request matches the client's fingerprint images just captured (the applicant fingerprints) against all other images on the SFIS database. For an Add where fingerprint images were captured and fingerprint images for this CIN are not already on the SFIS database, the only option available to the user is an Open Search. The Open Search request will conclude with an automatic add to the SFIS database if the search results in a No Match.

RFP OSI 2046 CURRENT SYSTEM

In an Open Search, fingerprint images are matched against other fingerprint images on the database, and a response is returned by 7 a.m. the next business day for Normal requests. Results of Priority requests are returned within fifteen (15) minutes. Conversion requests are returned within one (1) week.

The Open Search may result in a Match indicating that the same fingerprint images were found associated with a different CIN, or a No Match indicating that the fingerprint images were not found in the database. An Open Search Match is sent to a Verification Technician to determine that the Match Response is correct before it is returned to the workstation. If it is determined the Match Response is correct, it is sent to the resolution and Fraud Queue simultaneously. Once the online matching process and verification (if applicable) is complete, the response is sent back to the SFIS workstation that submitted the request, and the date and time the response was sent is recorded in the database log table.

Open Search Match Responses, returned to the workstation, are placed on a resolution queue for the site. The resolution queue is used to record the results of research. At any time, the user may check the status of a matching request through the Queues function. This function is further described in Section F, "Queues Function."

When the demographic information and images are transmitted to the Central Site for matching, the user may begin the next transaction by selecting the desired toolbar button.

Verifying a Client

The process of verifying a client occurs when the client's CIN exists in SFIS with fingerprint images already captured. In this situation, a Closed Search is done to validate the client at the workstation is the same person who previously had their fingerprint images captured for the particular CIN.

Using the demographics and photo image displayed on the screen, the user determines whether or not the client who is about to be entered into SFIS is the same client who was assigned the CIN from the File Clearance.

There are three (3) locations from which the user may start the process of verifying a client against fingerprint images stored on a particular CIN.

RFP OSI 2046
CURRENT SYSTEM

- **From SFIS Inquire** – The user may have performed an SFIS Inquire, chosen a client, and pressed the *Add/Update* button. When the Add/Update button is pressed from the Inquire screen, SFIS performs a File Clearance using the chosen CIN, and reports all SCI information on the Add/Update screen. The information displayed can be updated by the user. The process continues at the Updating Images subsection below.
- **From File Clearance** – The user may have performed a File Clearance, chosen a client, and pressed the *Add/Update* button. In this situation, the SCI information retrieved during the File Clearance is displayed and may be updated by the user. The process continues at the Updating Images subsection below.
- **Starting with CIN** – The user may have entered this screen directly from the toolbar, having obtained the CIN from another location. The user enters the CIN in the *CIN* field and presses the <Tab> key. The SFIS workstation submits a request to the SCI database for the demographic information on the CIN entered. If the CIN is not known to SCI, an error message is displayed. Otherwise, the Add/Update screen is populated with the client demographic information, along with the photo image from the SFIS database, if available. The user may update the client demographic data retrieved from SCI. The process continues at the Updating Images subsection below.

Updating Images

SFIS checks to see if the CIN is known to the SFIS database in order to retrieve a photo, if available. For clients waiting to be verified, the CIN would be known to the SFIS database, and the record would have fingerprint images attached. Clients whose CIN is unknown to SFIS, or is known to SFIS but who do not have fingerprint or photo images on file, would fall under the Adding Images section previously described.

The user then chooses a Case Option. When updating images, the Closed Search is used, when updating demographic only, the Update Demographics is used.

The Update Demographics case option should only be used if the client is not present and a demographic error is being corrected. If the client is present, a verify (Closed Search) transaction can be used (this is dependent on each county's business processes). Images cannot be captured in Update Demographics mode.

RFP OSI 2046
CURRENT SYSTEM

Upon choosing the Closed Search case option, SFIS asks if the user wants to capture both fingers for a one-to-one search. The user proceeds by clicking on the Yes button.

The user continues the Add/Update function by updating the client's photo and fingerprint images as needed, as described previously in the Adding Photo Images, Exempting Fingerprints, Adding Fingerprints, and Retaking Photo Images subsections.

Once all images are successfully captured, and all demographic information is entered correctly, the search request is then submitted by clicking the Transmit button. To end the transaction without transmitting to the Central Site, the user clicks on the Exit button to abort the Add/Update function or clicks on the Clear button to reset the data on the screen.

Closed Search

The Closed Search determines if the fingerprint images on the database for that CIN match those that were just captured by the user. If the Closed Search results in a Match and the incoming fingerprint images are of better quality, SFIS automatically replaces the fingerprint images on file with the new images (if the file images are from AFIRM, the images are replaced regardless of quality). If a fingerprint image is updated, SFIS records audit information of the transaction.

If the result of the Closed Search comparison is a No Match, SFIS automatically performs another Closed Search comparison of the two (2) records with the fingerprint images in one (1) of the records reversed.

If the reversed image Closed Search results in a No Match for a user that does not have override authorization, a user with override authority must enter his/her user ID in the user ID field.

**RFP OSI 2046
CURRENT SYSTEM**

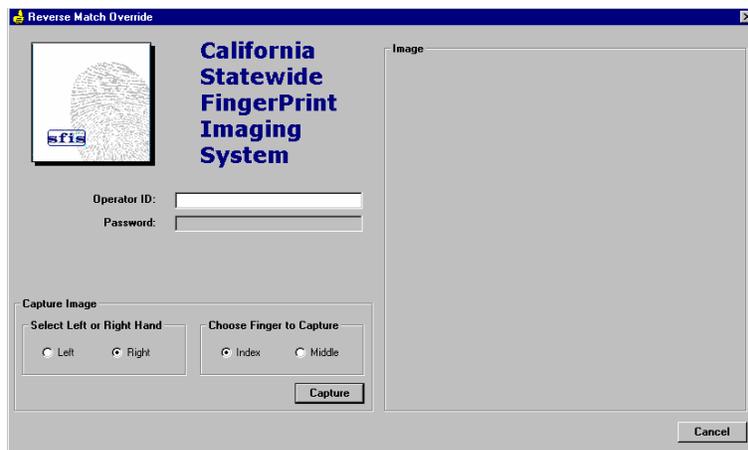


Exhibit: Reverse Match Override Screen

To capture the fingerprint, the user clicks on the Left or Right radio button in the Select Left or Right Hand box and the Index or Middle radio button in the Choose Finger to Capture box, and then clicks on the Capture button. The user with override authority must place the proper finger on the scanner when prompted. If the captured image is acceptable, the Reverse Match Override screen disappears and SFIS returns to the Add/Update screen with the Left tab activated. The user must now recapture both fingerprint images, making sure that the client is using the correct finger for each capture. The images previously captured are replaced by those captured the second time, if they are not reversed again.

To submit the search request, the user clicks on the Transmit button. The user knows that the record was sent to the Central Site successfully when they receive a message indicating the transaction was successful on the status menu.

**RFP OSI 2046
CURRENT SYSTEM**

FRAUD INVESTIGATION WORKSTATION (Only) USER FUNCTIONALITY

The Fraud Investigation Workstation users are the only users that utilize the following functions:

Fraud Review Function

SFIS provides a Fraud Review function to assist in the validation of search match results from the Central Site Matching subsystem. The purpose of the Fraud Review is to validate match results by displaying fingerprint images, client photos images, and client demographic data of matched cases side-by-side on the SFIS workstation screen. Fraud Investigators use the Fraud Review to view and analyze matches, and after following their county procedure for fraud investigation, log the results.

The records that are confirmed Open Search Match and Closed Search No Match by the Central Site verification staff are sent to the Fraud Review at the same time the Match Response is sent to the workstation that submitted the match request. The Fraud Investigator may review and investigate these match results to determine if fraud exists. The Fraud Investigator accesses the Fraud Review function by clicking on the *Fraud Review* button on the toolbar or selecting *Fraud Review* from the drop-down Function menu.

The Fraud Investigator has four (4) queues of information to view: Open Search – Match Found, Closed Search - No Match Found, Fraud Inquire, and Response List.

- **Open Search - Match Found** – The result of Open Searches that identified another CIN in the database with the same fingerprint images.
- **Closed Search - No Match Found** – The results of Closed Searches where the client's fingerprint images did not match the fingerprint images on file for a particular CIN.
- **Fraud Inquire** – The Fraud Investigator houses the requests for the images of any active CIN (CINs which have not been deleted by the State System Administrator) in the database.
- **Response List** – The Fraud Investigator may view and print the results of the relaunched search if it resulted in an Open Search Match.

The *Queues* area, in the center of the main Fraud Review screen, is the access point for the Fraud Investigator to view the current queues for the county or State, as applicable.

RFP OSI 2046 CURRENT SYSTEM

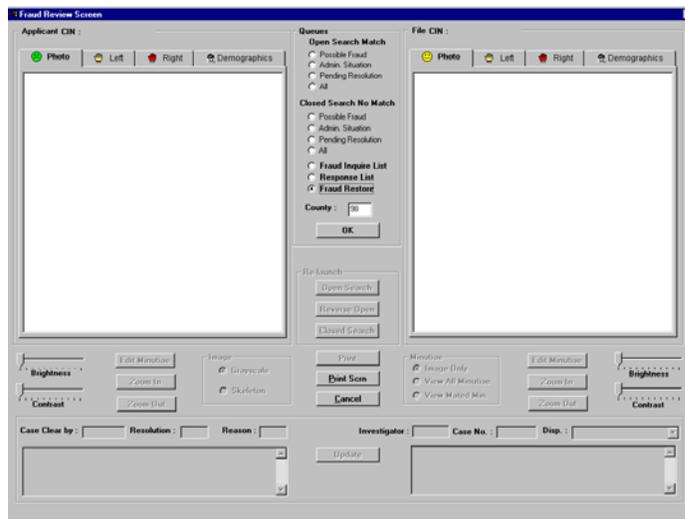


Exhibit: Fraud Review Screen

Viewing Records from the Queue

The Fraud Investigator decides which of the queues they are interested in viewing. With the Open Search - Match Found or Closed Search - No Match Found queue options, the Fraud Investigator has the following additional choices:

- **Possible Fraud** – Records in this section of the queue have been through the resolution process. For example, an authorized county staff member such as an Eligibility or Case Carrying Worker has researched the Match Response and determined that a Fraud Investigator should conduct further research on the client.
- **Administrative Situation** – Records in this section of the queue have also been through the Resolution process. The authorized county staff member has researched the Match Response and determined that the situation does not constitute possible fraud and is recommending no further investigation by the Fraud Investigator.
- **Pending Resolution** – Records in this section of the queue have not been through the resolution process. No one has responded with the results of research into the matching situation.

RFP OSI 2046 CURRENT SYSTEM

- **All** – This queue option displays all of the categories - Possible Fraud, Administrative Situation, and Pending Resolution - in one (1) queue list.

The Fraud Investigator chooses the queue view that they are interested in by selecting the appropriate radio button - *Possible Fraud*, *Administrative Situation*, *Pending Resolution*, or *All* - for either queue. The Exhibit below illustrates the queue after *Open Search Match - Possible Fraud* is selected.

Applicant CIN	Operator Id	Applicant Site	File CIN	File Site	Date	Resolution	PCN	Investigator	Disposition
71256712H	98AARI	9802	77447012H	9802	5/22/02	AS	9802B02142151519	JIMS	NF
71013471H	98EOGF	9802	90008656A	9802	6/19/01	AS	9802G01170183755	JIMS	NF
71013471H	98EOGF	9802	90009231A	9802	6/19/01	AS	9802G01170183755	BEBE	NF
78125212H	98DWEVW	9802	75399212H	9802	6/18/01	PR	9802J01167161641	SDJF	FA
90005881C	00GEOF	9802	90007132F	9802	6/18/01	AS	9802F01168094429	JOEY	PI
90738329A	00ALHH	9802	94171444D	9802	5/30/01	AS	9802H01150170156	JACK	NF
92136943A	00GEAN	9802	90887894A	9802	5/18/01	AS	9802B01138142223	MMMM	FA
90887894A	00GEAN	1999	70006358F	9802	5/18/01	PF	9802C01138141710	LJAR	UP

Exhibit: Fraud Queues

The queue is listed by the date and time of matching by default. Clicking the column title can change the sort order. For example, if the desired view is for PCN ascending order, the Fraud Investigator clicks the PCN column title once. Clicking it one (1) more time makes the queues display in descending order. From the list, the Fraud Investigator selects the desired match result to view in detail by highlighting the desired record and selecting the *OK* button. The Fraud Investigator can exit the queue display without viewing any further records by pressing *Cancel* button.

Fraud Review Screen Options

Upon selection of a record for review, the Fraud Review screen is populated with the selected search result information.

RFP OSI 2046 CURRENT SYSTEM

On the right side of the Fraud Review screen, SFIS displays information from the file client, which is the candidate or known case that was originally added to the SFIS database. Information from the applicant client, or newly captured record, is displayed on the left side of the screen, allowing the Fraud Investigators to perform a side-by-side validation.

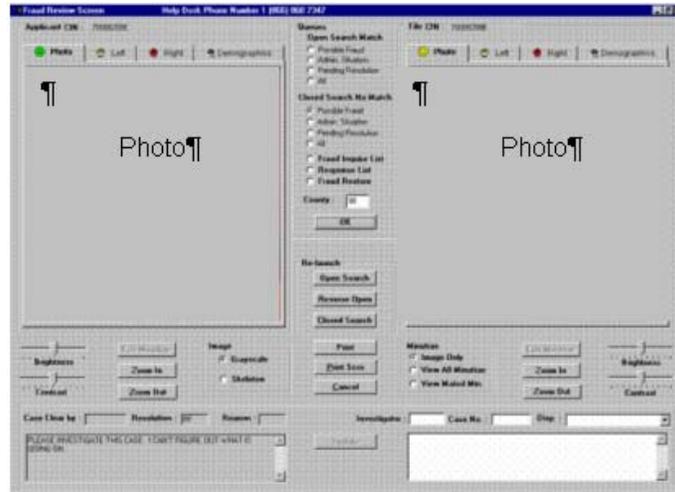


Exhibit: Fraud Review Screen with Photo Images

The Fraud Review screen displays with the Photo tab active. The Fraud Investigator may toggle between any of the available tabs (Photo, Left, Right, Demographics) by clicking the tab with the mouse pointer. For both the *Applicant* and *File* area tabs to toggle together, select an *Applicant* tab. For the file tabs to toggle independently of the *Applicant* tabs, select a *File* tab.

RFP OSI 2046 CURRENT SYSTEM

Fingerprint images (left and right) are selected separately by tab to allow appropriate viewing in the case of reversed images. For example, to view the right fingerprint image of the client under investigation, click on the tab marked Right under the *Applicant* client. The Fraud Review screen will then display the right fingerprint image for the applicant client and the file client, as shown below. Fingerprint images are selected separately by tab on the *File* client to allow appropriate viewing in the case of reversed images. For example, to view the left fingerprint image of the applicant under investigation, the Fraud Investigator would click on the tab marked Left under the *Applicant*. The Fraud Review screen will then display the left fingerprint image for both the applicant and the file client. To view the right fingerprint image for the *File* client, the Fraud Investigator would select the tab marked Right under the *File* client. This does not alter the view of the left fingerprint image displayed for the applicant.

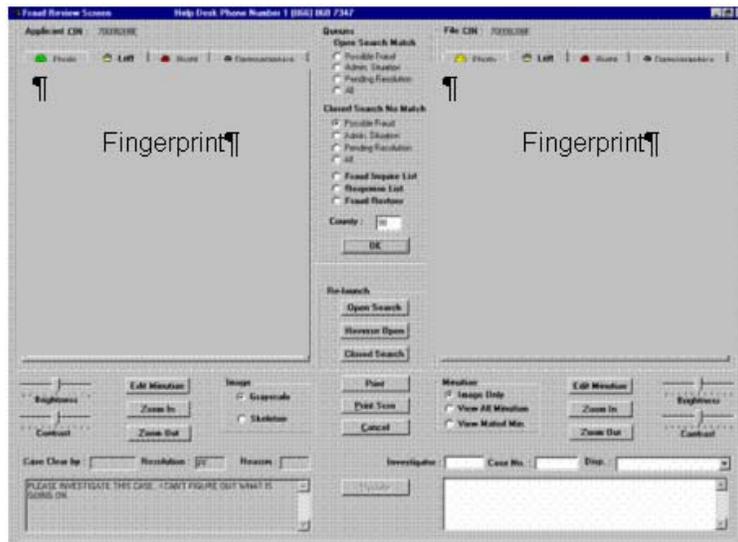


Exhibit: Fraud Review Screen with Fingerprint Images Displayed

RFP OSI 2046 CURRENT SYSTEM

Several tools are available to assist the Fraud Investigators in assessing match results. Below each displayed image, brightness and contrast controls are available to modify the image appearance. The fingerprint and photograph images may be enlarged first by clicking on the *Zoom In* button (up to ten (10) times), and then on the area of the fingerprint image to be enlarged. Click on the *Zoom Out* button to return to the original view. The same process can be performed on the fingerprint images independently.

Fingerprint images may also be displayed in a skeleton or binary view by clicking on the *Skeleton* button in the middle area of the screen. The Fraud Investigator may return to the original (grayscale) view by clicking the *Grayscale* button.

Client photograph images are displayed by selecting the Photo tab. The client photograph images are displayed in color, and may be enhanced utilizing the same brightness, contrast, and zoom tools used in the fingerprint image assessment.

Demographic information is displayed by clicking the Demographics tab. The Fraud Investigator cannot update information on the Demographics tab as the information is displayed as entered by the user and/or retrieved from SFIS/SCI. Demographic information for both the applicant client and the file client is displayed in place of the photos or fingerprint images.

RFP OSI 2046 CURRENT SYSTEM

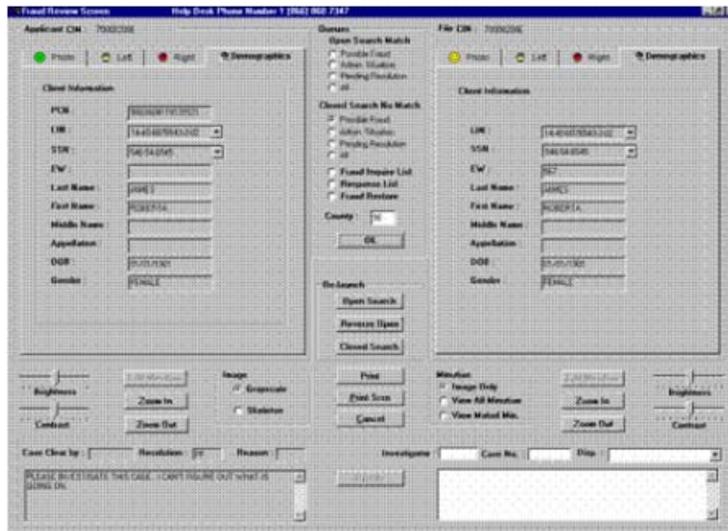


Exhibit: Fraud Review Screen with Demographic Information

The demographic information shown, in addition to the CIN, includes:

- PCN for Applicant CIN only;
- LIN;
- SSN;
- EW (Eligibility Worker Number);
- Last Name;
- First Name;
- Middle Name;
- Appellation (Jr., Sr., II, III, etc.);
- DOB (Date of Birth); and
- Gender.

The Fraud Investigator views multiple SSNs and LINs that have been entered into SFIS, by clicking on the down arrow on each of these fields.

RFP OSI 2046 CURRENT SYSTEM

The lower part of the screen contains image controls and additional information. The additional information displayed includes:

- Case Cleared By – The worker number of the person who determined the resolution code for the user to enter, if resolution is complete.
- Resolution Code – The resolution selection entered by the user (AS: Administrative Situation or PF: Possible Fraud) or an indication that the Match Response has not been resolved (PR: Pending Resolution).
- Reason Code – An additional code indicating the reason a resolution was determined to be an Administrative Situation.
- Comments from the user – Comments by the user who entered the resolution selection can be seen in the lower left side of the screen (this section is not labeled).
- Investigator – The worker number of the Fraud Investigator or person that has chosen to handle the review.
- Case No. – A seven (7) character field allowing a Fraud Investigator to note or assign a case number to the investigation.
- Disposition Code – The case disposition entered by the Fraud Investigator (NF: No Fraud, FA: Fraud Found Aided, FN: Fraud Found Not Aided, PI: Pending Investigation, UP: Under Prosecution).
- Fraud Comments Field – A free form field, on the lower right side of the screen, for comments entered by the Fraud Investigator. A Fraud Investigator may append notes in the field, but cannot remove notes previously entered.

Updating Information

The Fraud Investigator may update the following fields on the Fraud Review screen:

- Investigator (Fraud Investigator number);
- Case No. (internal fraud case number);
- Comments (by Fraud Investigator);
- Disp. (disposition code);

RFP OSI 2046 CURRENT SYSTEM

- Reason (the administrative reason when resolution is non-fraud; see below for explanation of how the reason is selected);
- Resolution (resolution code; see below for explanation of how the resolution is set).

To update the *Investigator* number, *Case No.*, or enter comments, the Fraud Investigator clicks in the desired field and types in the new information. Comments will append to any notes already in the free form field. Previously saved comments cannot be changed.

The disposition code (*Disp.*) is chosen from one (1) of the valid options on the drop-down menu, which is accessed by clicking on the down arrow next to the field. If the Fraud Investigator accesses the case before or without the user having processed it, the resolution code will be updated along with the disposition code. When the disposition code is NF (No Fraud), the resolution code is automatically set to AS (Administrative Situation). For all other disposition codes, the resolution code is set to PF (Possible Fraud). The Fraud Investigator ID is saved in the *Case Clear By* field. Whenever the disposition code is set to NF, the Fraud Investigator must also select a reason code. After selecting NF and pressing the *Update* button, an Administrative Situation Reason Code window appears.

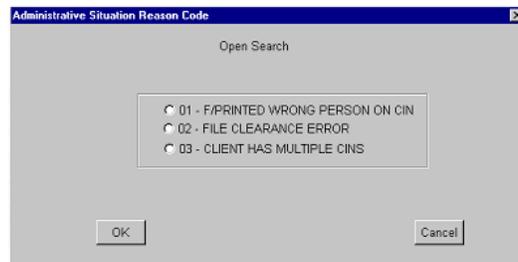


Exhibit: Administrative Situation Reason Code Window – Open Search

The values for the administrative reason code differ for Open and Closed Searches, as on the Resolution screen. Please refer to the Exhibit below for an example of an Administrative Situation Reason Code window for a Closed Search.

RFP OSI 2046 CURRENT SYSTEM

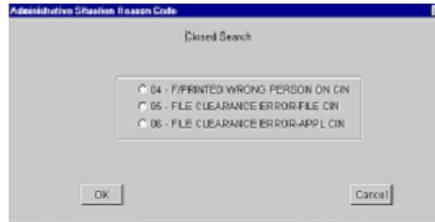


Exhibit: Administrative Situation Reason Code Window – Closed Search

The Fraud Investigator makes the reason code selection and presses the OK button. The system returns to the Fraud Review screen, and a message appears stating "Fraud Information Updated!"

If the OK button is pressed without making a reason code selection, a message appears advising "Select reason or click Cancel."

If the Cancel button is pressed, the Fraud Investigator is returned to the Fraud Review screen without completing the reason code selection, and a message is displayed stating "Disposition – Not Fraud – must have resolution reason!" The OK button is clicked to close the message box and the Fraud Investigator is returned to the Fraud Review screen as it was before the Update button was selected. The Fraud Investigator must either change the Disp. code to a fraud selection, or enter a reason code when prompted if NF is again selected for the disposition code.

Relaunch Images

Fraud Investigators have the ability to relaunch or rematch Open or Closed Searches. Typically, the Fraud Investigator would begin the process by viewing and editing minutiae.

The Fraud Investigator may choose to View All Minutiae or View Mated Minutiae. Clicking on one (1) of these radio buttons displays the system-determined minutiae points or system-mated minutiae points for the fingerprint image.

**RFP OSI 2046
CURRENT SYSTEM**

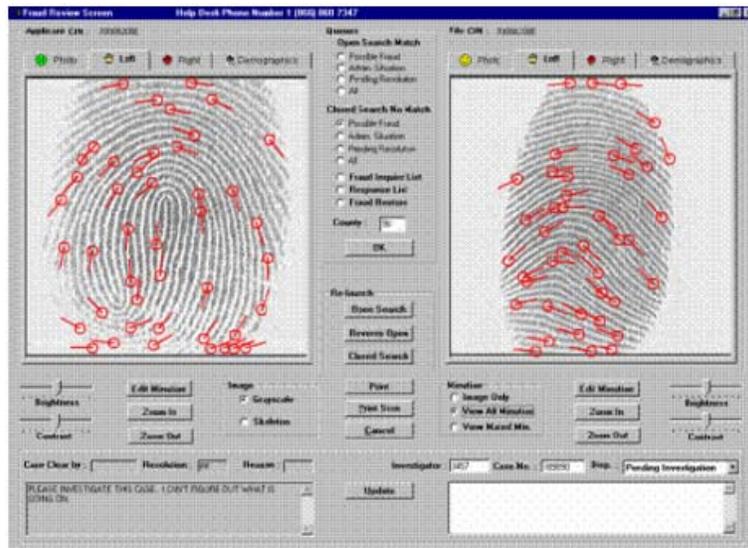


Exhibit: Fraud Review Screen View All or Mated Minutiae

When the Fraud Investigator clicks on the View All Minutiae radio button, all SFIS generated minutiae will be displayed for both images. Minutiae can be viewed in both grayscale and skeleton modes and can also be zoomed in and out. To add and remove minutiae, the Fraud Investigator clicks on the Edit Minutiae button under the fingerprint image to be edited. The Edit Minutiae screen is displayed. The fingerprint image on the Edit Minutiae screen is displayed in grayscale only.

The Fraud Investigator may click on the Add button to begin adding minutiae. Then, he/she clicks and holds the mouse button down where the minutiae point is to appear on the fingerprint image and drags the mouse pointer in the same direction that the ridge direction indicator is to appear on the fingerprint image. Once satisfied with the ridge indicator position, the Fraud Investigator may release the mouse button and a red line will appear on the screen along with the Minutiae Editing dialog box. The new minutiae point can be added simply by clicking on the OK button. If the minutiae point was added in error, or positioned incorrectly, click on the Cancel button.

RFP OSI 2046 CURRENT SYSTEM

The system-generated minutiae may be removed by clicking on the Remove button. The Fraud Investigator positions the mouse pointer near the minutiae to be removed, clicks and holds the mouse button, and drags the pointer toward the minutiae to be removed. An outline box will appear on the screen. Continue to drag the pointer in such a way as to completely encompass the minutiae to be removed. If the minutiae were not properly selected, the outline box will disappear when the mouse button is released. The minutiae will need to be reselected. Once the minutiae have been properly selected and the mouse button released, the Minutiae Editing dialog box will appear. The Fraud Investigator will click on the OK button to remove the minutiae, or on the Cancel button to leave the minutiae on the screen. Depending on the position of the intended minutiae and other minutiae near the one (1) to be removed, the minutiae point and the ridge indicators may need to be removed separately to avoid removing more than just the intended minutiae.



Exhibit: Minutiae Editing

The Fraud Investigator maneuvers the mouse pointer directly over a line (either the minutiae point or the ridge indicator) until the arrow changes into a gun sight. Click on the line, which will turn blue, and the Minutiae Editing dialog box will appear. Click on the OK button and continue until the desired minutiae are removed. When editing is complete, the Fraud Investigator clicks on the Save button and SFIS will return the user to the Fraud Review screen.

RFP OSI 2046 CURRENT SYSTEM

After reviewing the data and/or modifying the minutiae marked on the fingerprint images, the Fraud Investigator has the ability to launch a Closed Search Match against the File client by clicking on the Closed Search button. For an Open Search request, the Fraud Investigator selects the Open Search button to send the fingerprint images to the Central Site for matching. This process does not change the minutiae stored in the Matching subsystem. The Fraud Investigator clicks on the appropriate Re-launch button: Open Search, Reverse Open, or Closed Search. The Open or Closed Search Confirmation message window appears on the screen showing the PCN assigned to the search. Click on the OK button to remove the message.

When launching an Open Search, the request matches the fingerprint images against all other fingerprint images in the database, without adding the fingerprint images to the database after the matching process is complete.

If records exist that were previously requested by another Fraud Investigator as an Open Search or Reverse Open, the Existing Fraud Re-launches window appears.

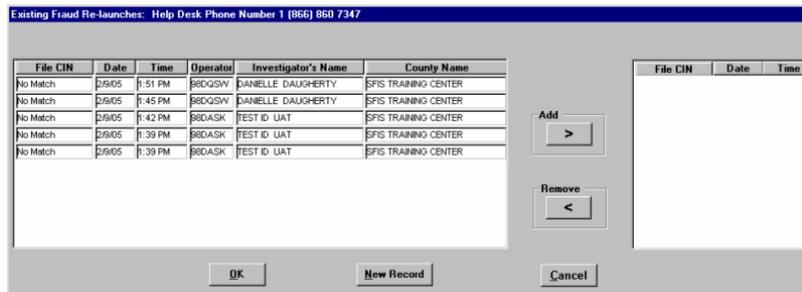


Exhibit: Existing Fraud Re-Launches Window

The Existing Fraud Re-Launches window functions the same as the Existing Fraud Inquiries window as previously explained in this document. Please refer to that section for more details on how to use this window.

If no existing requests exist, as is the most common scenario, the Open or Closed Search Confirmation message window appears on the screen showing the PCN assigned to the search. Click on the OK button to remove the message.

RFP OSI 2046 CURRENT SYSTEM

The Open Search Confirmation message window confirms that the request has been sent to the Central Site Matching subsystem and displays the PCN assigned to the search request.



Exhibit: Open Search Confirmation Window

Once the Central Site matching process is complete, the rematch search result is listed in the Response List pending further investigation. The Response List only contains records that have been requested by the current Fraud Investigator. Therefore, if the user wants a record to appear in the Response List, they must perform an Open, Reverse, or Closed Search relaunch of the record. The results remain on the Response List for 60 days following completion of the matching process.

Worker	Case	PCN	CIN	Last Name	First Name	DOB	Search Type	Match	Date	Time	Status
98DGMT		9802A05055112635	77866902H	WILLIS	GEORGE	04/09/1981	Reverse Open	N	02/24/2005	11:22:42	Completed
98DGMT		9802A05055112823	77866902H	WILLIS	GEORGE	04/09/1981	Closed Relaunch	Y	02/24/2005	11:24:28	Completed

Remove From Queue View Print Print List Cancel

Exhibit: Response List

The Remove from Queue button is used to manually remove records from the list when they are no longer needed. This removal applies only to the current Fraud Investigator's queue. If other investigators have requested a copy of the record it will still appear on their respective list. The Fraud Investigator may view and print the results of the relaunched search if it resulted in an Open Search Match or Closed Search No Match. Closed Search Match and Open Search No Match results appear as messages only and cannot be printed.

RFP OSI 2046 CURRENT SYSTEM

Results of relaunched Open Search Matches are retained on the database for six months; however results of Open Search No Matches are only kept on the database for 60 days.

Two Cin Search Function

The Two CIN Search function provides the capability to perform a Closed Search comparison on any two CINs containing fingerprint images in the database, at the request of the Fraud Investigator.

The Two CIN Search function is accessed by selecting the *Two CIN Search* icon from the toolbar, or by selecting *Two CIN Search* from Search on the drop-down Function menu. Once the Fraud Investigator selects *Two CIN Search*, the Two CIN Search window appears on the screen.

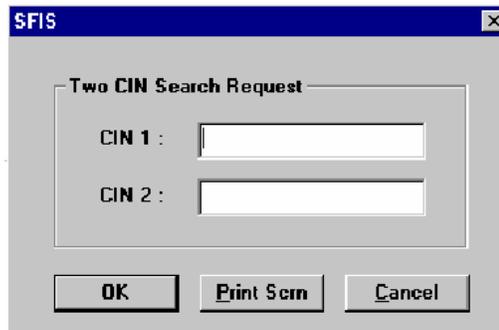
The image shows a screenshot of a software dialog box titled "SFIS" in the top-left corner. The main title of the dialog is "Two CIN Search Request". Inside the dialog, there are two text input fields. The first field is labeled "CIN 1 :" and the second field is labeled "CIN 2 :". Below these fields are three buttons: "OK", "Print Sern", and "Cancel". The "Print Sern" button appears to be a typo for "Print Screen".

Exhibit: Two CIN Search Window

The user enters the CIN of the first record in the *CIN 1* field, tabs to the *CIN 2* field, and enters the CIN of the second record. SFIS performs online edit checks to ensure only valid CINs are entered, and that both CINs have fingerprint images.

Once both CINs are entered correctly, the user selects *OK*. The Search dialog window disappears, and the Two CIN Search Confirmation message window displays the PCN generated for this search request. SFIS retrieves the fingerprint images for the requested CINs, and performs a one-to-one comparison. The results are returned immediately with either "Match" or "No Match" in red, along with the PCN, on the Two CIN Search Requested message box. Both types of responses are shown in the Exhibit below.

RFP OSI 2046 CURRENT SYSTEM



Exhibit: Match Results

The Fraud Investigator acknowledges the message, and clicks the *OK* button or presses the <Enter> key. It should be noted that results will be retained in the Response List for six (6) months.

Fraud Restore Function

The archive process is run on a nightly basis. When performing a Fraud Archive, the Fraud function looks for online fingerprints, photos, and demographics involved in an Open Search Match or Closed Search No Match that are older than six (6) months, with the following exceptions:

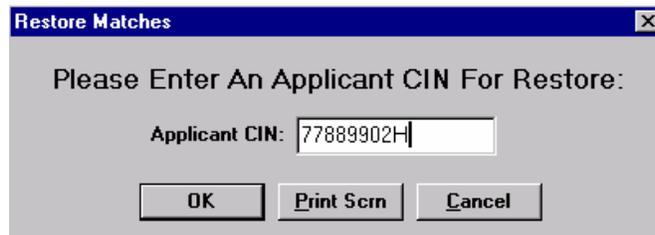
- PI – Pending Investigation disposition code
- UP – Under Prosecution disposition code
- PR – Pending Resolution status and no disposition code
- PF – Possible Fraud Resolution status and no disposition code

The Fraud Archive process finds all records that meet the archival criteria and removes each row into its own flat file. Each flat file is then inserted into the applicant zip file in the Fraud DIRS directory. A pointer to the fraud applicant zip file is placed in the Match Archive table (t26_marchive). If a Fraud Investigator needs to review the record again, they must retrieve it through the Fraud Restore function explained in the subsection below.

**RFP OSI 2046
CURRENT SYSTEM**

As long as there is space in the Fraud DIRs directory, all records will be kept online; therefore restores will take place immediately. However in the future, when the Fraud DIRs directory fills up, an archive to tape process will be necessary and therefore a restore could take up to two (2) business days. It is estimated that it will take four (4) to six (6) years (approximately 2008 at the earliest) for the directory to reach its maximum capacity. When a record is removed from online storage, it will be assigned a Digital Linear Technology (DLT) tape number in the database. The oldest records will be archived to tape first. Records archived to tape are stored offsite and will be retrieved by the Central Site when the Fraud Restore request is received.

The Fraud Investigator uses the Fraud Restore function to retrieve Open Search Match and Closed Search No Match records previously archived through the Fraud Archive process described above. To initiate a Fraud Restore, the Fraud Investigator selects Restore from the Function drop-down menu. The Restore Matches window opens. The restore is initiated using the applicant CIN. The Fraud Investigator enters the applicant CIN in the field provided and selects OK.



Restore Matches

Please Enter An Applicant CIN For Restore:

Applicant CIN: 77889902H

OK Print Scrn Cancel

Exhibit: Restore Matches Window

The Fraud Restore function checks the database for any archived records where the given CIN was the applicant on the fraud record. The Restore Request window then lists the records available to restore.

RFP OSI 2046
CURRENT SYSTEM



Exhibit: Restore Request Window – Records Available For Restore

The Fraud Investigator can select one (1) record at a time or all records available for restore. To select a record to restore, the Fraud Investigator highlights the desired record in the *Available for Restore* list and then presses the single *Add >* button to move the record to the *Records to Restore* list. The *Add all >>* button is used to move all records at once. If a mistake is made, the *Remove <* button is used to move the record back to the *Available for Restore* list, or the *Remove all <<* button is used to move all records at once.



Exhibit: Restore Request Window - Records to Restore

RFP OSI 2046 CURRENT SYSTEM

When all of the desired records have been moved to the *Records to Restore* list, the Fraud Investigator selects the *OK* button to complete the request. The Restore Request window is closed, and the records are flagged for restore. A confirmation message appears listing the number of records and status for the restore. The *OK* button is pressed to close the confirmation window.



Exhibit: Restore Confirmation Message

Assuming the records have not been archived to tape, any previously archived records associated with the CIN will be available for immediate viewing within the *Fraud Restore* queue. Restored record information includes demographics, fingerprint minutiae files, fingerprint images, and photograph images. The Fraud Investigator accesses the queue by opening the Fraud Review screen via the Function menu, and then selects the *Fraud Restore* button and presses *OK*.

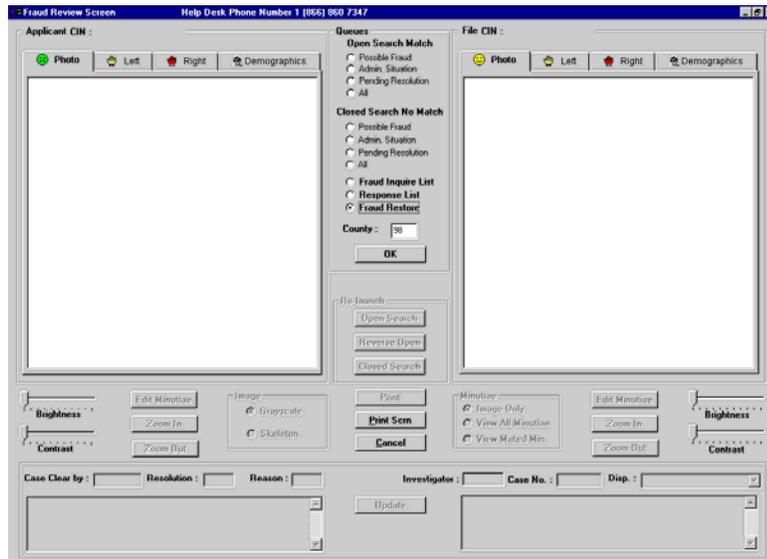
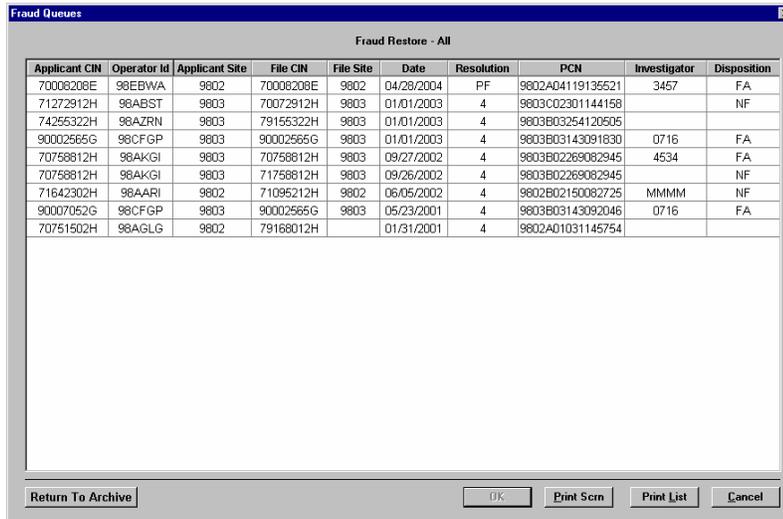


Exhibit: Fraud Review Screen with Fraud Restore Button

**RFP OSI 2046
CURRENT SYSTEM**

The Fraud Queues window then opens.



Applicant CIN	Operator Id	Applicant Site	File CIN	File Site	Date	Resolution	PCN	Investigator	Disposition
70008208E	98EBWA	9802	70008208E	9802	04/28/2004	PF	9802A04119135521	3457	FA
71272912H	98ABST	9803	70072912H	9803	01/01/2003	4	9803C02301144158		NF
74255322H	98AZRN	9803	79155322H	9803	01/01/2003	4	9803B03254120505		
90002565G	98CFGP	9803	90002565G	9803	01/01/2003	4	9803B03143091830	0716	FA
70758812H	98AKGI	9803	70758812H	9803	09/27/2002	4	9803B02269082945	4534	FA
70758812H	98AKGI	9803	71758812H	9803	09/26/2002	4	9803B02269082945		NF
71642302H	98AARI	9802	71095212H	9802	06/05/2002	4	9802B02150082725	MMMM	NF
90007052G	98CFGP	9803	90002565G	9803	05/23/2001	4	9803B03143092046	0716	FA
70751502H	98AGLG	9802	79168012H		01/31/2001	4	9802A01031145754		

Exhibit: Fraud Queues – Fraud Restore Window

The Fraud Investigator selects the desired record to view and presses *OK*. The record is then loaded into the Fraud Review screen for review. Restored records are kept on the restored table for a six (6) month period or can be removed at any time by the Fraud Investigator. If desired, the Fraud Investigator may return the restored record to archive by selecting the desired record and pressing the *Return to Archive* button.

If a record requires retrieval from tape, it will need to be retrieved from offsite storage first before being available for viewing in the *Fraud Restore* queue. Records which were archived to tape will be available within two (2) business days after the Fraud Restore request is received. The Central Site receives the restore request, retrieves the archived information, and posts the record to the Match table on the database.

**RFP OSI 2046
CURRENT SYSTEM**

SYSTEM ADMINISTRATION WORKSTATION (Only) USER FUNCTIONALITY

Typically, only the users of the System Administration Workstation use the following functions:

Security Function

The Security Function is used to create user IDs, reset passwords, enable password vs. fingerprint logon, capture user fingerprint images (Often, the SAW does not have a scanner attached, so the images must be captured at a Multifunction Workstation instead.), activate and deactivate users, assign security levels, customize security levels, unlock workstations, create and update site assignments, and update user information.

To enter the Security screen, the user clicks on the *Administration* icon on the toolbar, or selects *Administration* from the Security drop-down menu. The Maintain Security screen will appear.

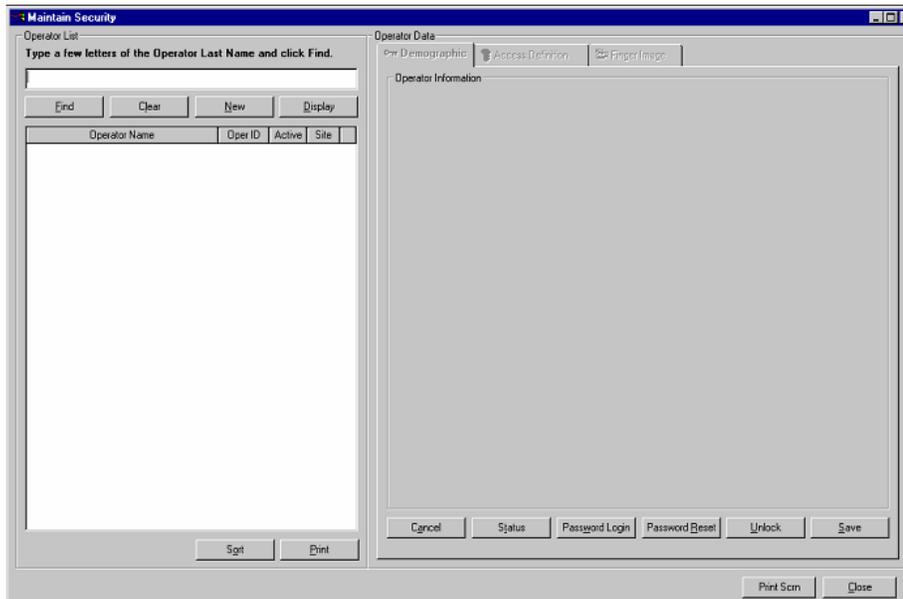


Exhibit: Maintain Security Screen

The user may leave the Security screen at any time by clicking the Close button.

RFP OSI 2046 CURRENT SYSTEM

Add New User

To add new users to the SFIS Security table, click on the New button and then enter all demographic information for the new SFIS user. Demographic information to be added includes:

- First Name – New user's first name;
- Last Name – New user's last name;
- Security Level – The security level of the new user. The appropriate security level could be selected from the drop-down box. The default value will be A;
- County – Select the county from the County field;
- Site ID – Chosen from the available Site ID options on the drop-down list; and
- Start Date – Defaults to the current date.

To add the user to SFIS, click on the Save button. An SFIS message box appears to advise, "Default access for the security level has been granted." Once the OK button is pressed, another message box advises, "Transaction completed successfully." After clicking on the OK button, SFIS generates and fills in a new user ID.

The Last Login Date is pre-filled with all zeros (0) (00/00/0000) to indicate that the user has not logged on to SFIS. This field is updated each time the user successfully logs on to SFIS to track user ID activity.

The Password Change field is pre-filled with nines (9) i.e. 99999999. This field will change when the user changes their password. To enable the new user to log on with a password instead of a fingerprint capture and match, click on the *Password Login* button. Two (2) message windows will appear. Once the OK button is pressed, the box next to Able to Login with Password will be checked and no fingerprint image for the user will be captured.

The user Status automatically defaults to "Active."

The Lock Status field is pre-filled with zero (0) to indicate that the user ID is not locked out and has had zero (0) failed logon attempts. The Lock Status field is incremented each time that a failed logon attempt via password is made. The Lock Status field gets reset back to zero (0) if the user has a successful logon on the second or third try. If the user fails to have a successful logon after three (3) attempts, (that is, the indicator reaches three), the user ID cannot be used until the Lock Status field is reset to zero (0).

RFP OSI 2046 CURRENT SYSTEM

After the Save button is pressed, the system performs data validation checks at the character and field level to ensure only valid information is added to the SFIS Security database table. The <Tab> key can be used to move from field to field. If data is entered in error, SFIS displays an error message.

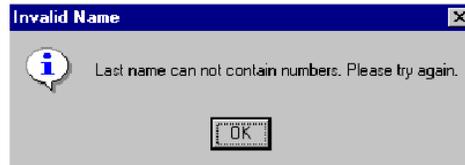


Exhibit: Data Entry Error Message Window

SFIS displays the Data Entry Error message window, and highlights all data fields that contain errors. Acknowledge the errors by clicking OK in the Data Entry Error message window, correcting the highlighted items, and then click on the Save button again.

Upon completion of the demographic field entry, the Access Definition tab should be selected in the user Data area of the screen.

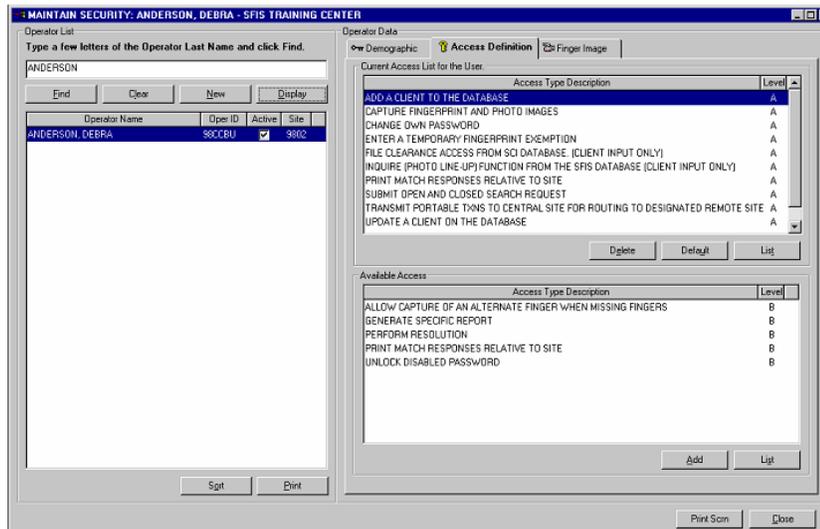


Exhibit: Access Definition Tab

The upper half of the *user Data* area labeled Current Access List for the User will be pre-filled with the user tasks that are the default for the security level entered.

RFP OSI 2046 CURRENT SYSTEM

Any of the tasks listed may be deleted by highlighting the task and clicking on the Delete button. A confirmation message will appear. Delete the task by clicking on the OK button. What was deleted will now be located under the *Available Access* area. The choices may be set back to the default setting for the security level by pressing the Default button. A message box will then appear. Click on the OK button to confirm.

Additional user tasks that may be given to a particular user are shown in the lower list labeled Available Access. Any items shown in the Available Access panel may be added to the Current Access List for the User by highlighting the desired item and pressing the Add button.

For a security level A user, the Available Access list will show those items unique in the default list for security level B users. For security level B users, the list will contain items unique to security level C users. For security level C users, the list will show those items unique to security level E users.

If the user ID is security level A, B, or C, SFIS activates the finger image capture area of the Maintain Security screen (if the password logon has not been enabled). The fingerprint images for these users are captured, as they may be required to log on to SFIS with their user ID and fingerprint.

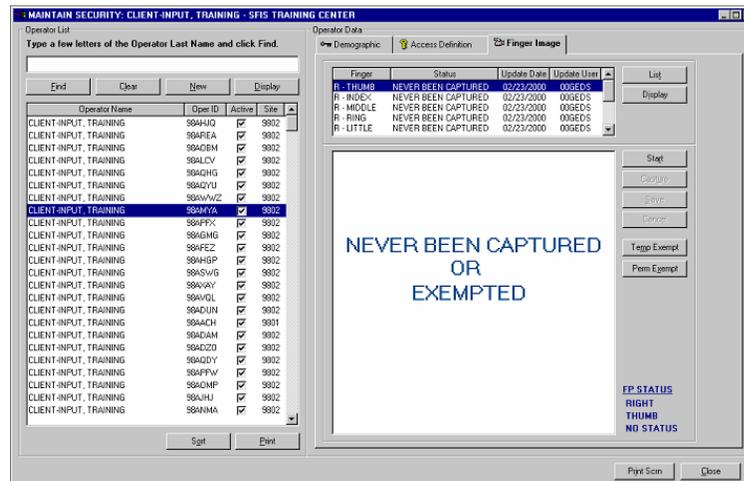


Exhibit: Finger Image Capture Tab

Begin by clicking on the Finger Image tab. Double click on a row representing the finger image to be captured from the list above the capture area. In the example shown in the Exhibit, the right thumb has been selected

RFP OSI 2046 CURRENT SYSTEM

from the list that has not been captured. Determine if the image will be captured or exempted. If the finger is determined to be exempt, indicate the exemption by clicking the Temp Exempt or Perm Exempt button. Select the Temp Exempt option if the user's finger is injured or bandaged and may be recaptured at a later date. Select the Perm Exempt option if the user's finger is missing.

To initiate the capture process, the user presses the *Start* button. This will cause the video capture window to become active. At this time there will be lines (crosshairs) on all four (4) sides of the live window that run almost to the center of the window. These lines signify where the core of the fingerprint should be placed. Additionally, fingerprint capture instructions will be displayed in place of the *user List* section of the screen. The instructions are: "Clean scanner with white wipe," "Clean finger with yellow wipe," "Center core," "Press finger lightly on scanner," "Press Capture," "Press finger harder on scanner (vary pressure during capture)," and "Remove finger when status bar appears."

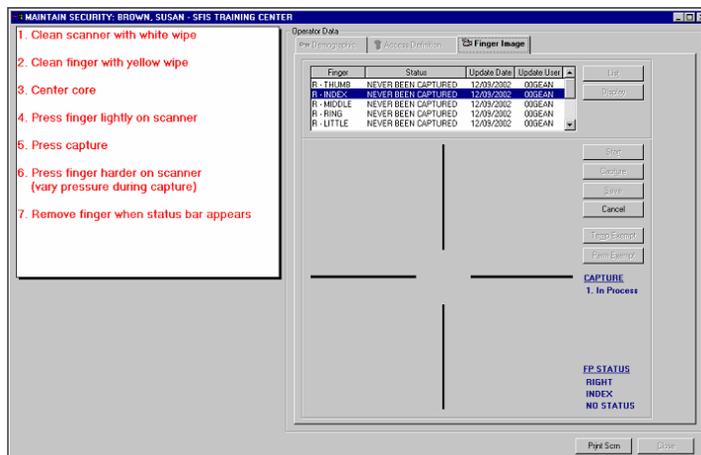


Exhibit: Maintain Security Screen with Crosshairs and Instructions

The only available option at this point is the Cancel button. To get the Capture button to become live, the user needs the person being fingerprinted to press their finger onto the fingerprint scanner platen. At this point, the software will sense the presence of a finger and will enable the *Capture* button. Press the capture button to start the capture session.

Once the maximum number of capture seconds (as defined in the .ini file) has passed, the message area will be replaced by a process meter. While the

RFP OSI 2046 CURRENT SYSTEM

process meter is displayed, the system will sort the results placing the best x images (x equals the number of capture attempts defined in the .ini file) at the top of the list to be processed. These images are then put through a more extensive Motorola/Printrak quality check. Once each of the five (5) images has been processed, the data is again sorted. The first sort criterion is the Check Image Quality (CIQ) value. In the event that multiple images have the same CIQ value, the Contextual Enhancement Processor (CEP) and Fast Image Quality (FIQ) values are used to break the tie. If the top image based on the secondary sort is of acceptable quality, the process will continue and prompt the user to Save the images. If the top image is deemed unacceptable, the application displays an error message.

Deleted: Printrak



Exhibit: Capture Error Message

The user acknowledges the message by pressing the OK button, and the application will prompt the user to attempt to capture the prints again. This can happen up to three (3) times before the software either chooses the best of the bad quality, or decides the prints are unacceptable. If a print is deemed unacceptable quality, the user can attempt to recapture the images at a later date. When the process is over, the capture instructions and process meter are hidden and the user List area will again be displayed.

Users are required to change their password at least every ninety (90) days. The last five (5) passwords utilized by the user are stored, prompting the user to generate a password that has not been used the past five (5) times. The number of unsuccessful logon attempts via password is limited to three (3) to prevent unauthorized persons from accessing SFIS.

Update User

To update user information, enter a few or all of the letters of the user's last name in the search field and click on the Find button. SFIS verifies that the user ID is found in the database. If the user ID is not found, an error message is returned to the screen. All users meeting the search criteria are displayed. A particular user may be selected from the return list by highlighting the appropriate row and pressing the Display button or double clicking on the highlighted name.

The information displayed can then be updated. The various updates are described below.

RFP OSI 2046 CURRENT SYSTEM

- Password – The password may be updated to a default password. This update has the effect of replacing the password when the remote workstation is networked to the Central Site, allowing assistance to the user who has forgotten their password.
- First or Last Name – These fields may be updated to correct clerical errors or name changes.
- Start Date – The original Start Date may not be modified.
- Lockout – Press the Unlock button to reset the Lock Status field. This effectively clears a lockout for a user who has had three (3) unsuccessful logon attempts. The user would then have three (3) more attempts to log on using their password before the lockout occurred again.
- Site ID – The Site ID may be updated to reflect a transfer to another office.
- Fingerprint Images (levels A, B, or C only) – The fingerprint information may be updated for users who had their original fingerprint capture entered as temporary exempt. Unacceptable quality images must be removed by the SFIS Help Desk.

For any of the items that may be updated on the Security screen, except for fingerprint images, type over the pre-filled information. Press the <Tab> key to move from field to field. Once all updates are complete, press the Save button to transmit the updated information to the Central Site for storage. When the Save button is clicked, the system performs data validation checks at the character and field level to ensure only valid information is added to the SFIS Security database table. A Transfer Completion message box will appear. Click on the OK button to acknowledge the successful completion.

To initiate the capture process, the user presses the Start button. This will cause the video capture window to become active. At this time there will be lines (crosshairs) on all four (4) sides of the live window that run almost to the center of the window. These lines signify where the core of the fingerprint should be placed. Additionally, fingerprint capture instructions will be displayed in place of the user List section of the screen. The instructions are: "Clean scanner with white wipe," "Clean finger with yellow wipe," "Center core," "Press finger lightly on scanner," "Press Capture," "Press finger harder on scanner (vary pressure during capture)," and "Remove finger when status bar appears."

RFP OSI 2046 CURRENT SYSTEM

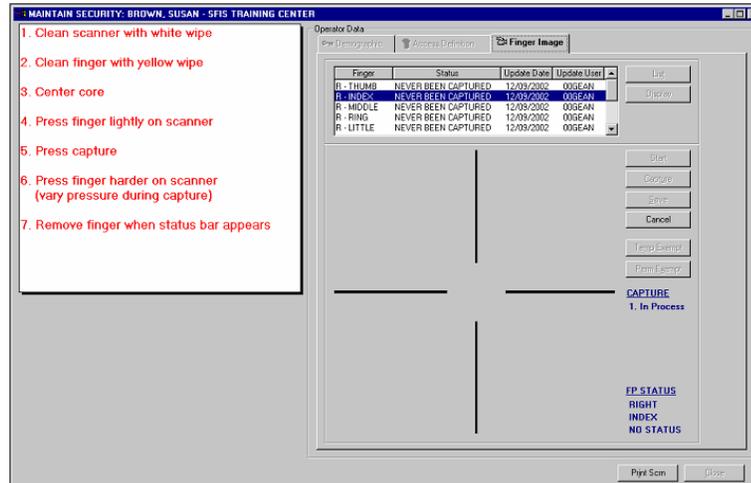


Exhibit: Maintain Security Screen with Crosshairs and Instructions

The only available option at this point is the Cancel button. To get the Capture button to become live, the user needs the person being fingerprinted to press their finger onto the fingerprint scanner platen. At this point, the software will sense the presence of a finger and will enable the Capture button.

Once the maximum number of capture seconds (as defined in the .ini file) has passed, the message area will be replaced by a process meter. While the process meter is displayed, the system will sort the results placing the best x images (x equals the number of capture attempts defined in the .ini file) at the top of the list to be processed. These images are then put through a more extensive Motorola/Printrak quality check. Once each of the five (5) images has been processed, the data is again sorted. The first sort criterion is the CIQ value. In the event that multiple images have the same CIQ value, the CEP and FIQ values are used to break the tie. If the top image based on the secondary sort is of acceptable quality, the process will continue and prompt the user to Save the images. If the top image is deemed unacceptable, the application displays an error message.

Deleted: Printrak



Exhibit: Capture Error Message

RFP OSI 2046 CURRENT SYSTEM

The user acknowledges the message by pressing the OK button, and the application will prompt the user to attempt to capture the prints again. This can happen up to three (3) times before the software either chooses the best of the bad quality, or decides the prints are unacceptable. If a print is deemed unacceptable quality, the user can attempt to recapture the images at a later date. When the process is over, the capture instructions and process meter are hidden and the user List area will again be displayed.

Once an acceptable quality fingerprint image is captured, select another row or choose to capture a fingerprint image on the other hand using the same process. When the updates are complete, press the Save button to send the updates to the Central Site.

Inactivate User ID

To inactivate a user ID, type a few or all of the letters of the user's last name in the Search field and click the Find button. All users meeting the search criteria are displayed. To select a particular user, highlight the appropriate row and click the Display button or double click on the highlighted name. If the user ID is not found, an error message is returned to the screen.

Press the Status button to inactivate the user ID. SFIS will display a Confirmation window asking, "Are you sure you want to inactivate the user?" Complete the transaction by pressing the OK button on the Confirmation window and again on the Success message box. The Active box is then shown unchecked. SFIS removes the user ID from the active user IDs, effectively preventing its use to log on to SFIS. The user ID is then inactivated, but may be re-activated at a later time by using the Search window to locate the user ID and clicking on the Status button. Click the OK button on the two (2) message boxes. The Active box will be shown checked.

County Preferences

County Preference selections are entered on the Maintain County Preference screen. The Maintain County Preference screen allows the State System Administrator to modify county parameters such as the default printing of responses, match reasons, and operating hours. It only allows the County System Administrator to modify the county default printing of responses.

The State System Administrator chooses the county to update on the left side of the screen in the County List area.

RFP OSI 2046 CURRENT SYSTEM

On the Match Response tab, all defaults for match response printing are initialized to automatically print text plus photo. The State System Administrator (and the County System Administrator) can use the Maintain County Preference screen to change the default to print text plus photo and fingerprint images by clicking on the appropriate radio button. The default setting may be resumed by clicking on the Default button. Please refer to the Exhibit below.

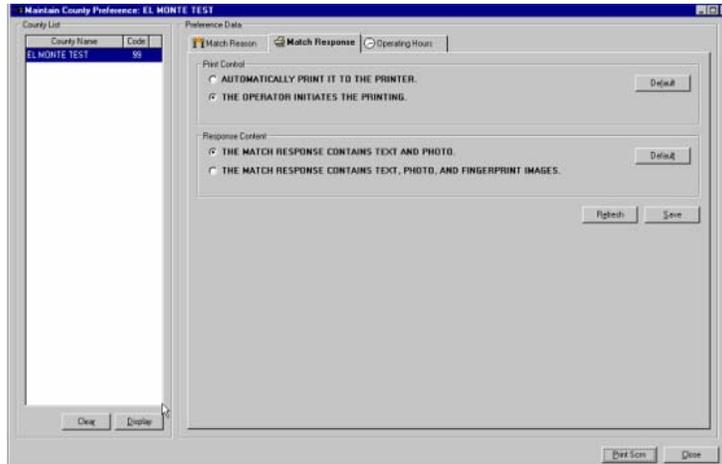


Exhibit: Maintain County Preference Screen

Printing automatically can also be updated to “The user initiates the printing” by clicking on the appropriate radio button. The default setting may be resumed by clicking on the Default button. Preference selections take effect for each individual user at their next logon to the SFIS application.

During the resolution process, users enter either Administrative Situation or Possible Fraud on Open Search Match or Closed Search No Match results. Each Administrative Situation also requires a Match Reason to be entered. The reasons are maintained by the State System Administrator and can be updated on the Match Reason tab of the Maintain County Preference screen.

RFP OSI 2046 CURRENT SYSTEM

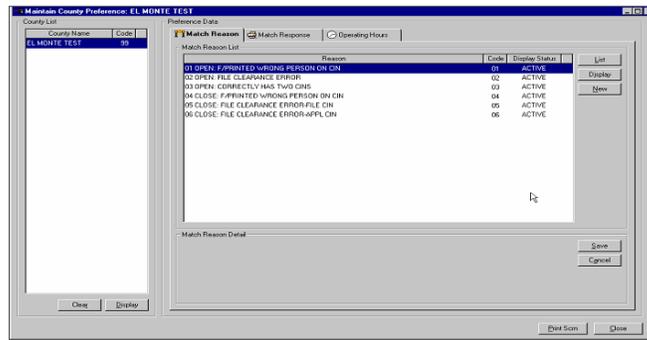


Exhibit: Match Reason Tab

To select a reason, the State System Administrator highlights the reason in the list and then double clicks on it. The reason detail displays underneath in the Match Reason Detail area. Reasons can be deactivated by clicking on the checkbox next to Active. A blank field indicates that the reason code is no longer active. The reason description can be updated by simply typing over the existing description text. New codes can be added (up to a total of ten (10) active codes) by clicking the New button. After making any changes, the information must be saved by clicking the Save button.

Operating hours for the selected county can be viewed by selecting the Operating Hours tab as shown below. The State system administrator has the option to set operating hours from 7 a.m. to 7 p.m.

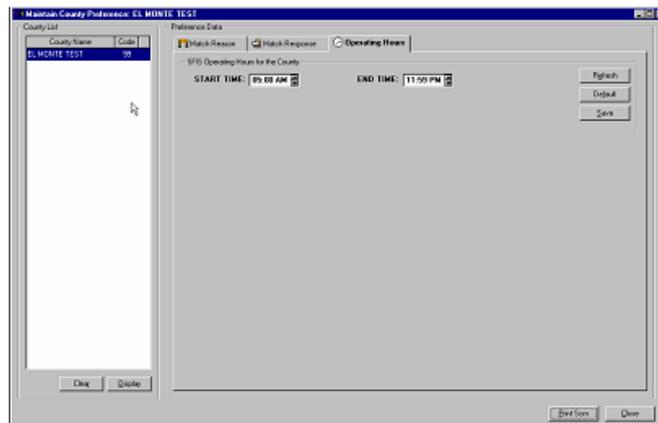


Exhibit: Operating Hours Tab

RFP OSI 2046 CURRENT SYSTEM

Crystal Reports

Seagate Crystal Reports is a standard desktop reporting and analysis tool that combines ease of use with flexibility and power to deliver professional reports. The Crystal Reports application is available at the System Administration Workstation to provide access to ad hoc reporting capabilities against the SFIS database. The application queries the SFIS database and returns the result to the workstation. The user can design the report format desired and print the report on the attached laser printer.

Audit Controls And Security

General Explanation

SFIS currently has internal controls, quality assurance, indexing, security, and other features to demonstrate that fingerprint images and photographs represent an accurate facsimile of the originals, and that rigid security criteria have been met in their capture, storage, and reproduction. These features include logging of all transactions to create an audit trail, quality assurance, testing, indexing of all transactions and associated image files through the Process Control Number (PCN), password and fingerprint logon protection, and limited access by programmers to data files. All fingerprint images represent accurate facsimiles of the originals.

Rigid security criteria are enforced in the capture, storage, and reproduction of fingerprint data. SFIS provides the following levels of security protection:

- Multi-level controls that protect every SFIS workstation against unauthorized access. Each individual must enter a valid username and fingerprint image or password to sign-on before beginning work with SFIS. This required sign-on is also used for the system consoles. For example, if the sign-on combination is valid on the matching subsystem console, the System Mode Selection menu is displayed; otherwise, a log-on failure message is displayed.
- Mandatory redefinition of passwords (every ninety (90) days).
- Defined sets of privileges that limit the functions each user can perform once logged on to the system. The State System Administrator controls privileges centrally and can assign appropriate privileges to any user and/or workstation. Each

RFP OSI 2046 CURRENT SYSTEM

additional level of access typically includes privileges of lower levels.

- Batch file processing restricted to system consoles connected to the Central Site processors. The State System Administrator maintains a separate set of user accounts, passwords, and privileges for these consoles, separate from the remote site workstations. This allows the State System Administrator to restrict the ability to purge minutiae and image files to certain key personnel.

User Password

SFIS provides restricted access to information system facilities, systems operating environments, and data file contents. The security attributes ensure only authorized access to State data. Each user is provided a unique ID that limits access by the security level to which they are assigned, and all fingerprint imaging workstation operating systems are secure against unauthorized access. SFIS is designed to accept either a user password or perform a CLOSED search on the Remote Input Workstation to verify user ID (Fingerprint logon). As requested, the system requires periodic changes to user passwords (ninety (90) day intervals).

Permission Table

The Permission Table in the Informix database is controlled by the State System Administrator and designated representative(s) to control individual workstation, workstation group, individual operator, and operator group transaction authority and/or default system performance. The following functions are assigned by the State System Administrator and designated representative(s) via the Permission Table:

- Workstation level security attributes;
- Workstation group level security attributes;
- Operator level security attributes;
- Operator classification security attributes; and
- Text Only or Text Plus Images match response default.

Security And Access Control Requirements

RFP OSI 2046
CURRENT SYSTEM

Restricting Access

SFIS provides a means of restricting access, so that access to the system's files and programs can be made available only to authorized persons and workstations.

RFP OSI 2046
CURRENT SYSTEM

SFIS ensures data security and integrity by using both physical and logical security features. All SFIS workstations and servers require a user name login ID and either password or fingerprint image to access SFIS. A password is used when a fingerprint scanner is not attached to a workstation. On the Remote Input Workstation this login ID causes a startup script to execute the SFIS logon screen on the workstation display. Where enabled by the administrator to do so, and where scanners are present (Client Input and Multi Function Workstation) the SFIS application requires a user name user ID and fingerprint match.

A system of security levels is used to determine access to the SFIS application functions. These security levels grant or restrict access to specified user functionality.

Each time a request is made to modify the security access for a workstation or a user, authorized personnel can modify certain fields in the SFIS security screen. Any change takes place immediately and is effective at the next logon.

The current Contractor only allows authorized personnel, who have signed confidentiality agreements to maintain data confidentiality, to handle reports and to obtain access to SFIS. Each SFIS workstation in the network is assigned an administrative password that is known only to the current Contractor and to State authorized staff. Access to the SFIS database requires another password. The database password is changed on a regular basis and is known only to the current Contractor and to the State staff authorized to work on the SFIS project.

Central Site servers also require the use of a user ID and password to access the operating system. Additional user IDs and passwords are required to access the database software or the matching subsystems.

Staff responsible for the routine operation of the system is not allowed to access SFIS system files. Only the operations staff assigned to the SFIS project are permitted access. Even then, assigned operations staff only access SFIS when responding to a documented request for assistance or when working on problem resolution. The current Contractor security system protects data against unauthorized modifications, disclosure, accidental erasure, theft, or destruction.

**RFP OSI 2046
CURRENT SYSTEM**

ACCESS LEVELS

SECURITY LEVEL A

Operator(s): Client Input Operator

Workstation(s): Client Input, Multifunction, and Portable Input Workstations

Functionality includes:

- File clearance access from Statewide Client Index (SCI) database (Client Input and Multifunction Only).
- Inquire (Photo line-up) function from the SFIS database (Client Input and Multifunction Only).
- Capture fingerprint and photo images.
- Enter a temporary fingerprint exemption.
- Add a client to the database.
- Update a client on the database.
- Submit Open and Closed Search requests.
- Upload transactions from zip disk (Client Input and Multifunction Only).
- Transmit portable transactions to central site for routing to designated remote site (Portable Input Only).
- Change own password.

SECURITY LEVEL B

Operator(s): Clerical Supervisor, Portable Input Operator

Workstation(s): Client Input and Multifunction Workstations

Functionality includes:

- All level A responsibilities.

RFP OSI 2046 CURRENT SYSTEM

- Allow capture of an alternate finger when missing fingers.
- Change priority of match requests generated by the site.
- Change own password.
- Reset disabled passwords.
- Enter resolution results.
- Authorize permanent client exemptions.

SECURITY LEVEL C

Operator(s): District Supervisor

Workstation(s): Client Input and Multifunction Workstations

Functionality includes:

- All level A and B responsibilities.
- Register new end users.
- Customize security options for levels A and B.
- Delete end users.
- Enable passwords rather than fingerprint logon.
- Reset passwords.
- Receive “floater” user ID from Help Desk.
- View queues relative to site.
- Print match responses relative to site.

SECURITY LEVEL D

Operator(s): Fraud Investigator

Workstation(s): Fraud Investigation and Multifunction Workstations

Functionality includes:

- View and confirm match results.

RFP OSI 2046 CURRENT SYSTEM

- Access Open Search Hit and Closed Search Miss queues.
- Submit Open and Closed Search requests of existing records.
- Request active file view (allows inquiry on clients not involved in responses placed on the Fraud Queue).
- Restore records previously in the Fraud Investigator queues.
- Generate specific reports.
- Print all search responses.
- Change own password.
- Update disposition code, fraud worker number and comments field.
- Allow access to the State Fraud Investigator at a statewide level.
- Allow access to the County Fraud Investigator at a countywide level.

SECURITY LEVEL E

Operator(s): County System Administrator.

Workstation(s): System Administration and Multifunction Workstations

Functionality includes:

- Create reports through Crystal Reports.
- Register new end users.
- Delete end users.
- Change own password.
- Enable passwords instead of fingerprint logon.
- Reset passwords.
- View queues and perform SFIS inquiries relative to county.

RFP OSI 2046
CURRENT SYSTEM

- Print match responses and reports relative to county.
- Receive “floater” user ID from Help Desk.
- Customize security levels.
- Perform resolution.

SECURITY LEVEL F

Operator: CDSS

Workstation: System Administration and Multifunction Workstations

Functionality includes:

- Create reports through Crystal Reports.
- Change own password.
- Generate CDSS reports.

SECURITY LEVEL G

Operator: State System Administrator

Workstation: System Administration, Program Management, and Multifunction Workstations

Functionality includes:

- All level E responsibilities.
- Create reports through Crystal Reports.
- Register and inactivate end users.
- Reset State passwords.
- View queues and perform SFIS inquiries for State.
- Print State Match Responses and reports.
- Receive floater user ID from Help Desk.
- Change parameters for State.
- Remove images.

RFP OSI 2046 CURRENT SYSTEM

- Update State Bulletin Board messages.

SECURITY LEVEL I

Operator: Verification Technician

Workstation: Verification and Multifunction Workstations

Functionality includes:

- Overturn Match and No Match error conditions.
- Confirm Match and No Match error conditions.

Security Standards

SFIS supports security standards established for access to the SCI database. The use of open architecture hardware, software and networking protocols including HP servers, PC workstations, UNIX, Windows NT, and TCP/IP enables SFIS to support the interface security with different platforms.

Audit Information

The current Contractor maintains and provides audit information pertinent to all SFIS transactions. Each transaction creates a row in the SFIS database log table for purposes of inquiry, reporting, and archiving. The log information includes the Client Index Number (CIN), the system transaction for the specific CIN, user ID, workstation ID, site, date and time of modification, and the information that was modified.

Contractor Certification

The current Contractor certified that SFIS is secure in that it meets the security requirements stated in the initial SFIS RFP.

SFIS is designed to provide security features to prevent unauthorized access to the system. The current Contractor has incorporated provisions that specify internal controls and necessary security features to provide the maximum assurance that the system allows only approved users and secured database administrator's access to SFIS.

RFP OSI 2046 CURRENT SYSTEM

The current Contractor ensures data integrity through the use of on-line and batch edits of transactions and data elements. The system enforces data security through the use of access levels, passwords, where applicable, and finger images, where applicable, by authorized SFIS users. These security features are assigned by the County and State System Administrator and apply to specific applications, screens, and data elements.

Password Protection

Each SFIS user is assigned a user name identification code (logon/operator id), a password, and an access level that is displayed on the Security screen. The access level controls the functions that the user can perform. Different levels of access exist for SFIS County users, Verification Technicians, and System Administrators. Logging on to the system at any access level requires that the user know their user ID. On workstations that require entry of password, the user will also need to know and correctly enter their password. On workstations with fingerprint scanners, such as the Remote Input Workstations, the finger image must match the image stored in the security table for that particular operator to complete the log in process. This secures SFIS from unauthorized access and prevents fraudulent use of the system. For a description of adding a user to SFIS, please refer to the System Administration Workstation User Guide.

Audit Trail and Reports

SFIS provides a security audit trail. This includes identification, tracking, and reporting of security exceptions cases to OSI management. Security information such as unsuccessful attempts to access the System are captured and reported to OSI management. Security reports are capable of being printed on demand.

The current Contractor provides detailed audit trails of every on-line and batch transaction processed by SFIS. The current Contractor uses operational programs to detect and store all unauthorized attempts to penetrate the AFIS, program, or file. Each transaction attempt is stored as a row in the SFIS database log table for reporting on demand. A user access tracking report details unauthorized access activity, including location, date, time, user ID, workstation ID, commands, and log-in/log-off time. Security reports are capable of being printed on demand.

RFP OSI 2046 CURRENT SYSTEM

Access Control Mechanisms

Every SFIS Remote Input Workstation user is assigned a user ID. When enabled by the System Administrator and when the scanner equipment is present, these workstation users may also use their finger image (at individual county option) to match against the image stored for their user ID. A match of the finger image is required to complete the logon process. All other workstation users such as those within the Central Site premises, are assigned a unique user ID and password by their supervisor.

The designated County or State coordinator approves the user ID. When the user receives approval and logs on to SFIS for the first time, the user enters their assigned user ID and assigned password. The new user is requested to change their password at this time.

Subsequently, each time a user logs on to SFIS they enter their unique user ID and password. SFIS verifies that the user's password matches to the stored password on the security database at the time of logon, and either allows or denies access to SFIS. If the password matches to the password stored in the security table for that operator, the SFIS Main Menu screen appears, and the user has successfully accessed SFIS.

The following controls are enforced regardless of location of the workstation:

- SFIS prompts each user to change his/her password periodically (Every ninety (90) days).
- SFIS limits the number of unsuccessful consecutive logon attempts. After a maximum of three (3) unsuccessful attempts, the user ID is locked out. Only another SFIS user with appropriate security access can unlock the user ID.
- The password field on the logon screen is populated with asterisks as the password is entered into the password field to prevent other persons in the room from obtaining the SFIS user's password.
- Each workstation and/or user is only able to access the SFIS network during State-specified office hours. A configuration table entry in the SFIS database records the proper working hours for each county and prevents access before or after the designated times. The table entry is available to be set by the State System Administrator.

RFP OSI 2046 CURRENT SYSTEM

- The entered password is first matched against the criterion required to create a password (The criterion is described in the sentences that follow). The editing occurs after the operator leaves the password field. An error message appears if the password does not meet the criterion. If the password meets the criterion, SFIS edits the password against other common use words that also meet the same criterion, such as required length of word. If the password completes both edits, the SFIS user is allowed to continue the password change process.
- Each operator is allowed to sign on to one (1) SFIS workstation at a time. The information related to an operator's sign-on is stored on the database table that is accessed prior to each sign-on. If the Operator ID is marked as "in use" on another workstation, an error message will be generated on the second workstation, disallowing connection to SFIS.
- SFIS stores the last five (5) passwords used by each operator on the security table in the relational database. The newly entered password is checked against the last five (5) passwords used. If the newly entered password is found in the table, an error message will result, prompting the operator to generate a password that has not been used in the past five (5) times.
- New passwords are edited to ensure that they are different by at least three (3) characters from the preceding passwords.
- SFIS requires passwords to be a minimum of seven (7) characters and contain alphabetic, numeric, or national characters.

Password File

Passwords are stored/maintained in the database in an encrypted file and are accessible only to the authorized current Contractor's systems engineers and State personnel. The systems engineers manipulate the fields only when responding to documented requests from the State to ensure system integrity and security.

PASSWORD TRANSMISSION

All passwords are transmitted in encrypted form and are not printed.

RFP OSI 2046 CURRENT SYSTEM

Root Access

Only authorized current Contractor staff that interact with the operation of SFIS and the State System Administrator are allowed "Super User" or "Root" access. This access is restricted to the system console. Remote Input Workstations do not have access to the server root access level.

System Reboot

If the Remote Input Workstation is temporarily disconnected from the Central Site or rebooted, the workstation comes up in a secured mode requesting that the operator complete the Windows NT logon process. Upon receiving the correct logon information, a script executes to begin the SFIS application by displaying the SFIS logon screen. SFIS prompts the user to complete the SFIS logon process. Any Central Site server or the system console that is rebooted also returns to the logon prompt upon completing the reboot cycle.

Default Passwords

The current Contractor certified that all default and installation passwords have been removed or changed, as appropriate, prior to placing the Remote Input Workstations into production.

RFP OSI 2046 CURRENT SYSTEM

Modem Access

SFIS provides dial-up access capability by modem for Portable Input Workstations. This capability has not been used since SFIS was implemented. However, if the capability should be used, the current Contractor provides a modem network with an additional layer of security. The current Contractor uses password security that protects SFIS data integrity and confidentiality. Before modem connection is established, the remote user is prompted for a password to verify authorized access to the network. Anti-spoofing software, which ensures the interface on which a packet enters the gateway corresponds to its IP address, also prevents the ability to gain unauthorized access. If the Central Site does not recognize the incoming IP address of the Portable Input Workstation, this workstation is not able to access SFIS. The SFIS logon screen appears after the modem dial-in password and the IP address of the Portable Input Workstation is verified. SFIS prompts the user for the user ID, password or their index finger image, as applicable. After the Central Site confirms the logon information, the user can proceed using SFIS. Currently, counties are not using modem access.

Changing Passwords

Passwords are changed every ninety (90) days. When the required change period has expired, following entry of the SFIS user ID and password, the change password screen appears. SFIS prompts the user to enter a new password and to reconfirm the new password. SFIS edits the new password to determine that it meets the criteria, as described above, for an SFIS password. If it passes all edits, the password is accepted and the operator is allowed to continue. If any of the edits has failed, the user is prompted to enter a different password.

User Privileges

State and County personnel designated to be responsible for SFIS security are assigned to the appropriate levels of access control. Only persons assigned to these access levels are able to alter the security level of lower level users, in addition to performing all functions allowed by any lower access level. SFIS users are prevented from increasing their own security privileges.

**RFP OSI 2046
CURRENT SYSTEM**

System Generated Reports

SFIS programs are used to detect and to store unauthorized access activity for the entire system. The unauthorized access activity information related to the entire system is stored in the Informix database. The stored information is used to generate the user access tracking report. This report is system-generated and the designated staff member authorized to monitor this activity is not able to delete or modify the audit/file report. The report details the violation, workstation ID, location, time, user ID, commands, and login/logoff time of the activity.

Automatic Workstation Log-Out

SFIS inactivates workstations by automatically logging them out after the system has not been used for fifteen (15) minutes.

Grant System Administrator Authority

SFIS has defined various categories of access authority. These categories are designed to provide the State System Administrator with the ability to grant access authority to County Coordinators for system administration functions

**RFP OSI 2046
CURRENT SYSTEM**

Remote Input Workstation Security

Operator Security

An operator's fingerprint images (all ten (10) fingers may be captured) may be captured and the System Administrator may enable the user for fingerprint logon. If captured, the fingerprint image data from all ten (10) fingers of a user are available for a local CLOSED SEARCH match associated with the log-on security function of the Remote Input Workstations that have scanners attached to them and that are connected to the network. In addition, on every workstation that a particular user is authorized to use, the user's system access permission level(s), ID, etc. is available to the workstation's security logic in order to limit the user's access to those functions, databases, etc. that have been authorized to that user by the State or County System Administrator. This information is not available to the workstation when the workstation cannot communicate with the Central Site.

LEADER INTERFACE

Introduction

To accommodate the LEADER requirements from Los Angeles County, changes were made to the SFIS Batch System and Online application. Also, bar code scanning was implemented.

The following table lists the components involved in SFIS LEADER processing.

Component name	Type	Description
notification_letter.pbl	PowerBuilder PBL	Create Notification Letters
leader_recon.pbl	PowerBuilder PBL	LEADER Reconciliation Process
sfisprint.pbl	PowerBuilder PBL	Print
caap1111.ec	C batch program	Update Notification Letter Data
caap4223.ec	C batch program	Create Notification List
caap4501.ec	C batch program	Ensures Consistent t101_csemst Data
caap4510.ec	C batch program	SFIS to LEADER Response
caap4515.ec	C batch program	LEADER to SFIS Add/Update

**RFP OSI 2046
CURRENT SYSTEM**

Component name	Type	Description
cdsi19.dat	Response file	File sent from SFIS to LEADER
cs4223w	Online report	Notification Notice Listing
in011b1moddhhmi.dat	LEADER file	File sent from LEADER to SFIS
tracking.exe	PowerBuilder executable	Tracking Application
t01_csemst	Table	Case Master
t02_csemin	Table	Case Minutiae
t09b_appt_list	Table	Notification List
t16_bknd_txn	Table	Transaction Log for Upload Process
t27_appsch	Table	Notification Schedule
t51_ssntbl	Table	Social Security
t45_cnty_conf	Table	County Configuration
t52_lintbl	Table	Local Identification Number
t101_csemst	Table	County Specific
t999_appt_ltr	Table	Notification Letter
w_print_main	Window	Print

Batch System

The batch system performs the following functions to accommodate LEADER:

- An interface that receives adds and updates from LEADER to SFIS, and sends fingerprint responses from SFIS to LEADER.
- A notification subsystem. (The operation of this subsystem is currently (03/03/2006) suspended.)
- A notification tracking application.
- A reconciliation process assures concurrency between SFIS and LEADER client status.

RFP OSI 2046 CURRENT SYSTEM

Interface

The LEADER interface to SFIS consists of several C Language daily batch programs, which perform the LEADER to SFIS add/update and send a response file back to LEADER. The file sent from LEADER includes demographic and benefit information, along with information used to determine which clients should be notified of the need for fingerprinting. SFIS sends the Match Responses back to LEADER.

NOTIFICATION (The operation of this subsystem is currently (03/03/2006) suspended.)

To facilitate the fingerprinting of applicants, the Notification subsystem creates notification letters, and a Notification Listing for each Los Angeles County site. The notification letters are printed at EDS' facility in Monrovia, CA and are sent next day express to the Los Angeles County Office of Information Technology, who then forwards them to a County mailing facility where they are put into envelopes and sent to clients.

NOTIFICATION TRACKING

Run daily, the application determines all workstations that are both inoperative and located within Los Angeles County. Once a site is determined to be a down site, it tracks every applicant that has not been fingerprinted for that site that is scheduled for today (today meaning the current system date when Notification Tracking is executed), to the following weekday. This is a change to tables only and does not affect applicants. No notification letters are generated that day for those applicants that were scheduled for down sites.

RECONCILIATION PROCESS

The reconciliation process assures the client information related to the program status applied for is synchronized with LEADER information.

Online System

The online version of SFIS in use by Los Angeles County has the following functionality that differs from the SFIS version in use by all other California Counties:

RFP OSI 2046
CURRENT SYSTEM

- Reschedule checkbox appears on the Add/Update screen.
- File Clearance is disabled.
- A Los Angeles County only tab appears on the Print screen.

Bar Code Scanners

To facilitate the entry of data fields from the LEADER Client Fingerprinting Required form, bar code scanners can be attached to the Client Input Workstations. Once the Add/Update screen is displayed, the Operator can scan the CIN. When the CIN has been decoded, and demographic information is displayed on the screen, the Operator may also scan the LIN, SSN, and DOB if needed. Before using the scanner for the first time, it must be programmed by scanning the set of startup barcodes in the required order.

**RFP OSI 2046
CURRENT SYSTEM**

D. COUNTY ENVIRONMENT

COUNTY OFFICE EQUIPMENT

County office equipment includes PC workstations, fingerprint scanners, cameras, and laser printers. Only Multifunction, Client Input, and Portable Input Workstations have the entire complement of hardware. Fraud Investigation Workstations have no fingerprint scanners or cameras. Selected System Administration Workstations have fingerprint scanners to support logon by fingerprint. (The exact same application is loaded on every remotely located workstation.) In addition to the workstation hardware and associated peripheral equipment, each location has networking equipment consisting of the following:

- Cisco router.
- CSU/DSU or DSL card.
- Ethernet hub, enabling online access to the SFIS application and data.

SFIS workstation and system availability are monitored by the current Contractor and are reported monthly. Availability is measured on a twelve (12) hour workday from 7 a.m. to 7 p.m.

Currently, there are a total of two hundred and sixty-eight (268) workstations located in counties with the Client Input Workstation (CIW) and Multifunction Workstation (Multi) capability, twenty-nine (29) Fraud Investigation Workstations (FIW), twenty-one (21) System Administration Workstations (SAW) and thirty-two (32) Portable Input Workstations (PIW). There are seventeen (17) additional Multifunction Workstations allocated for SFIS training. The Monrovia, California training center operated by the current Contractor uses seven (7) Multifunction Workstations and the Sacramento, California center operated by OSI utilizes ten Multifunction Workstations.

The Remote Input Workstations (Workstations used for capturing client finger images: CIW, Multi, and Port.) are capable of storing up to one thousand (1K) transactions on the workstation's local-disk drives. Locally, transactions are stored when the workstation is unable to communicate with the Central Site, and typically results from a network failure. Storing transactions on the local disk drive is the normal mode of operation for all Portable Input Workstations. Additionally, the design of the Remote Input Workstation brings up-front processing to the county sites. Up-front processing includes quality verification that finger images captured at the workstation are of adequate quality for matching. The workstation also locally edits all demographic data, extracts finger image minutiae points, performs closed matching, and performs data compression.

RFP OSI 2046
CURRENT SYSTEM

PC workstations are used for the following SFIS related functions (Please refer to the SFIS User Guides for a comprehensive explanation of each workstation's functionality. The exact same application is loaded on every remotely located workstation.):

- Client Input Workstation (Remote Input)
 - Capture and transmit client fingerprint images, photos, and demographic data with the Add/Update function.
 - Conduct File Clearance to obtain the client's CIN.
 - Conduct File Inquire to ascertain if a client is currently in the SFIS database.
 - Assign codes to resolutions in order to explain unexpected results (Closed Search No Match or Open Search Match) or refer them to the fraud investigator.
 - Print out match responses and reports.
 - Operate scanner diagnostics.
- Fraud Investigation Workstation
 - View unexpected results that are potential fraud cases on the Fraud Review screen.
 - Log research conclusions on the Fraud Review screen.
 - Relaunch fingerprint images in the database in order to see if different matching results may be found.
 - Conduct a Two CIN Search function to compare fingerprints associated with two (2) different CINS.
 - Inquire to ascertain if a client is currently in the SFIS database.
- System Administration Workstation
 - Establish operator IDs, reset passwords, unlock operator IDs, capture operator finger images (at county option), enable password or finger logon using the security function.
 - Print reports using the print function and to create ad hoc reports using Crystal Reports.
 - Modify print out preferences using the preference function, and modify match response priority using the queues function.
 - Operate scanner diagnostics.
- Multifunction Workstation (Remote Input)
 - Used when all end users must use the same workstation: System Administrators, Client Input Operators, and Fraud Investigators.

RFP OSI 2046
CURRENT SYSTEM

- Portable Input Workstations (Remote Input)
 - Collect client fingerprint images and photos (using the Add/Update function) on a notebook workstation at a temporary location that does not have network access (such as a home visit or a hospital).
 - Transfer the client files to a zip disk or via dial-up for processing.
 - Operate scanner diagnostics.

**RFP OSI 2046
CURRENT SYSTEM**

E. GENERAL COUNTY & CENTRAL SITE HARDWARE DESCRIPTION

Remote Workstation hardware currently used by the SFIS project is documented in the table below. The first column of the table describes each component of the hardware. The second column describes the attributes and model numbers being used in the project.

Workstation Type	Description	Model, Size, Feature
Remote Input, Fraud Investigation, System Administration and Verification	PC	Gateway E-4200
	Pentium II Processor	Four hundred and fifty megahertz (450MHz) single processor unit
	ZIP Drive	All PC's have a ZIP Drive. Available for use on all machines except for FIW
	Diskette Drive	All PC's have 1.44 MB Floppy.
	CD-ROM	All PC's have 17x – 40x max.
Remote Input, Fraud Investigation, System Administration and Verification	PC Peripherals	
	Color Monitor	All PC's have nineteen (19) inch. Counties may request seventeen (17).
	Notebook PC	Gateway Solo Pro 9300
Portable Input Workstation	Pentium II Processor	Six hundred and fifty megahertz (650MHz) single processor unit

**RFP OSI 2046
CURRENT SYSTEM**

Workstation Type	Description	Model, Size, Feature
	Notebook Peripherals	
Portable Input Workstation	Color Monitor	Fifteen (15) inch XGA Display
Portable Input Workstation	Docking Station	Gateway Solo MD-3 Docking Station
Process Coordinators, System Console and Test Process Console	PC	HP Visualize B1000
	PA-8500 Processor	Three hundred megahertz (300MHz) single processor unit
	RAM	Five hundred and twelve megabytes (512MB)
	Internal Disk (Fiber Channel Bus)	Nine gigabytes (9GB)
	DAT Tape Drive	Four millimeter (4mm) DDS-3
	CD-ROM	32x ATAPI
	Communications Device	10/100 Mbps Ethernet
	Operating System	HP-UX 10.20
All Workstations except the Portable Workstation	Workstation Peripherals	
	Color Monitor	Nineteen (19) inch viewable Hitachi
	Keyboard	PS/2
	Mouse	PS/2

**RFP OSI 2046
CURRENT SYSTEM**

Workstation Type	Description	Model, Size, Feature
All Remote Input Workstations	Fingerprint Scanner	Identix Touchview II TV-555
	Resolution	Five hundred dots per inch (500dpi), two hundred and fifty-six (256) levels of gray-scale
All Remote Input Workstations	Frame Grabber	Integral Technologies: Flashpoint BUS MV Lite (Portable), MVI Lite
	Bus	PCI 2.1
	Video Capture	Twenty-four (24) bit color, eight (8) bit gray scale
	MDRAM	Eight megabytes (8MB)
All Remote Input Workstations	Photographic Camera	Howard Enterprises NCK41CV
	Picture Elements	Seven hundred and sixty-eight height (768 H) x four hundred and ninety-four vertical (494 V)
	Minimum Object Distance Lens	Three hundred millimeter (300 mm)
All workstations except the Portable	Printer	HPLaserJet 2100 xi Parallel Printer cable available in six (6) and twenty (20) feet
	Print Speed	Ten pages per minute (10ppm)

**RFP OSI 2046
CURRENT SYSTEM**

Workstation Type	Description	Model, Size, Feature
Client Input and Multifunction Workstations (Los Angeles County Only)	Bar Code Scanner	Symbol Technologies LT-1806
	Scanner Type	Bi-directional, retrocollective
	Scan Rate	36 +/- 3 scans per second
	Separate Components	
All Remote Input Workstations	Light	Single halogen fixture
All Remote Input Workstations	Light Control Switch	Manual switch
Client Input and Multifunction Workstation	Stationary Backdrop	Eighteen percent (18%) Grey. Four feet by four feet (4' x 4')
Portable Input Workstation	Foldable Backdrop	Eighteen percent (18%) Grey. Opens from three feet by two feet (3' x 2') to three feet by four feet (3' x 4')
Portable Input Workstation	Portable Easel	Adapts from thirty-four inches (34") to fifty-four inches (54") high
Client Input Workstation	Stationary Easel	Seven feet six inches (7' 6") tall.
Portable Input Workstation	Portable Zip Disk Drive	Iomega Z100P2
Portable Input Workstation	Zip disk	Any brand
All Remote Input Workstations	All cables	Scanner power pack and coax cable. Camera power pack and s-video cable. Six feet (6') extension cord.

**RFP OSI 2046
CURRENT SYSTEM**

Workstation Type	Description	Model, Size, Feature
Portable Input Workstation	All cables	All Remote Input Workstation cables. Portable zip disk drive power pack and connector cable.
	<i>Installation Equipment</i>	
All Workstations	Security Cables Padlocks	Generic forty millimeter (40mm)
All Workstations	Power Strip	Belkin SurgeMasterII
Portable Input Workstation	Extension Cord	Nine feet (9') heavy duty

**RFP OSI 2046
CURRENT SYSTEM**

WORKSTATION MAINTENANCE AND REPAIR

The current Contractor has an agreement with a subcontractor for workstation and printer maintenance and repair with the exception of Los Angeles County. The current Contractor performs all maintenance and repair actions for Los Angeles County sites. The maintenance approach is on-site replacement in lieu of on-site repair. The current Contractor pre-configures workstations that are used to replace failed units. Internal component replacement is avoided within the PC systems unit, but external components such as the fingerprint scanner, the camera, and the monitor are individually replaced. Please refer to the Maintenance section of this document for a comprehensive explanation of the SFIS Project's workstation maintenance.

Workstation Operating System

The SFIS workstations described in the paragraphs above support an industry standard operating system, and commercial off-the-shelf (COTS) application software packages. All workstations use the Windows NT operating system.

County & Central Site Software

The SFIS workstation software includes the following:

Workstation Type	Software
Remote Input, Fraud Investigation, Verification, and System Administration	Microsoft WindowsNT version 4.0/SP5
Remote Input, Fraud Investigation, Verification, and System Administration	Computer Associates Control IT Workstation Remote Control Option version 4.5.
Remote Input, Fraud Investigation, Verification, and System Administration	Computer Associates eTrust Virus Protection Software version 6.0
Remote Input, Fraud Investigation, Verification, and System Administration	Computer Associates Unicenter Software Delivery Option version 3.1
Remote Input, Fraud Investigation, Verification, and System Administration	Computer Associates Unicenter TNG Network Management Option version 2.4
Remote Input, Fraud Investigation, Verification, and System Administration	Flashbus Imaging Software version 3.7

**RFP OSI 2046
CURRENT SYSTEM**

Workstation Type	Software
Remote Input, Fraud Investigation, Verification, and System Administration	LEADTOOLS Document Imaging Software version 10.10
Remote Input, Fraud Investigation, Verification, and System Administration	Motorola/Printrak Application Software Components version 1.01.0002
System Administration	Seagate Crystal Reports version 7.0
Remote Input, Fraud Investigation, Verification, and System Administration	Sybase SQL Anywhere version 5.0

Deleted: Printrak

County LAN Environment

Each Client Input, Multifunction, Fraud Investigation, and System Administration Workstation is connected to the DTS Wide Area Network (WAN) through Local Area Networks (LAN). The DTS WAN is connected to LANs at each site where a Remote Workstation is located. The type of LAN used at each county site is Ethernet. It is the current Contractor's responsibility to configure each Remote Workstation with the hardware and software necessary to connect the workstation to the LAN at each installation site.

The SFIS workstations described in the paragraphs above are on dedicated LANs in County sites. Residence on dedicated LANs protect SFIS from networking problems. SFIS workstations are connected to ten megabit (10mb) ports on either an ATI or 3COM Ethernet hub. The hub is connected to the DTS Cisco router via CATV cable. The router uses a CSU/DSU to connect to the State's Frame cloud, and an ATM ADSL card that connects to local Central Office (CO) for the ADSL sites.

The current Contractor uses CA Unicenter TNG to monitor connectivity and availability of the SFIS routers, hubs, and workstations. Unicenter is constantly pinging or checking the equipment for connectivity. Unicenter signals alerts when any of the monitored equipment is found to be unreachable.

**RFP OSI 2046
CURRENT SYSTEM**

Image Transmission

Remote Input Workstations send all data for the record including the (compressed) fingerprint images to the Central Site over the network. Each Remote Input Workstation includes software for analysis of fingerprint images, production of minutiae data for each fingerprint image used for any type of fingerprint matching, and compression of fingerprint image data via an FBI-approved WSQ compression algorithm. The analysis of the quality of each fingerprint image and production of minutiae data is accomplished through the use of the [Motorola/Printrak](#) Advanced Fingerprint Processor (AFP) software. The Remote Input Workstation sends all data for the record including the (compressed) fingerprint images to the Central Site over the network.

Deleted: Printrak

Download Demographic Data

The SFIS Remote Input Workstations have the capability to accept a download of demographic data from the SCI interface. This demographic update function provides the ability to change or to update the demographic data of any record within the SFIS database. This operation is initiated by a transaction from SFIS that includes the Client Index Number (CIN), which is the unique number used to identify clients from the Department of Health Services. SCI sends the current demographic data to the SFIS Central Site for update on the SFIS database and displays on the operator screen (Add/Update).

Workstation Printer

All (except the Portable Input) of the SFIS workstations described above have one (1) high-resolution printer that is directly attached to the workstation. The workstation printer is capable of generating a printout of any image (fingerprint and/or photo) displayed on a workstation screen. Printouts are automatically sent to the local printer associated with the workstation (Unless the Printout Preference is changed to Manual Print by the County or State System Administrator). Printouts of fingerprint images are 'full binary' images (full resolution images with the gray level of each pixel converted to white or black) with an 'along-scan' and 'cross-scan' direction resolution of five hundred (500) pixels/inch, plus or minus five (5) pixels per inch. Fingerprint images are printed with a physical size of at least ten (10) times the original size. Printouts of photo images are in gray scale in sufficient resolution so that an operator can determine if two (2) photo images printed side-by-side are or are not from the same individual.

**RFP OSI 2046
CURRENT SYSTEM**

PHYSICAL CHARACTERISTICS

UL Compliant

The SFIS workstations are industry standard workstation configurations and are ergonomically designed and in compliance with UL (Underwriters Laboratory) standards for operator safety.

FCC Class B Compliant

The workstation peripheral components are FCC Class B certified. The following table presents the peripheral and the FCC Certification Number for each workstation component.

<u>Peripheral Component</u>	<u>FCC Certification Number</u>
Identix Touchview II Fingerprint Scanner	108503-206
Integral Frame Grabber	EN55022
Howard Enterprises Photo Camera	CISPR 22
HP 2100 Laserjet	A3L ML85
Symbol Technologies LT-1806 Bar Code Scanner (Los Angeles County Only)	EN60950

**RFP OSI 2046
CURRENT SYSTEM**

CURRENT (as of 12/01/2004) COUNTY WORKSTATION LOCATION DETAILS

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Alameda	01	02	4501 Broadway	Oakland	94612	C01021
Alameda	01	03	6955 Foothill Blvd.	Oakland	94605	C01031
Alameda	01	03	6955 Foothill Blvd.	Oakland	94605	C01033
Alameda	01	04	8477 Enterprise Way	Oakland	94621	C01041
Alameda	01	06	24100 Amador Street	Hayward	94544	C01061
Alameda	01	07	39155 Liberty	Fremont	94538	C01071
Alameda	01	08	3311 Pacific Avenue	Livermore	94550	C01081
Contra Costa	07	01	4545 Delta Fair	Antioch	94509	C07011
Contra Costa	07	03	40 Muir Road	Martinez	94553	C07031
Contra Costa	07	04	151 Linus Pauling	Hercules	94547	C07041
Contra Costa	07	05	1305 MacDonald	Richmond	94801	C07051
Contra Costa	07	09	1275A Hall Street	Richmond	94804	C07091
El Dorado	09	01	3057 Briw Road (SFIS Coord.)	Placerville	95667	C09011
Fresno	10	01	4468 E. Kings Canyon Road	Fresno	93702	C10011
Fresno	10	02	4455 E. Kings Canyon Road (SFIS Coord.)	Fresno	93702	C10021

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Fresno	10	04	311 Coalinga Plaza	Colinga	93210	C10041
Fresno	10	06	2314 Mariposa Street	Fresno	93702	C10061
Fresno	10	09	3800 McCall Avenue	Selma	93662	C10091
Fresno	10	11	2025 E. Dakota	Fresno	93727	C10111
Fresno	10	12	3151 N. Millbrook Avenue	Fresno	93726	C10121
Fresno	10	13	1680 Manning Avenue	Reedley	93654	C10131
Fresno	10	14	15180 West Whitesbridge Ave.	Fresno	93726	C10141
Glenn	11	02	604 East Walker Street, Suite A	Orland	95963	C11021
Humboldt	12	01	929 Koster (SFIS Coord.)	Eureka	95501	C12011
Humboldt	12	03	727 Cedar Street	Garberville	95542	C12032
Humboldt	12	04	1200 Airport Road (K'Ima:w Medical Clinic)	Hoopa	95546	C12042
Inyo	14	01	380 North MT. Whitney Drive	Lone Pine	93545	C14011
Inyo	14	05	Tacopa Hot Springs Road	Tacopa Hot Springs	92389	C14051
Kern	15	01	100 E. California Avenue (SFIS Coord.)	Bakersfield	93302	C15012
Kern	15	01	100 E. California Avenue (SFIS Coord.)	Bakersfield	93302	C15013
Kern	15	02	7050 Lake Isabella Blvd.	Lake Isabella	93240	C15021

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Kern	15	03	1816 Cecil Avenue	Delano	93215	C15031
Kern	15	04	10215 Stobaugh St.	Lamont	93241	C15041
Kern	15	05	2340 Hwy 58	Mojave	93501	C15051
Kern	15	06	1400 N. Norma	Ridgecrest	93555	C15061
Kern	15	07	115 Central Valley Hwy	Shafter	93263	C15071
Kern	15	08	1830 Flower Street	Bakersfield	93305	C15081
Kern	15	09	315 Lincoln	Taft	93268	C15091
Kings	16	02	951 Chitenden	Corcoran	93212	C16021
Lassen	18	02	2545 Main Street	Susanville	96130	C18021
Los Angeles	19	01	4680 San Fernando Road	Glendale		C19011
Los Angeles	19	01	4680 San Fernando Road	Glendale		C19012
Los Angeles	19	02	955 N. Lake Avenue	Pasadena	91104	C19021
Los Angeles	19	03	3350 Aerojet Avenue (El Monte)	El Monte	91731	C19031
Los Angeles	19	04	5445 Whittier Blvd.	Los Angeles	90022	C19041
Los Angeles	19	05	8130 S. Atlantic	Cudahy	90201	C19051
Los Angeles	19	06	11390 W. Olympic	Los Angeles	90064	C19061

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Los Angeles	19	07	14545 Lanark Street	Panorama City	91402	C19071
Los Angeles	19	08	3833 South Vermont Avenue	Los Angeles	90037	C19081
Los Angeles	19	09	2615 S. Grand Avenue	Los Angeles	90007	C19091
Los Angeles	19	10	2855 E. Olympic	Los Angeles	90023	C19101
Los Angeles	19	10	2855 E. Olympic	Los Angeles	90023	C19102
Los Angeles	19	11	1740 E. Gage Avenue	Los Angeles	90001	C19111
Los Angeles	19	12	3350 Aerojet Avenue (San Gabriel)	El Monte	91731	C19121
Los Angeles	19	12	3350 Aerojet Avenue (San Gabriel)	El Monte	91731	C19122
Los Angeles	19	13	211 E. Alondra	Compton	90220	C19131
Los Angeles	19	14	10728 S. Central	Los Angeles	90059	C19141
Los Angeles	19	15	17600-A Santa Fe Avenue	Rancho Dominguez	90221	C19151
Los Angeles	19	16	349-B East Avenue K-6	Lancaster	93535	C19161
Los Angeles	19	16	349-B East Avenue K-6	Lancaster	93535	C19162
Los Angeles	19	17	2040 W. Holt Avenue	Ponoma	91768	C19171
Los Angeles	19	17	2040 W. Holt Avenue	Ponoma	91768	C19172
Los Angeles	19	18	2601 Wilshire Avenue	Los Angeles	90057	C19181

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Los Angeles	19	19	12727 Norwalk Blvd.	Norwalk	90650	C19191
Los Angeles	19	20	27233 Camp Plenty Road	Canyon Country	91351	C19201
Los Angeles	19	22	2961 Victoria Street	Rancho Dominguez	90221	C19221
Los Angeles	19	23	4077 N. Mission Road	Los Angeles	90032	C19231
Los Angeles	19	24	21415 Plummer Street	Chatsworth	91311	C19241
Los Angeles	19	25	923 E. Redondo	Inglewood	90302	C19251
Los Angeles	19	26	17600-B Santa Fe Avenue	Rancho Dominguez	90221	C19261
Los Angeles	19	26	17600-B Santa Fe Avenue	Rancho Dominguez	90221	C19262
Los Angeles	19	26	17600-B Santa Fe Avenue	Rancho Dominguez	90221	C19263
Los Angeles	19	27	1819 W. 120th. St.	Los Angeles	90044	C19271
Los Angeles	19	27	1819 W. 120th. St.	Los Angeles	90044	C19272
Los Angeles	19	28	2415 W 6th Street	Los Angeles	90057	C19281
Los Angeles	19	28	2415 W 6th Street	Los Angeles	90057	C19282
Los Angeles	19	29	813 E. Fourth Place	Los Angeles	90013	C19291
Los Angeles	19	29	813 E. Fourth Place	Los Angeles	90013	C19292
Los Angeles	19	30	12847 Arroyo Street	Sylmar	91342	C19301

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Los Angeles	19	31	11110 W. Pico Blvd.	Los Angeles	90064	C19311
Los Angeles	19	31	11110 W. Pico Blvd.	Los Angeles	90064	C19312
Los Angeles	19	32	2707 S. Grand Avenue	Los Angeles	90007	C19321
Los Angeles	19	32	2707 S. Grand Avenue	Los Angeles	90007	C19322
Madera	20	01	720 E. Yosemite Avenue (SFIS Coord.)	Madera	93639	C20011
Madera	20	02	41969 Hwy 41	Oakhurst	93644	C20021
Madera	20	03	327 Trinity Avenue	Chowchilla	93610	C20031
Marin	21	01	120 Redwood Way	San Rafael	94903	C21011
Marin	21	03	100 6th Street	Point Reyes Station	94956	C21031
Merced	24	01	2115 West Wardrobe Avenue	Merced	95340	C24011
Merced	24	03	415 F Street	Los Banos	93635	C24031
Merced	24	05	1471 B Street, Suite F, G, and H	Livingston	95334	C24051
Monterey	27	01	1000 South Main (SFIS Coord.)	Salinas	93901	C27011
Monterey	27	02	116 Broadway	King City	93930	C27021
Monterey	27	03	1281 Broadway	Seaside	93955	C27031
Napa	28	02	650 Imperial Way	Napa	94559	C28021

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Nevada	29	01	10075 Levone, Suite 204	Truckee	95731	C29011
Orange	30	02	2020 West Walnut	Santa Ana	92703	C30021
Orange	30	03	1928 S. Grand, Bldg. A	Santa Ana	92705	C30031
Orange	30	04	1928 South Grand, Bldg. C	Santa Ana	92705	C30042
Orange	30	04	1928 South Grand, Bldg. C	Santa Ana	92705	C30043
Orange	30	05	25292 McIntyre Road, Suite K	Laguna Hills	92653	C30051
Orange	30	06	3320 East La Palma Avenue	Anaheim	92806	C30062
Orange	30	06	3320 East La Palma Avenue	Anaheim	92806	C30063
Orange	30	07	12912 Brookhurst	Garden Grove	92842	C30072
Orange	30	09	6100 Chip Avenue	Cypress	90630	C30091
Orange	30	10	23330 Moulton Parkway	Laguna Hills	92653	C30101
Placer	31	02	100 Stonehouse Court, Suite A	Roseville	95678	C31021
Placer	31	04	5225 North Lake Blvd.	Carnelian Bay	96140	C31041
Riverside	33	03	4260 Tequesquite Avenue	Riverside	92501-4064	C33032
Riverside	33	05	451 N. San Jacinto Street	Hemet	92543	C33051
Riverside	33	06	23119 Cottonwood Avenue, Bldg. C	Moreno Valley	92553	C33061

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Riverside	33	07	575 Chaney Street	Lake Elsinore	92530-3796	C33071
Riverside	33	08	63 So 4th Street	Banning	92220	C33081
Riverside	33	09	2055 N. Perris Blvd. B	Perris	92571-2542	C33091
Riverside	33	10	44-199 Monroe Street, Suite D	Indio	92201	C33101
Riverside	33	11	1225 W. Hobson Way	Blythe	92225	C33111
Riverside	33	12	43264 Business Park Drive	Temecula	92591-6032	C33121
Riverside	33	13	68615-A Perez Road, #9	Cathedral City	92234-7200	C33131
Riverside	33	14	11060 Magnolia	Riverside	92503	C33141
Sacramento	34	01	1725 28th Street (SFIS Coord. @ 3737 Marconi Ave.)*	Sacramento	95816	C34011
Sacramento	34	02	3960 Research Drive	Sacramento	95838	C34021
Sacramento	34	03	2700 Fulton Avenue	Sacramento	95821	C34031
Sacramento	34	04	10013 Folsom Blvd.	Rancho Cordova	95827	C34041
Sacramento	34	05	257 South Lincoln Way	Galt	95632	C34051
Sacramento	34	06	9136 Elk Grove Blvd.	Elk Grove	95624	C34061
Sacramento	34	07	2450 Florin Road	Sacramento	95822	C34071
Sacramento	34	08	5747 Watt Avenue	North Highlands	95660	C34081

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Sacramento	34	09	9727 Auburn Blvd.	Citrus Heights	95610	C34091
Sacramento	34	10	4433 Florin Road	Sacramento	95823	C34101
San Bernardino	36	01	494 North E Street	San Bernardino	92415	C36011
San Bernardino	36	02	2050 North Massachusetts	San Bernardino	92415	C36021
San Bernardino	36	03	56357 Pima Trail	Yucca Valley	92284	C36031
San Bernardino	36	04	881 West Redlands Blvd.	Redlands	92373	C36041
San Bernardino	36	06	1300 East Mt. View	Barstow	92311	C36061
San Bernardino	36	08	9655 9th Avenue	Hesperia	92392	C36081
San Bernardino	36	09	7977 Sierra Avenue	Fontana	92335	C36092
San Bernardino	36	10	1300 Bailey Street	Needles	92363	C36101
San Bernardino	36	15	1627 East Holt Boulevard	Ontario	91764	C36151
San Bernardino	36	18	12219 Second Avenue	Victorville	92392	C36181
San Bernardino	36	19	2040 West Woodpine Avenue	Colton	92324	C36191
San Bernardino	36	25	10825 Arrow Route	Rancho Cucamonga	91730	C36251
San Bernardino	36	27	16534 Victor Street	Victorville	92392	C36271
San Bernardino	36	28	1585 Highlands Avenue	Highlands	92404	C36281

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
San Bernardino	36	29	73629 Sun Valley Drive	29 Palms	92277	C36291
San Bernardino	36	30	10875 Rancho Road	Adelanto	92301	C36301
San Diego	37	01	220 South First Street	El Cajon	92019-4701	C37011
San Diego	37	02	620 E. Valley Parkway	Escondido	92025	C37021
San Diego	37	04	5201 Ruffin Road, Suite K	San Diego	92123	C37041
San Diego	37	05	7065 Broadway	Lemon Grove	91945	C37051
San Diego	37	06	1255 Imperial Avenue	San Diego	92101	C37061
San Diego	37	07	1130 10th Avenue	San Diego	92101	C37071
San Diego	37	08	7947 Mission Center Court	San Diego	92108	C37081
San Diego	37	09	5001 73rd Street	San Diego	92115	C37091
San Diego	37	10	1315 Union Plaza Court	Oceanside	92054	C37101
San Diego	37	11	690 Oxford Street, Suite E	Chula Vista	919111	C37111
San Diego	37	12	4588 Market Street	San Diego	92102	C37121
San Diego	37	16	1521 Main Street	Ramona	92065	C37161
San Diego	37	17	1030 S. Main	Fallbrook	92028	C37171
San Francisco	38	01	170 Otis Street (SFIS Coord.)	San Francisco	94120	C38012

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
San Francisco	38	01	170 Otis Street (SFIS Coord.)	San Francisco	94120	C38013
San Francisco	38	02	1235 Mission	San Francisco	94103	C38021
San Francisco	38	02	1235 Mission	San Francisco	94103	C38022
San Francisco	38	02	1235 Mission	San Francisco	94103	C38023
San Francisco	38	04	1440 Harrison	San Francisco	94103	C38041
San Francisco	38	06	3120 Mission Street	San Francisco	94110	C38061
San Joaquin	39	01	333 East Washington Street (SFIS Coord.)	Stockton	95202	C39011
San Joaquin	39	01	333 East Washington Street (SFIS Coord.)	Stockton	95202	C39013
San Luis Obispo	40	01	9415 El Camino Real	Atascadero	93422	C40011
San Luis Obispo	40	02	1086 Grand Avenue	Arroyo Grande	93420	C40021
San Luis Obispo	40	06	530 12th Street.	Paso Robles	93446	C40061
San Luis Obispo	40	07	671 W. Tefft Street, Suite 1	Nipomo	93444	C40071
San Luis Obispo	40	08	1130 Napa Street, Suite D & G	Morro Bay	93442	C40081
San Mateo	41	01	2415 University Avenue	East Palo Alto	94303	C41011
San Mateo	41	02	1487 Huntington Avenue	So. San Francisco	94080	C41021
San Mateo	41	03	2500 Middlefield Road	Redwood	94063	C41031

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
San Mateo	41	04	271 92nd Street	Daly City	94015	C41041
San Mateo	41	06	550 Quarry Road	San Carlos	94070	C41061
San Mateo	41	08	350 90th Street	Daly City	94015	C41081
Santa Barbara	42	01	1100 W. Laurel Avenue	Lompoc	93436	C42011
Santa Barbara	42	05	234 Camino Del Remedio (SFIS Coord.)	Santa Barbara	93110-1369	C42051
Santa Barbara	42	06	2125 S. Centerpointe Ply.	Santa Maria	93455-1338	C42061
Santa Barbara	42	07	1410 So. Broadway	Santa Maria	93454	C42071
Santa Barbara	42	09	1133 North H Street, Suite E	Lompoc	93436	C42091
Santa Clara	43	01	1919 Senter Road	San Jose	95112	C43011
Santa Clara	43	01	1919 Senter Road	San Jose	95112	C43021
Santa Clara	43	03	591 North King Road	San Jose	95133	C43031
Santa Clara	43	04	100 Moffett Blvd.	Mountain View	94043-1424	C43041
Santa Clara	43	05	190 Leavesley Road	Gilroy	95020-3635	C43051
Santa Clara	43	08	1670 Las Plumas, Suite H	San Jose	95133-1670	C43081
Santa Cruz	44	01	119 W. Beach Street	Watsonville	95076	C44011
Santa Cruz	44	02	1020 Emeline Street	Santa Cruz	95060	C44021

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Shasta	45	01	36911 Main Street	Burney	96013	C45011
Shasta	45	02	2460 Breslauer Way (SFIS Coord.)	Redding	96001	C45021
Shasta	45	03	1400 California Street	Redding	96049-6005	C45031
Siskiyou	47	02	293 A Main Street	Weed	96064	C47021
Solano	48	02	1680 Fairgrounds Drive	Vallejo	94590	C48021
Solano	48	04	354 Parker Street	Vacaville	95688	C48041
Sonoma	49	01	2550 Paulin Drive	Santa Rosa	95402	C49011
Stanislaus	50	01	251 East Hackett Road (SFIS Coord.)	Modesto	95353	C50011
Stanislaus	50	01	251 East Hackett Road (SFIS Coord.)	Modesto	95353	C50012
Stanislaus	50	03	101 Lander Avenue	Turlock	95380	C50031
Tehama	52	03	703 4 th Street	Corning	96021	C52031
Tulare	54	01	100 E. Center Street	Visalia	93279	C54011
Tulare	54	02	75 West Olive	Porterville	93258	C54021
Tulare	54	03	900 N. Sequoia	Lindsay	93247	C54031
Tulare	54	05	1066 N. Alta Avenue	Dinuba	93618	C54051
Ventura	56	02	725 Main Street, Suite 300	Santa Paula	93060	C56021

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Ventura	56	03	4651 Telephone Road, Suite 100	Ventura	93003	C56031
Ventura	56	04	2003 Royal Avenue	Simi Valley	93065	C56041
Ventura	56	05	1400 Vanguard Drive, 1st Floor	Oxnard	93033	C56052
Yolo	57	01	500 Jefferson Blvd.	West Sacramento	95605	C57012
Yolo	57	02	25 N Cottonwood Street	Woodland	95695	C57021
Yuba	58	02	1114 Yuba Street	Marysville	95901	C58021
Total Client Input Workstations						214
Alameda	01	03	6955 Foothill Blvd.	Oakland	94605	F01032
Butte	04	02	2445 Carmichael Drive	Chico	95928	F04022
Fresno	10	03	3127 N. Millbrook Avenue	Fresno	93726	F10031
Humboldt	12	01	929 Koster (SFIS Coord.)	Eureka	95501	F12014
Imperial	13	01	2995 South Fourth Street, Suite 105 (SFIS Coord.)	El Centro	92244	F13011
Inyo	14	03	301 W. Line Street, Suite B	Bishop	93545	F14031
Los Angeles	19	34	12000 Hawthorne Blvd.	Hawthorne	90250	F19341
Los Angeles	19	34	12000 Hawthorne Blvd.	Hawthorne	90250	F19342
Madera	20	06	425 N. Gateway Drive	Madera	93637	F20061

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Marin	21	04	10 North San Pedro Road, Suite 1023	San Rafael	94903	F21041
Mendocino	23	02	747 South State Street	Ukiah	95482	F23021
Merced	24	04	626 West 18th. Street	Merced	95340	F24041
Napa	28	03	1500 Third Street, Suite B7	Napa	94559-2936	F28031
Orange	30	08	401 Civic Center	Santa Ana	92704	F30081
Riverside	33	02	3021 Franklin Street	Riverside	92507	F33021
Sacramento	34	12	3443 Routier Road	Sacramento	95827	F34121
San Bernardino	36	26	606 East Mill Street	San Bernardino	92402	F36261
San Diego	37	13	4990 Viewridge Avenue	San Diego	92123	F37131
San Francisco	38	05	160 S. Van Ness Avenue	San Francisco	94130	F38051
San Joaquin	39		343 E. Main Street, 6th. Floor	Stockton	95202	F39021
San Mateo	41	05	400 Harbor Blvd., #C (SFIS Coord.)	Belmont	94002	F41052
Santa Clara	43	07	217 Devcon Drive	San Jose	95133	F43071
Shasta	45	04	1505 Court Street	Redding	96001	F45041
Siskiyou	47	01	818 S. South Main Street (SFIS Coord. @ 818 Marconi Ave.)*	Yreka	96097	F47011
Solano	48	03	275 Beck Street	Fairfield	94533	F48032

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Tehama	52	02	633 Washington Street	Red Bluff	96080	F52021
Tulare	54	07	113 N. Church, Suite 418	Visalia	93291	F54071
Ventura	56	06	4245 Market Street	Ventura	93003	F56061
Yolo	57	01	500 Jefferson Blvd.	West Sacramento	95605	F57011
Yuba	58	01	6000 Lindhurst Avenue (SFIS Coord.)	Marysville	95901	F58013
Total Fraud Workstations						30
CDSS	00	01	2525 Natomas Park Drive	Sacramento	95833	M00012
Alpine	02	01	75 Diamond Valley Road	Markleeville	96120	M02011
Amador	03	01	1003 Broadway	Jackson	95642	M03011
Butte	04	02	2445 Carmichael Drive	Chico	95928	M04021
Butte	04	04	78 Table Mountain Blvd.	Oroville	95965	M04041
Calaveras	05	01	509 St. Charles	San Andreas	95249-9709	M05011
Colusa	06	01	251 E. Webster Street	Colusa	95932	M06011
Contra Costa	07	02	30 Muir Road	Martinez	94553	M07021
Del Norte	08	01	880 Northcrest	Crescent City	95531-2313	M08011
El Dorado	09	01	3057 Briw Road (SFIS Coord.)	Placerville	95667	M09012

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
El Dorado	09	02	971 Silver Dollar Avenue	South Lake Tahoe	96150-2600	M09021
Glenn	11	01	420 East Laurel	Willows	95988	M11011
Imperial	13	01	2995 South Fourth Street, Suite 105 (SFIS Coord.)	El Centro	92244	M13012
Inyo	14	04	914 North Main Street	Bishop	93514	M14041
Kern	15	01	100 E. California Avenue (SFIS Coord.)	Bakersfield	93302	M15014
Kings	16	01	1200 South Drive, Bldg. 8 (SFIS Coord.)	Hanford	93230	M16011
Lake	17	01	15975 Anderson Ranch Road	Lower Lake	95457	M17011
Lassen	18	01	720 Richmond Road (SFIS Coord.)	Susanville	96130	M18011
Madera	20	04	629 E. Yosemite Avenue	Madera	93638	M20041
Mariposa	22	01	5186 Hwy 49 North	Mariposa	95338	M22011
Mariposa	22	02	5200 Hwy 49 North	Mariposa	95338	M22021
Mendocino	23	01	737 South State Street	Ukiah	95482	M23011
Mendocino	23	03	825 S. Franklin	Fort Bragg	95437	M23031
Modoc	25	01	120 North Main (SFIS Coord.)	Alturas	96101	M25011
Mono	26	01	452 Old Mammoth Road	Mammoth Lakes	93546	M26011
Mono	26	02	85 Emigrant Street	Bridgeport	93517	M26021

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Mono	26	03	107384 Hwy 395	Walker	96107	M26031
Monterey	27	01	1000 South Main (SFIS Coord.)	Salinas	93901	M27012
Napa	28	01	2261 Elm Street (SFIS Coord.)	Napa	94559-3731	M28011
Nevada	29	03	950 Maidu Avenue	Nevada City	95959	M29031
Placer	31	01	11519 B Street	Auburn	95603	M31011
Plumas	32	01	270 County Hospital Way, Suite. 207	Quincy	95971	M32011
Riverside	33	04	3178 Hammer Avenue	Norco	91760	M33041
San Benito	35	01	1111 San Felipe Road (SFIS Coord.)	Hollister	95023	M35011
San Bernardino	36	26	606 East Mill Street	San Bernardino	92402	M36262
San Joaquin	39	01	333 East Washington Street (SFIS Coord.)	Stockton	95202	M39014
San Luis Obispo	40	04	3433 S. Higuera (SFIS Coord.)	San Luis Obispo	93401	M40041
Santa Cruz	44	02	1020 Emeline Street	Santa Cruz	95060	M44022
Sierra	46	01	202 Front Street (SFIS Coord.)	Loyalton	96118	M46011
Siskiyou	47	01	818 S. South Main Street (SFIS Coord. @ 818 Marconi Ave.)*	Yreka	96097	M47012
Solano	48	01	355 Tuolumne Street	Vallejo	94590	M48011
Solano	48	03	275 Beck Street	Fairfield	94533	M48031

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Sonoma	49	02	2225 Challenger Way, Suite 101	Santa Rosa	95407	M49021
Sonoma	49	03	520 Mendocino Avenue	Santa Rosa	95402	M49031
Stanislaus	50	01	251 East Hackett Road (SFIS Coord.)	Modesto	95353	M50013
Sutter	51	01	190 Garden Highway (SFIS Coord.)	Yuba City	95992	M51011
Tehama	52	01	22840 Antelope Blvd.	Red Bluff	96080	M52011
Trinity	53	01	1-A Industrial Park Way (SFIS Coord.)	Weaverville	96093	M53011
Tulare	54	04	458 E. O'Neal Avenue	Tulare	93275	M54041
Tuolumne	55	01	20075 Cedar Road North	Sonora	95370	M55011
Yolo	57	02	25 N Cottonwood Street	Woodland	95695	M57022
Yuba	58	01	6000 Lindhurst Avenue (SFIS Coord.)	Marysville	95901	M58011
Total Multi Function Workstations						52
El Dorado	09	01	3057 Briw Road (SFIS Coord.)	Placerville	95667	P09013
Fresno	10	02	4455 E. Kings Canyon Road (SFIS Coord.)	Fresno	93702	P10051
Fresno	10	02	4455 E. Kings Canyon Road (SFIS Coord.)	Fresno	93702	P10101
Imperial	13	01	2995 South Fourth Street, Suite 105 (SFIS Coord.)	El Centro	92244	P13013
Imperial	13	01	2995 South Fourth Street, Suite 105 (SFIS Coord.)	El Centro	92244	P13021

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Inyo	14	02	162 Grove Street, Suite A (SFIS Coord.)	Bishop	93514	P14022
Kern	15	01	100 E. California Avenue (SFIS Coord.)	Bakersfield	93302	P15015
Kings	16	01	1200 South Drive, Bldg. 8 (SFIS Coord.)	Hanford	93230	P16012
Lake	17	01	15975 Anderson Ranch Road	Lower Lake	95457	P17012
Lassen	18	01	720 Richmond Road (SFIS Coord.)	Susanville	96130	P18012
Monterey	27	01	1000 South Main (SFIS Coord.)	Salinas	93901	P27013
Riverside	33	01	4060 County Circle Drive (SFIS Coord.)	Riverside	92503	P33151
Riverside	33	01	4060 County Circle Drive (SFIS Coord.)	Riverside	92503	P33161
Sacramento	34	01	1725 28th Street (SFIS Coord. @ 3737 Marconi Ave.)*	Sacramento	95816	P34013
San Benito	35	01	1111 San Felipe Road (SFIS Coord.)	Hollister	95023	P35012
San Francisco	38	01	170 Otis Street (SFIS Coord.)	San Francisco	94120	P38014
San Francisco	38	01	170 Otis Street (SFIS Coord.)	San Francisco	94120	P38015
San Joaquin	39	01	333 East Washington Street (SFIS Coord.)	Stockton	95202	P39015
San Luis Obispo	40	04	3433 S. Higuera (SFIS Coord.)	San Luis Obispo	93401	P40051
San Mateo	41	05	400 Harbor Blvd., #C (SFIS Coord.)	Belmont	94002	P41091
Santa Barbara	42	05	234 Camino Del Remedio (SFIS Coord.)	Santa Barbara	93110-1369	P42052

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Shasta	45	02	2460 Breslauer Way (SFIS Coord.)	Redding	96001	P45051
Shasta	45	02	2460 Breslauer Way (SFIS Coord.)	Redding	96001	P45052
Sierra	46	01	202 Front Street (SFIS Coord.)	Loyalton	96118	P46021
Siskiyou	47	01	818 S. South Main Street (SFIS Coord. @ 818 Marconi Ave.)*	Yreka	96097	P47013
Solano	48	05	201 Georgia Street	Vallejo	94590	P48051
Stanislaus	50	01	251 East Hackett Road (SFIS Coord.)	Modesto	95353	P50021
Sutter	51	01	190 Garden Highway (SFIS Coord.)	YubaCity	95992	P51021
Trinity	53	01	1-A Industrial Park Way (SFIS Coord.)	Weaverville	96093	P53021
Tulare	54	06	5957 South Mooney Blvd. (SFIS Coord.)	Visalia	93277	P54012
Ventura	56	01	77 California (SFIS Coord.)	Ventura	93001	P56053
Yuba	58	01	6000 Lindhurst Avenue (SFIS Coord.)	Marysville	95901	P58012
Total Portable Workstations						32
CDSS	00	01	2525 Natomas Park Drive	Sacramento	95833	S00011
Alameda	01	09	1351 Harbor Bay	Alameda	94501	S01091
Butte	04	03	202 Mira Loma	Oroville	95965	S04031
Contra Costa	07	07	40 Douglas Drive	Martinez	94553	S07071

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Fresno	10	07	3109 N. Millbrook Ave.	Fresno	93703	S10071
Humboldt	12	05	507 F Street	Eureka	95501	S12051
Los Angeles	19	33	14714 Carmenita	Norwalk	90650	S19331
Marin	21	01	120 Redwood Way	San Rafael	94903	S21012
Merced	24	01	2115 West Wardrobe Avenue	Merced	95340	S24012
Orange	30	01	888 North Main Street	Santa Ana	92704	S30011
Placer	31	05	375 Nevada Street	Auburn	95603	S31051
Riverside	33	01	4060 County Circle Drive (SFIS Coord.)	Riverside	92503	S33011
Sacramento	34	11	3737 Marconi Ave.	Sacramento	95821	S34111
San Diego	37	06	1255 Imperial Avenue	San Diego	92101	S37062
San Francisco	38	02	1235 Mission	San Francisco	94103	S38025
San Mateo	41	05	400 Harbor Blvd., #C (SFIS Coord.)	Belmont	94002	S41051
Santa Barbara	42	06	2125 S. Centerpointe Ply.	Santa Maria	93455-1338	S42062
Santa Clara	43	06	333 West Julian Street	San Jose	95110	S43061
Shasta	45	02	2460 Breslauer Way (SFIS Coord.)	Redding	96001	S45022
Tulare	54	06	5957 South Mooney Blvd. (SFIS Coord.)	Visalia	93277	S54061

**RFP OSI 2046
CURRENT SYSTEM**

County Name	Co. No.	Site No.	Address	City	ZIP	WS Name
Ventura	56	01	77 California (SFIS Coord.)	Ventura	93001	S56011
Total System Admin Workstations						21

Total Client Input Workstations 214

Total Fraud Workstations 30

Total Multi Function Workstations 52

Total Portable Workstations 32

Total System Admin Workstations 21

**RFP OSI 2046
CURRENT SYSTEM**

F. CENTRAL SITE ENVIRONMENT

Central Site computing equipment for SFIS is located in the DTS South Annex; 3301 S Street; Sacramento, CA 95816. The current Contractor operates the Central Site equipment. The following describes Central Site interaction, facility, computing equipment, network, and processes.

CENTRAL SITE INTERACTION

SFIS workstations are capable of interacting with the SFIS Central Site database. Depending on the type of workstation and the type of user, the SFIS workstation interacts with the Central Site database for the purposes of:

- Adding a new client record for search, match, and filing (client and control data, fingerprint image(s), and color photo).
- Updating a client record and (optionally) re-submitting the record for Closed or Open Search.
- Inquiring on a client record.
- Receiving a Match/No Match Confirmation.
- Inquiring on (full digital) fingerprint image(s) with split screen workstation display for comparison of two (2) different fingerprint images.
- Inquiring on (full digital) photo image(s) with split screen workstation display for comparison of two (2) different photo images.
- Printout of full or partial client record information (digital fingerprint image(s), client data, photographic images, etc.).
- Confirmation of the identity of a client based on side-by-side photo comparisons and/or side-by-side fingerprint image comparisons.

DTS FACILITIES

The SFIS Central Site computer systems are housed at the California DTS facilities. These facilities consists of two (2) physical locations about one thousand feet (1,000') apart, DTS and the South Annex. SFIS computer systems are installed in the South Annex location. The facility is secured and equipped with UPS battery backup systems and diesel generators for continued operation in the event of disruptions to utility power. DTS services and supports over two thousand (2K) State and County locations using over one hundred thousand (100K) terminals and PC workstations. The DTS wide-area network interconnects all fifty-eight (58) County government networks and all State data centers.

**RFP OSI 2046
CURRENT SYSTEM**

NETWORK ENVIRONMENT

The Production network connects approximately two hundred and seventy-five (275) SFIS county locations to DTS (A listing of all remote SFIS workstation locations may be found in the tables above, in the paragraphs about the County environment.). Until recently, the wide-area network (WAN) utilized DS1 (one point five megabits per second (1.5Mbps)) Frame Relay data communication services exclusively. However, a recent WAN redesign project replaced many of the DS1 ports with DS0 (fifty-six kilobits per second (56Kbps)) ports and ADSL (Asymmetric Digital Subscriber Line) technology. Currently, WAN changes occur only if a change occurs at a site that causes them to be the single users of the circuit versus sharing the circuit with another State Project.

DTS LAN and WAN Overview

DTS is responsible for the design, engineering, implementation, and operation of the SFIS wide-area network (WAN) and for the DTS portion of the local-area networks (LANs). OSI, in conjunction with the SFIS Project Team, determines the LAN and WAN specifications based on SFIS application requirements. From these specifications, DTS procures equipment, provides data circuits, and installs the data service. Once installed, DTS is responsible for ongoing monitoring, support, and maintenance of the DTS LAN and SFIS WAN environments.

The SFIS Central Site equipment is housed in the South Annex. The South Annex and DTS sites are interconnected with dual Gigabit Ethernet ports two gigabits per second (2Gbps) and Cisco's Fast EtherChannel technology configured at eight hundred megabits per second (800Mbps) capacity for a total bandwidth of two point eight gigabits per second (2.8Gbps). Cisco's Fast EtherChannel bundles up to four (4) full-duplex Fast Ethernet two hundred megabits per second (200Mbps) links into one (1) circuit.

DTS has standardized on Cisco Systems communication equipment (switches, hubs, routers, etc), Kentrox CSU/DSUs, and SBC Communications Frame Relay data communications services.

A Channel Service Unit/Data Service Unit (CSU/DSU) is required at both ends of a digital communications circuit. The CSU provides protective and diagnostic functions for the circuit and the DSU is needed to connect the communication router to the circuit. Typically, the two (2) devices are packaged as a single unit.

**RFP OSI 2046
CURRENT SYSTEM**

SFIS WAN Redesign Project

Initially, all SFIS county sites were connected to DTS via frame relay services. Frame relay is a connection oriented, packet (frame) based communications service with speed ranging from DS0 (fifty-six kilobits per second (56Kbps)) to DS3 (forty-three megabits per second (43Mbps)). There are four (4) DS3 access circuits that enter DTS and four (4) DS3 access circuits that enter the South Annex. These circuits act as backups to one another. Should a data communications problem arise in one site, the production traffic will continue to flow into the other site. SFIS production traffic shares these DS3 access circuits with other DTS customers.

Recently, a SFIS network redesign project occurred that reduced the Frame Relay circuit DS0 at approximately sixty (60) county locations. The reduction in bandwidth was recommended based on past network utilization and cost savings. The sites selected for conversion did not share the data circuit with any other State project and each contained only one (1) input capture workstation. The estimated bandwidth required for a single image capture workstation is less than forty-eight kilobits (48Kbps).

The network redesign project also resulted in implementation of ADSL (Asymmetric Digital Subscriber Line) services in approximately one hundred (100) SFIS county locations.

The DTS/SBC Communications' DSL service offering available to SFIS is Asymmetrical Digital Subscriber Line (ADSL). DTS/SBC offered three (3) downstream/upstream bandwidth combinations: 1) 384Kbps/128Kbps, 2) 384Kbps/384Kbps, and 3) 1.5Mbps/384Kbps. SFIS utilizes the 384Kbps/384Kbps w/Committed Information Rate (CIR) of 128Kbps for their remote sites.

Contractor Site Network Charges

The current Contractor is responsible for all charges associated with establishing communication network services between any current Contractor office requiring SFIS access and the SFIS Central Site. The purpose of these network services would be to link Contractor personnel who are responsible for maintenance and/or operation of SFIS to the SFIS Central Site.

**RFP OSI 2046
CURRENT SYSTEM**

Network Management

DTS is responsible for network problem management and ongoing network performance monitoring and capacity planning of both the DTS LAN and SFIS WAN environments. The DTS Network Operations Center (NOC), which operates twelve (12) hours per day from 7 a.m. to 7 p.m., five (5) days per week, is the front-line monitoring organization. The NOC utilizes HP Openview, CiscoWorks2000, and Concord Network Health to monitor and manage the LANs and WAN. With these products, the NOC can identify failures in the networks, perform problem diagnosis, and obtain network performance and utilization information.

HP Openview

DTS utilizes HP Openview for network monitoring.

CiscoWorks2000

Cisco Systems' CiscoWorks2000 is a family of products that provide management and operation solutions for LANs and WANs. DTS utilizes two (2) CiscoWorks2000 products to help monitor and manage the SFIS production environment: The LAN Management Solution and the Routed WAN Management Solution.

Concord eHealth Suite

The eHealth suite of software tools provides the components for managing the network portion of the computing infrastructure. It enables critical data to be collected from network devices and communication technologies including LANs, WANs, routers, switches, and Frame Relay circuits, throughout the network infrastructure.

With this tool the NOC manages the entire DTS portion (the WAN and DTS LAN) of the SFIS network. A Daily Health Report is created that identifies any network components that exceed preset utilization and performance thresholds. NOC personnel review this report and take action as appropriate to correct any identified network related problems.

**RFP OSI 2046
CURRENT SYSTEM**

CENTRAL SITE LAN, HARDWARE AND SOFTWARE

The Central Site Production LAN consists of a Cisco Systems 2600 Series Router and two (2) Cisco Catalyst 3500 Series XL Switches. On one side, the 2600 Series Router is directly connected to the DTS router providing access to the SFIS sites through the WAN. On the other side, the router connects to the two (2) production Catalyst 3500 Ethernet Switches. The two (2) Catalyst switches connect the Central Site servers, Motorola/Printrak servers, process coordinator workstations, and administrative workstations to the SFIS LAN.

Deleted: Printrak

The current Contractor router operations staff monitors the SFIS Central Site Cisco router and Catalyst switches. The current Contractor / SFIS operations staff maintains operational coverage at the Central Site from 6 a.m. to 9 p.m. SFIS end users have access to the system from 7 a.m. to 7 p.m.

The SFIS Central Site equipment consists of the following major components:

- Database server;
- DBA Workstation;
- Process Coordinator Workstations;
- System Console Workstation;
- Network Printers; and
- Motorola/Printrak Automated Fingerprint Identification System (AFIS).

Deleted: Printrak

Database Server

The Database Server is a Hewlett Packard (HP) 9000 N4000 (One (1) primary and one (1) backup). The Database Server acts as the primary transaction processor in SFIS. The server receives incoming requests from the remotely located SFIS workstations and responds from its available database of demographic information, minutiae feature data from the fingerprints, transaction queuing data (including transaction status), security data, etc. Any data not stored in the Informix RDBMS, which resides on the server, will be accessed over the local area network (LAN) from the Digital Image Retrieval Subsystem (DIRS). This server acts as the master transaction processor. The HP N4000 contains the queuing information that tracks each transaction through the system and coordinates the response to remotely located SFIS workstations.

The specific hardware components comprising the Database Server, the associated peripherals and the software installed are listed in the following chart.

**RFP OSI 2046
CURRENT SYSTEM**

Database Server Configuration

Description	Size/Model/Version as Applicable
Server	HP 9000 N4000
Processor	N-Class three hundred and sixty megahertz (360MHz) PA-8500 (4 processors)
RAM	Four gigabytes (4GB) High Density SyncDRAM Memory
Internal Disk (Fiber Channel Bus)	Eighteen gigabyte (18GB) HotPlug Ultra2 SCSI LP Disk
DAT Tape Drive	Four millimeter (4mm) DDS-3
CD-ROM	32x DVD-ROM
Communications Device	10/100 Mbps Ethernet NIC
Monochrome Monitor	Fifteen (15) inch
Operating System	HP-UX 11.0

Workstation Configuration

The DBA, Process Coordinator, Image Coordinator, Match Coordinator, and Purge Coordinator are all configured the same, yet used for different purposes. There are twelve (12) total workstations.

**RFP OSI 2046
CURRENT SYSTEM**

Workstation Configuration

Description	Size/Model/Version as Applicable
<i>Workstation – used for DBA, process coordinators, system console and test process console</i>	HP Visualize B1000
PA-8500 Processor	Three hundred megahertz (300MHz) single processor unit
RAM	Five hundred and twelve megabytes (512MB)
Internal Disk (Fiber Channel Bus)	Nine gigabytes (9GB)
DAT Tape Drive	Four millimeter (4mm) DDS-3
CD-ROM	32x ATAPI
Communications Device	10/100 Mbps Ethernet NIC
Color Monitor	Nineteen (19) inch High Resolution
Operating System	HP-UX 11.0

DBA Workstation

The Database Administrator (DBA) Workstation is available for monitoring the performance of the database and database maintenance activities including upgrades, index reorganization, table changes associated with specific change requests, etc.

The specific configuration of the DBA Workstation is listed in the table above.

**RFP OSI 2046
CURRENT SYSTEM**

Process Coordinator Workstations

The process coordinators include image coordinators, match coordinators, and purge coordinators. These coordinators are necessary to off-load processes from the Database Server which involve moving and storing large image files. These process coordinators perform tasks such as the I/O intensive processes of handling the fingerprint image and photo files, to ensure that the server has adequate processing power available to respond in a timely manner to all workstations. Off-loading is an important design feature in preventing delays in Database Server response.

Image Coordinator Workstation

The image coordinators are responsible for receiving all incoming fingerprint and photo image files from the remote workstations, as well as sending images to remote workstations. The Database Server maintains queues to indicate that the remote workstation sent the file. This same queue is updated by the image coordinator to indicate what files were received, allowing the Database Server to communicate to the remote workstation for a resend of an image if necessary. The Database Server is, however, never involved in the actual I/O intensive process of receiving the image. Though the Database Server is constantly aware of the status of the transaction, it has not used resources by becoming involved in the actual transmission and receipt of the large image files. The image coordinators then ensure that the image files are stored in the DIRS, once again updating the transaction status on the Database Server to indicate that the storage is complete and place the index to the images on the correct database row for the corresponding CIN.

RFP OSI 2046 CURRENT SYSTEM

Match Coordinator Workstation

The match coordinators serve a purpose for the Open Search matching process, off-loading a CPU intensive process from the server. The match coordinators communicate with the Database Server to access the Open Search processing queue. Upon determining the next search to process, based on the priority and length of time on the queue, the match coordinator formats the correct request for the Motorola/Printrak matching subsystem and attaches the corresponding fingerprint image file based on the internally generated PCN number. The match coordinator then submits the request to the Motorola/Printrak subsystem for matching. While the matching process is occurring, the match coordinator continues to post requests to the matching subsystem's queue. Upon receiving the response from the matching subsystem, the match coordinator posts the information to the RDBMS for verification or response to the workstation as appropriate.

Deleted: Printrak

Deleted: Printrak

Purge Coordinator Workstation

The purge coordinator off-load Input/Output (I/O) intensive work from the Database Server by managing the archive of purged data. The purge coordinator is attached to an optical disk library, which stores all purged data. The purge coordinator handles the storage of purge data by retrieving the data stored on the Database Server and the DIRS, and placing it in the optical disk library. An index to the information is returned to the Database Server for tracking and potential retrieval. Should the Database Server receive a request for archived data from a remote workstation, the purge coordinator is responsible for locating the archived information and returning the appropriate data to both the Database Server and the DIRS. The purge coordinator then marks the transaction complete, indicating to the Database Server that the data has been restored.

Network Printers

Network printers are available to all workstations and servers on the Central Site LAN. Any reporting, batch cycle or ad hoc, system administration messages, or specific printout requests from any workstation such as the DBA Workstation or the coordinator workstations are routed to the network printers.

The configuration of the network printers is shown on the following chart.

**RFP OSI 2046
CURRENT SYSTEM**

Network Printer Configuration

Description	Size/Model/Version as Applicable
Network Printer	Xerox DocuPrint N24
Print Speed	Twenty four (24) pages per minute one (1) or two (2) sided
Paper Tray	Maximum Media Output Capacity

Motorola, Inc./Biometrics Business Unit Subsystems

Technology provided by Motorola, Inc./Biometrics Business Unit (referred to hereafter as Motorola/Printrak, and formerly known as Motorola/Printrak International, a Motorola Company) has been installed at the SFIS Central Site to perform Open Search matching capability and data storage and retrieval. Motorola/Printrak processing at the Remote Input Workstation includes image quality check, extraction, Wavelet Scalar Quantization (WSQ) compression, and Closed Search matching.

Deleted: Printrak

Deleted: Printrak

Deleted: Printrak

Matching Subsystem

SFIS fingerprint matches are performed on a Search Processor 2000 (SP 2000). The SP 2000 is designed to meet storage and workload specifications with proven real-time architecture. The technical search engine, the SP 2000, employs multiple parallel Adaptive Match Processors (AMPs) controlled by a Minutiae Match Controller (MMC). This parallel processing, in which multiple segments of the fingerprint databases are searched simultaneously, supports the real-time processing needs of the State.

A MMC stores the entire SFIS minutiae database on mirrored disks. This MMC oversees multiple AMPs, which operate in parallel. The minutiae database is distributed evenly among the AMPs and is stored in RAM for fast search/match processing. Each AMP searches its own segment of the database and reports search results to the MMC, which combines all results into a single Match Report, sorted in descending order of probability of a match. Fingerprint and demographic data are held in RAM and on magnetic disks, with a tape unit provided for off-site archival purposes.

RFP OSI 2046 CURRENT SYSTEM

When a search is submitted, an AMP uses geometric based matching to compare the location and orientation of fingerprint minutiae (or feature points) between the search print and the file print. The AMP calculates a match score for each search print against file prints from the database. High match scores are candidates for the true match. [Motorola/Printrak](#)'s EXPERT Match Processor emulates the verification process of a fingerprint expert. The objective of the EXPERT Matcher is to apply a very detailed matching process to the search print and each of the top N number of file prints in the respondent (or candidate) list in order to boost the match score of the correct candidate and move it to the top of the list.

Deleted: Printrak

The EXPERT Matcher process is based on cognitive theory and makes use of structural and graph based topological features such as minutiae type, minutiae neighbor similarity, minutiae connectivity, minutiae constellation matching, distance-based ridge count similarity, ridge-trace similarity, and ridge-flow similarity. These feature comparison processes are the same skills that the fingerprint "expert" would use to visually compare two (2) side-by-side images. To accomplish these processes, the EXPERT Matcher requires the extracted minutiae as well as the thinned image (skeleton) for each print. This data is extracted by the [Motorola/Printrak](#) AFP and is stored as compressed data within the EXPERT Match Redundant Array of Independent Disks (RAID) that allows rapid retrieval and processing. Adequate EXPERT Match processors are designed into the system in order to accomplish the required workload within the available time. Typically, fingerprint candidates are compared by the matching subsystem within twenty (20) seconds.

Deleted: Printrak

The configuration of the SP 2000 (one (1) processor only), including its MMCs, AMP, and EXPERT Matcher components, is listed in the following chart.

**RFP OSI 2046
CURRENT SYSTEM**

Matching Configuration

Description	Size/Model/Version as Applicable
<i>Search Processor (Match/Server Cabinet)</i>	SP 2000
<i>Minutiae Match Controller</i>	MMC 2000
Processor	DEC Alpha 1000A
RAM	Two hundred and fifty-six megabytes (256MB)
Internal Disk	Two by four gigabytes (2 x 4 GB) and two by nine gigabytes (2 x 9 GB)
Operating System	UNIX
DLT Drive	Quantum
<i>Adaptive Match Processors</i>	AMP
Processor	Compaq Personal Workstation 6333E
RAM	Two hundred and fifty-six megabytes (256MB)
<i>EXPERT Match Processor</i>	EM 2000
Processor	DEC Alpha 1000A
RAM	Two hundred and fifty-six megabytes (256MB)
Internal Disk	Two by four gigabytes (2 x 4 GB)
Operating System	UNIX

RFP OSI 2046 CURRENT SYSTEM

Digital Image Retrieval Subsystem (DIRS)

The DIRS manages the storage and retrieval of the large image files in SFIS. These files include the fingerprint images and photos associated with each client. The DIRS consists of a server with attached RAID technology for quick access to the image files. Specifically, the DIRS uses RAID, Level 5 magnetic disk arrays for database storage. (Search Processor (SP) data is also stored on its own-mirrored RAID-1 array.) Data recovery is achieved without interrupting the normal operation of the system.

In the Motorola/Printrak AFIS for SFIS, the Informix relational database management system (RDBMS) is used for indexing of fingerprint data. RDBMS data is accessed via Structured Query Language (SQL), an industry standard used for data access and report generation. Informix software resides on the HP9000/N4000, which communicates directly with the Database Server.

Deleted: Printrak

The Informix RDBMS supports every component of AFIS operations. Fingerprint images, feature data, photographs, and descriptive data are all indexed via Informix to ensure fast and accurate data retrieval for all applicant records. Fingerprint images and *EXPERT* feature data are stored on the HP XP256, and descriptive and minutiae feature data are stored in a Sybase database on the SP 2000. Informix and Sybase databases are capable of storing a nearly unlimited number of records. Sybase automatically mirrors the contents of the minutiae/descriptor database. If the database is lost, it can be recreated from its mirror image. This database, as well as the image and secondary feature data, is also protected by redundant RAID storage. The DIRS is equipped with a DLT library tape drive used for backing-up image data.

The RAID and tape solutions are designed to improve reliability of SFIS, but also contribute to real-time system speed by reducing image retrieval time. Fast tape drives and RAID-based disk partitioning allows restoration of data.

**RFP OSI 2046
CURRENT SYSTEM**

The configuration of the DIRS is shown on the following chart.

Digital Image Retrieval System Configuration

Description	Size/Model/Version as Applicable
<i>Data Storage/Retrieval</i>	HP XP256 Disk Array
Processor	HP9000/N4000
RAM	Four gigabytes (4GB)
Internal Hard Disk	Eighteen gigabytes (18GB)
DAT Drive	Four millimeter (4mm) DDS-3
External RAID	Thirty-six point nine gigabytes (36.9GB) per Disk
Operating System	UNIX
Relational Database Management System	Informix

HP SureStore E XP256 Disk Array

The SFIS Database and the DIRS data both reside on an HP XP256 Disk array. The Database Server utilizes the process coordinators and the Informix relational database software to store SFIS and DIRS information on the HP XP256 Disk Array.

When a fingerprint image is captured at the remote workstation, the workstation generates the following files:

- WSQ – Compressed image of the fingerprint;
- THN – Thinned image of the fingerprint;
- FDP – Minutiae data of the fingerprint;
- DAT – Index and key data for the fingerprint;
- JPG – Photo of the recipient in JPEG format; and
- BMP – Raw fingerprint image bitmap.

RFP OSI 2046 CURRENT SYSTEM

The WSQ, THN, FDP, DAT, and JPG files are transmitted to the Central Site Database Server and then stored in DIRS on the XP256. At night, BMP files are copied to the XP256 where it is temporarily stored until it is written to DLT tape for long-term, off-site storage.

The XP256 disk array is based on a Hitachi storage engine with HP specific enhancements in firmware, performance, and Fiber Channel connectivity. The XP line of Disk Arrays provides:

- High availability, no single point of failure, non-disruptive upgrades;
- Continuous data availability and data storage protection with RAID1 and RAID5 and battery-protected, mirrored write cache;
- Multi-terabyte scalability from seventeen gigabytes (17GB) to nine terabytes (9TB); and
- High performance with one hundred megabytes per second (100MBps) Fiber Channel ports.

Currently, there are twenty-five (25) disk drives in the XP256, twenty-four (24) in use and one (1) serves as a spare. At thirty-six gigabytes (36GB) each, there is a total of eight hundred and sixty-four gigabytes (864GB) disk space. The disk drives are configured for redundancy using RAID5.

The use of RAID5 reduces the total of eight hundred and sixty-four gigabytes (864GB) disk space to six hundred and fifteen gigabytes (615GB) of usable disk space. Of the six hundred and fifteen gigabytes (615GB) of usable disk space, five hundred gigabytes (500GB), or eighty-one percent (81%), are allocated for production use. Of the five hundred gigabytes (500GB) allocated for production, only sixty-eight gigabytes (68GB), or fourteen percent (14%), are currently utilized. The SIFS production data residing on the XP256 consumes only eleven percent (11%) of the total usable disk space.

HP SureStore E Tape Library

The Central Site uses an HP SureStore E DLT tape library for backup. The tape library subsystem is configured with two (2) DLT 8000 tape drives and capacity for forty (40) tape cartridges. This provides one point six terabytes (1.6TB) of storage capacity. The backup system software is HP Omniback.

RFP OSI 2046 CURRENT SYSTEM

The tape subsystem is used to backup the Database Server, all HP B1000 UNIX workstations, all Windows NT workstations at the Central Site, the SFIS/Informix database, and the DIRS data located in the XP256. The original fingerprint images (.bmp files) are also copied onto DLT 8000 tape cartridges. The current Contractor uses ARCUS (formerly known as Iron Mountain Inc.) as the off-site tape storage vendor.

HP-UX Operating System Software

The operating system in use on the Database Servers and the Process Coordinators is HP-UX 11.0.

Informix Dynamic Server Software

The SFIS HP9000 Database Servers use Informix Dynamic Server 7.31.UC4 as the relational database management system. The Informix database, or SFIS database, maintains information about the system including general configuration data, county specific configuration data, case information, transaction status, and system status information. The SFIS/Informix database is stored on the HP XP256 Disk Array that provides hardware redundancy through RAID5 disk configurations.

For recovery purposes, the current Contractor has configured Informix transaction logging. SFIS database transactions are written directly to a DLT 8000 tape. Database recovery is achieved by first restoring the database from full and incremental backups, and next applying the transactions in the log file.

Fraud Investigation/Verification Workstation

Fraud Investigation Workstations and Verification Workstations are used to view side-by-side fingerprint images, photos, and demographic information of records in the various verification queues. These queues include Closed Search No Match Found, Open Search Match Found, and SFIS File Request images (Fraud Investigation Workstation Only) requested for viewing from the SFIS database. The Verification Technicians indicate their concurrence or change the matching status of the viewed images using their workstation. The configuration of the Fraud Investigation/Verification Workstation is shown on the following chart.

**RFP OSI 2046
CURRENT SYSTEM**

Fraud Investigation/Verification Workstation Configuration

Description	Size/Model/Version as Applicable
PC	Gateway E-4200
Pentium II Processor	Four hundred and fifty megahertz (450MHz) single processor unit
ZIP Drive	All PC's have a ZIP Drive. Available for use on all machines except for MAU.
Diskette Drive	All PC's have a 1.44 MB Floppy. Available for use on DAU only.
CD-ROM	All PC's have a 17x – 40x max. Available for use on DAU only.

System Expansion

Two (2) system design features, central site modularity and workstation processing, ensures system expansion to at least twice the number of transactions per day (As described in the workload and throughput paragraphs of this document) and an expansion to the number of records stored in the SFIS database (As described in the database paragraphs of this document), without affecting performance in terms of system accuracy or the capability of handling progressively increasing volumes of transactions, stored records, and additional workstations.

The Central Site functionality is performed by multiple workstations in addition to the Database Server. This modular design allows large image file manipulations to be placed on a number of smaller workstations that are easily expanded. By placing the functions of image, match, and purge coordination on Central Site workstations, the Database Server is allowed to focus on receiving requests from remote workstations, queuing functions, transaction logs, and audit trails, and responding to remote workstations. The large image file processes of Remote Input Workstation image receipt, transfer of images to the matching subsystem and DIRS, and movement of files from the DIRS to archive are all off-loaded to smaller workstations.

RFP OSI 2046 CURRENT SYSTEM

The SFIS finger image database is partitioned into multiple subsets so that both inquiry and matching functions can occur in parallel mode. This parallel processing design results in a modular hardware setup.

Since the components of SFIS are modular, additional matching capacity can be easily added.

Motorola/Printrak claims to have designed Series 2000 to provide a family of modular, scaleable AFIS solutions that could be adapted to a wide variety of project needs. Series 2000 solutions are scaleable, so the practical limit of system capacity may be far beyond the typical project's capacity and workload needs.

Deleted: Printrak

The Search Processor (SP 2000) can be expanded.

The MMC directs parallel AMPs; this parallel processing architecture offers parallel searching of segments of an entire database. Each AMP in turn accommodates a variable quantity of DRAM memory (storing minutiae data and specific descriptors).

The number of MMCs, AMPs, and the amount of memory are all defined to meet the specific needs of SFIS for database capacity, workload, and response time.

Much of the required processing of a transaction is completed at the workstation prior to transmission to the Central Site. Finger image quality check, demographic data field edits, remote minutiae extraction, WSQ compression, and performance of Closed Searches are functions performed by the Remote Input Workstation, thus reducing the processing load on the Central Site.

Database

Currently, the SFIS database contains about seven (7) million fingerprint images. The SFIS database is designed to potentially accommodate fourteen point six million (14.6M) database records because of growth of existing programs as well as the addition of new programs.

**RFP OSI 2046
CURRENT SYSTEM**

Purge

The Purge table contains specific destination information such as volume, directory, and subdirectory of an archived client record. When the State System Administrator (or his/her staff) marks the record to be deleted (referred to as "image removal" by the County), a transaction record is inserted in this table to indicate what record has been deleted and where that record is located. Image Removal occurs at the request of the County to the State.

SFIS TEST AND TRAINING ENVIRONMENT

The current Contractor has built and maintains an SFIS test and training environment. The test servers, process coordinators, and Motorola/Printrak AFIS reside at the Central Site. Two (2) training facilities, one (1) in Monrovia operated by the Contractor and one (1) in Sacramento operated by OSI, are equipped with Multifunction Workstations. The counties have direct access to the training database via a method called SFIS Direct Training (DT), which allows a county to have their production workstation pointed to the training database via the Help Desk changing an .ini file. The test/training environment uses dedicated hardware (HP Database Server, HP process coordinator workstations, disk storage, tape backup, Motorola/Printrak Matching system) and software (Informix database, Motorola/Printrak database) and is isolated from the SFIS production environment to prevent conflicts with production. The test/training environment was configured to support production-like testing of application modifications and provides a testing and training environment for SFIS.

Deleted: Printrak

Deleted: Printrak

Deleted: Printrak

Test Bed System

The Test Bed system provides full functionality of SFIS for a five hundred thousand (500K) client-test database. The Database Server runs the same software as the primary server. A single process coordinator provides all the functionality running the same software as the image, match, and purge coordinators. The process coordinators are placed on separate machines for the production system solely due to the large volume of transactions. The test process coordinator handles the storage of purge data by retrieving the data stored on the Database Server and the DIRS and placing it in the optical disk library. Multifunction Workstations provide SFIS application testing functionality, as well as verification and quality review at the Central Site. The test workstation also includes a scanner, photo camera, and laser printer. Separate Motorola/Printrak subsystems are also installed in smaller quantity, but sufficient to provide response time and accuracy testing on a database of five hundred thousand (500K) clients.

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

The configuration of the Test Bed is provided in the following table.

Test Bed Configuration

Description	Size/Model/Version as Applicable
<i>Test Server</i>	HP R-Class R380/2 way
Processor	PA-8000 one hundred and eighty megahertz (180MHz) dual processor unit
RAM	One gigabyte (1GB)
Internal Disk (Fiber Channel Bus)	Eighteen gigabytes (18GB)
Disk Array	One hundred and eight gigabytes (108GB)
Communications Device	10/100 Mbps Ethernet
Operating System	HP-UX 11.0
<i>Test Server Peripherals</i>	
Monochrome Monitor	Fifteen (15) inch
Keyboard	USB

Testing

Before most application changes are tested, OSI and CDSS forms a County Design Group that has a representative perspective on proposed changes. For example, if there are proposed changes relative to the Fraud Investigation Workstation, Fraud Investigators will be members of the design group. The design group validates, prioritizes, and assists in designing the change. Upon confirmation from the County Design Group, the current Contractor will prepare the

RFP OSI 2046 CURRENT SYSTEM

change according to the requirements established by the Design Group, and begin testing.

The current Contractor created and maintains a test system that provides full functionality of SFIS for a five hundred thousand (500K) client-test database. The current Contractor conducts Unit Testing, System Integration Testing (SIT), and Regression Testing on Multifunction Workstations at the Central Site prior to State acceptance and Pilot Testing of a system change.

The current Contractor demonstrates the system change to the State, and if the State accepts it, the change may be piloted at the county sites. If the State does not accept the change, the current Contractor will make the necessary adjustments and demonstrate it again to the State upon completion of the adjustments.

Pilot tests are coordinated by OSI and CDSS and target the counties represented by design group participants, and additional counties/sites that have relevance to the changes. OSI's Programmer provides QA services to testing and deployment of major changes and performs this in person at the Central Site. Upon completion of pilot testing, OSI makes a recommendation of acceptance or rejection to CDSS. Upon CDSS acceptance, the changes are deployed to the production environment.

BACKUP AND RECOVERY

The following paragraphs explain backup and recovery procedures that restore data in case of external (loss of power) or internal (abnormal program end) system failure. The procedures are designed to ensure that data is not lost, thus preventing the need to re-enter data. Also described are system-monitoring functions that minimize downtime by early detection of potential and actual problems. All backup and recovery procedures are fully described in the System Operation and Support Plan (SOSP).

Backup

The files in the Matching Subsystem, DIRs, and the SFIS database are backed up during the Daily, Weekly, and Monthly Batch Cycles.

Raw Image Backup

Every workday evening, the current Contractor collects the raw images stored on the Remote Input Workstations in order to store them at the Central Site.

RFP OSI 2046 CURRENT SYSTEM

Once twenty-five thousand (25K) images have been collected, they are written to tape and sent off site for storage.

Matching Subsystem

There are two (2) components in the Matching Subsystem that need to be backed up. One (1) is the Sybase database. A full backup is done nightly to a Digital Linear Technology (DLT) tape (Matching Subsystem tape drive) using a Matching Subsystem Graphical User Interface (GUI).

The other component is the data volumes. These Matching Subsystem volumes contain the files needed to perform a match. The active volume is backed up nightly. The full volumes are backed up monthly. Both components are written to DLT using the Matching Subsystem GUI.

The Matching Subsystem GUI gives the user three (3) backup choices: Sybase database, current volume, or a previous volume. Choosing the appropriate selection allows backup of the components discussed. Please refer to the SOSP for more details on how to use this GUI.

DIRs Backup

The DIRs is a large chunk of disk space that has been split up into multiple volumes (v001, v002, v003, etc.). Under each volume there are multiple directories (d001, d002, d003, etc.). In each directory there are subdirectories (s001, s002, s003, etc.). When a client is added to the SFIS databases, the zip files of the image are stored in a DIRs location that consists of the volume, directory, and subdirectory. For example, if zip file "A" is in Volume 001, Directory 005, Subdirectory 026, the file is located in /v001/d005/s026 (UNIX directory). Each DIRs location consists of five hundred (500) zip files. When a volume fills up the next consecutive volume is employed.

OmniBack is used to backup each of the volumes in the DIRs to DLT. The active DIRs volume is backed up on a daily basis. For example, if Volumes 1 and 2 are full, the active directory is Volume 3, meaning all new images added are written to Volume 3 until it becomes full. Therefore, every night the Operator performs an incremental backup of Volume 3 to DLT using OmniBack. On a monthly basis the Operator executes a full backup of all the used volumes. The full volumes are backed up again because some of the zip files in the full volumes may have been updated with better quality prints or new photos.

RFP OSI 2046 CURRENT SYSTEM

It takes approximately ten (10) hours to back up the DIRs files (four hundred and eighty gigabytes (480GB) of data using two (2) DLT drives at an approximate speed of eight megabytes per second (8MBps)). Backup on the DIRs can be performed at the same time as an SFIS database backup.

SFIS Database Backup

The SFIS Database daily backup processes consist of incremental and full archives. An incremental backup will be performed daily before the batch cycle. The incremental backup is for preserving the integrity of data before the changes of the Daily Batch Cycle. The database is fully backed up at the end of the Daily Batch Cycle. It takes approximately two (2) hours to archive the SFIS database (forty-five gigabytes (45GB) of data using a single DLT drive at an approximate speed of eight megabytes per second (8MBps)). An incremental backup is also performed daily on the files in the DIRs as previously described.

The SFIS database has transaction logs constantly written for each transaction "commit." This combination of archive and transaction logs allows the database to be fully rebuilt, if necessary.

In the event that data is corrupted in the database as a result of changes during the day, a restoration is performed using the previous day's full backup, with that day's incremental backup, along with the logical logs that were written up to the failing period. A complete restoration of the SFIS database takes approximately two and a half (2 ½) hours using a single DLT tape drive. If the database application fails, a backup application is available from a mirrored disk in less than thirty (30) minutes. Each of the primary and backup Database Servers has a set of mirrored hard disks with hot-swapping capability.

Spare Backup

DIRs uses RAID technology that houses a set of hard disks. Data on the DIRs are constantly backed up. Therefore, the system is functional even though two (2) of the hard disks might fail. Two (2) spare hard disks are located in the DIRs for replacement.

In the event of a malfunction within a component of the Central Site system, SFIS can be restored to full operational status within approximately two (2) hours of original system failure.

Backup systems are provided for the following subsystems:

RFP OSI 2046 CURRENT SYSTEM

- Database server;
- Process coordinators;
- Image coordinators;
- Match coordinators;
- Interface coordinators;
- DBA Workstation;
- Network printer;
- System console;
- Verification Workstations; and
- Matching Subsystem.

Duplicate hardware is provided online at the Central Site to replace failed hardware. Crucial hardware components, including Database Servers and matching servers have replacement duplicates on site. If the information on a magnetic disk becomes unavailable, it is restored by replacing the failed disk (if necessary) and copying the data from the corresponding archive and log tapes. If the information in the master and, if applicable, the mirror volume has become unavailable, it is restored by copying the data from the Informix archive tape and applying all applicable journalized transactions.

Application Backup

The application software is backed up on a regular basis and sent to the off-site storage facility to ensure the complete restoration of the system in case of system failure. This software backup includes all build scripts, source code, preloaded system default data, and settings.

Database Transaction Journal

The real-time backup process that involves archiving and backing up the logical logs are features of Informix used at the SFIS Central Site. SFIS archives a copy of the entire Informix database that reflects the status of the data at a point in time, while the logical logs journal all transactions that modified the database tables since the last backup copy of the tables was made. The Informix logs are immediately written to DAT tape as they are journalized. The log table is written to tape during each archive nightly, as well as being included in each Informix automatic log as a transaction. These archive tapes and subsequent journal log tapes may be used to restore the database in the event of a system failure.

RFP OSI 2046 CURRENT SYSTEM

Online Data Backup

The Informix database is created with online mirror (backup) copies of all dynamic demographic and minutiae databases, as well as transactions waiting in queues. Additionally, backup copies of this database are written to tape daily with constant transaction logs also written to tape. Backup copies of the image database are also performed on a regular basis. RAID technology provides for active and inactive partitions. As partitions of the RAID fill, they are marked inactive. A full backup of these inactive partitions are made to tape. These partitions do not require additional backup procedures, though on a regular, but long interval schedule additional backups are taken. The active partitions are the target of incremental backups to tape on a daily basis. The image database is restored from the combination of full and incremental backups. The full backups of inactive RAID partitions are applied along with the last full backup of the active RAID partition. The incremental backups of the currently active RAID partition are then applied in fully recovering the DIRs.

Transactions in process during a system failure will be automatically reintroduced from a previous checkpoint. Because all database processes are logged as the transaction "commits" to the database, the demographic and minutiae data added to the database since the last backup are available. The checkpoints taken provide fast recovery of the database tables. All the queue data is fully restored in this manner allowing transactions to be reintroduced from their position at the point of failure.

Offline Backup

All demographic data and minutiae data will be backed up to tape both as the transaction occurs in the Informix transaction log and as part of the nightly archive. Duplicate backup high capacity tape is stored off-site to safeguard data in the event of a major system failure.

The DIRs and Matching Subsystem contain data that is vital to SFIS operation. In addition to other data preservation methods (RAID-based image data storage, storage of memory-based minutiae and descriptor data in an online database, and RDBMS-based mirroring of the minutiae/descriptor database), a multi-generation tape backup procedure is employed, with off-site storage for all backup media as a standard safety precaution. The DIRs is equipped with a DLT tape drive, used for backing up image data. The Matching Subsystem is equipped with its own tape drives.

RFP OSI 2046 CURRENT SYSTEM

DIRs image data occupies a large amount of disk space. Using RAID logic, the image data is divided into smaller logical partitions in which, in a typical matching configuration, are approximately seventeen gigabytes (17GB) each. Only one (1) partition is designated as active at any one time, and incremental backups are performed on the data from this partition. As this partition is filled, it is designated inactive, and one or more full backups of that partition are created by the current Contractor System Administrator. Each partition takes approximately fifteen (15) minutes (incremental), and one (1) hour and seventeen (17) minutes (full) to back up using twenty gigabytes (20GB) DLT tapes.

Storage of Memory-based Minutiae and Descriptor Data in the Online Database

Minutiae and descriptor data are stored in the Matching Subsystem Random Access Memory (RAM), supporting real-time searches. Because the RAM-based minutiae/descriptor database is also retained in an online magnetic disk database, it can easily be used to reload the appropriate segment of the database for any matching component that requires corrective maintenance. This architecture provides an online backup of the minutiae and descriptor data files as well as normal archive capability.

Off-site Storage

Application software is stored with an escrow company. When the application software is modified, a copy of the modified application is provided to the escrow company. Multi-generation DLT backup tapes will also be stored off-site as a safety precaution to ensure all necessary and sufficient elements are available to completely rebuild the system.

Archive Audit Trails

SFIS logs multiple transactions to the SFIS database. Due to finite space on the database, the logged data will be archived to the DLT tapes periodically, then purged from the database. The archive tapes include the case history, operator logon, remote workstation transaction, and fraud transaction tracking.

For each of these archives the database table is unloaded to a file that is written to DLT tape using the OmniBack tape utility. The table below lists the database table name, the unload file naming convention, and the archive name. Note that the reference to *juliandate_year* in the naming convention is replaced by the actual Julian date and year in the file name. Each of these archives is copied to DLT tape monthly.

**RFP OSI 2046
CURRENT SYSTEM**

Database Table Name	Unload File Naming Convention	Archive Name
T06_cm_history	T06_CMHIST.UNLD. <i>juliandate_year</i>	Case History
T19_security_txn	T19_SECTXN.UNLD. <i>juliandate_year</i>	Operator Logon Transaction
T16_wrst_txn	T16_WRKTXN.UNLD. <i>juliandate_year</i>	Remote Workstation Transaction
T56_frdwrst_txn	T56_FWSTXN.UNLD. <i>juliandate_year</i>	Fraud Workstation Transaction

The following subsections describe each of these named archives further.

Case History

The following transactions related to the client case record will be logged on the Case Master History table.

- Add (Open Search);
- Update (Closed Search); and
- Update (Demographics).

Any of these events triggered by the Operator will be logged in the Case Master History and the Case History Log tables. A snapshot of the Case Master table will be taken after the information has been added or updated and logged on the Case Master History table including the Image Updated flag.

The daily batch program will archive the Case Minutiae table along with all image files captured for the day onto the DLT tape.

During the Month-end Batch Cycle, the data on the Case Master History table will be archived to the DLT tape then purged from the table. The session ID and file name for the archive will be stored on the Case Master Log table. If archive data is needed, the information is accessible from the DLT tapes and can be reloaded into a temporary version of the Case Master History table on the backup Database Server.

**RFP OSI 2046
CURRENT SYSTEM**

User Logon Transaction

The users perform logon and logout transactions. These transactions will be logged in the Operator Logon Transaction History table. The batch reporting programs use this table to produce the system reports. The Monthly Batch Cycle program will archive the Operator Logon Transaction History table to the DLT tape. This DLT tape will be created with only the user logon/logout transaction data to facilitate the access of the data. The table will be purged monthly after the archive program completes writing the tape.

Remote Workstation Transaction

The users perform the following remote workstation transactions:

- SFIS Inquire;
- File Clearance;
- Open Search Request;
- Closed Search Request;
- Update Priority in Queue;
- Remove Images (Online Delete); and
- Update Demographics.

Any of these transactions triggered by the user will be logged in the Remote Workstation Transaction History table. The batch reporting programs use this table to produce the system reports. The Monthly Batch Cycle program will archive the Remote Workstation Transaction History table to the DLT tape. This DLT tape will be created with only the remote workstation transaction data to facilitate the access of the data. The table will be purged monthly after the archive program completes writing the tape.

The inquire search criteria used in the SFIS Inquire and File Clearance functions will be recorded in this table. For example, if the Operator submits a File Clearance search on the Social Security Number (SSN), name, and date of birth, the data will be recorded.

The default setting on the remote workstation prints the Match Responses automatically. The county has the option to change the setting. The change in the default setting will be recorded in the table.

**RFP OSI 2046
CURRENT SYSTEM**

Fraud Workstation Transaction

The Fraud Investigators perform the following Fraud Workstation transactions:

- Fraud Query;
- Fraud Search;
- Fraud Inquire;
- Fraud Two CIN Search; and
- Restore.

Any of these transactions triggered by the Operator will be logged in the Fraud Workstation Transaction History table. The Monthly Batch Cycle program will archive the Fraud Workstation Transaction History table to the DLT tape. This DLT tape will be created with only the Fraud Workstation transaction data to facilitate the access of the data. The table will be purged monthly after the archive program completes writing the tape.

Additional Tables Archived to Tape

In addition to the audit trail information described in the previous subsections, other database tables are also archived to DLT tape. This archiving is in addition to the regular database backups used for potential database recovery. The other database tables are listed in the following chart. Each of the tables is unloaded to a file and the file naming convention is illustrated in the chart along with the archive frequency. Note that the reference to *juliandate_year* in the naming convention is replaced by the actual Julian date and year in the file name.

Database Table Name	Unload File Naming Convention	Archive Frequency
T02_csemin	T02_CSEMIN.UNLD	Daily
T11_stagng	T11_STAGNG.UNLD	Daily
T39_otoreq	T39_OTOREQ.UNLD	Daily
T04_matched	T04_MATCH.UNLD. <i>juliandate_year</i>	Monthly

**RFP OSI 2046
CURRENT SYSTEM**

Database Table Name	Unload File Naming Convention	Archive Frequency
T07_print	T07_PRINT.UNLD. <i>juliandate_year</i>	Monthly
T09_report	T09_REPT.UNLD. <i>juliandate_year</i>	Monthly

System Monitoring

The Informix database provides continuous logical logs of the system performance, which are monitored by Contractor staff. System monitoring is also accomplished by running programs that check whether or not processors are keeping up with their work. For instance, if completion codes in the match request records consistently indicate that a certain processor is not responding, the monitoring program notifies the console Operator of the condition.

CA-Unicenter

Another system monitoring tool utilized by the current Contractor is CA-Unicenter TNG application. The product provides a complete view of the system, integrating monitoring features for network management, hardware and software management, batch cycles, version control, virus control, and numerous other tasks. This information is integrated to provide a view of the system in its entirety, as well as an ability to drill down into individual components on the desktop.

The current Contractor use the following CA-Unicenter TNG components and options:

- **Remote Control Option (Computer Associates ControlIT)** – Controls remote PCs. This option enables System Administrators and Help Desk staff to assume control over one (1) or more desktop workstations from any remote location. For example, Administrators can restart Windows or log onto an NT server, simultaneously view several PCs, or have several end users simultaneously view one (1) PC.

RFP OSI 2046 CURRENT SYSTEM

- **Software Delivery Option** – Provides a centralized software library to house custom software, maintains a centralized record of software installed, provides event monitoring for software delivery, and automates the delivery of operating system and application upgrades.
- **Enterprise Discovery** – Automatically discovers the entire spectrum of technology assets and populates the object repository with the information identified about the various devices, their relationships, connections, and topology.
- **Network Security Option** – Centrally controls network traffic; authenticates and authorizes users; enables efficient security administration through centralized definition and consistent enforcement of security policies; detects and fends off attacks such as IP Spoofing and others; and provides notification of attempted security breaches and logging of attacks and failed logon attempts.

Recovery

The recovery process employed by SFIS allows reconstruction of database tables without re-entry of the data. Similar to the backup process, the recovery process can be divided into online and offline recoveries. Offline recovery is performed during off-hours, while the online recovery is performed during SFIS normal operating hours.

OFFLINE RECOVERY

The batch recovery process is initiated if all or some of the database tables become damaged during the off-hours of SFIS operations. The process uses files backed up during the nightly archive process to restore affected tables in the database. However, if tables became damaged during, or prior to, completion of the nightly archive process, backups of the database tables from the previous archive and log files that contain database table update transactions are used to recreate the database tables. Should the database be damaged, the evening batch cycle may not complete in time. Two (2) batch cycles will be performed the following evening. These recovery procedures enable the system to be ready for the next day's operation. The following steps describe the batch recovery process.

RFP OSI 2046
CURRENT SYSTEM

Case 1 - Off-hour Recovery After Backup Copies of Database Tables are Made

- Ensure that the database table space is in working order. Find alternative space if necessary.
- Define the table in the database.
- Using the backup copy of the database table from the current day, load the newly defined table.

Case 2 - Off-hour Recovery Before or During Backup Copies of Database Tables are Made

- Ensure that the database table space is in working order. Find alternative space if necessary.
- Define the table in the database.
- Using the backup copy of the database table from previous day, load the newly defined table.
- Mount the archive and logical logs for the day.
- Use the DB-Monitor program of Informix to restore the database table.
- Backup the restored database table for possible future use.

ONLINE RECOVERY

The online recovery process is used if all or some of the database tables become damaged during the day. This recovery process uses the most current copy of the database tables and log files containing the day's transactions to reconstruct the database tables up to the point when the system failure occurred. The recovery process includes redefining and loading the affected database tables with the most current backups and applying updates to the database tables from the log files, thus freeing SFIS users from re-entering data due to the system failure. The following illustrates the on-line recovery process.

RFP OSI 2046 CURRENT SYSTEM

ONLINE RECOVERY PROCESS

- Ensure that the database table space is in working order. Find alternative space if necessary.
- Define the table in the database.
- Using the backup copy of the database table from previous day, load the newly defined table.
- Mount the archive and logical logs for the day.
- Use the DB-Monitor program of Informix to restore the database table.
- Backup the restored database table for possible future use.
- Initiate the archiving and logical logging process.

After entering the system queues, transactions will not be lost if a system anomaly occurs that requires system restart. When the system is restarted, previously queued transactions will start with no System Administrator interaction. During Central Site downtime, the remote Operators will be able to continue acquisition, subject to the workstation's acquisition queue capacity.

The image database is also restored in a similar manner. The full backups of inactive RAID partitions are applied along with the last full backup of the active RAID partition. The incremental backups of the currently active RAID partition are then applied to fully recover DIRs.

RECOVERY FROM EQUIPMENT FAILURE

If any Central Site processor failure including communication equipment occurs, the network and hardware are reconfigured so that a spare processor assumes the processing duties of the failed processor. For example, should a matching supervisor fail, a spare matching supervisor in the local area network is reconfigured to handle the processing. Once the matching supervisor is activated, it resumes where the failed processor stopped.

The following steps describe the reconfiguration process:

RFP OSI 2046 CURRENT SYSTEM

- Activate the graceful shutdown process of the Informix system.
- Deactivate the failed processor by disconnecting communication cables.
- Reconfigure the spare processor to appear as the failed processor in the network.

Functions of the reconfiguration process are as follows:

- Update the spare processor's ID to the failed processors ID.
- Re-establish the network link to include the spare processor.
- Start the matching supervisor program on the spare processor.
- Bring up Informix to restore full data processing capabilities of SFIS.

DATABASE REORGANIZATION

The Matching Subsystem provided by Motorola/Printrak ensures that the entire database of minutiae and descriptor information can be completely reorganized in a short period of time. The loading of minutiae data into RAM for matching purposes allows the Matching Subsystem to not require regular lengthy database reorganizations. Database reorganization is only required when the number of match processors is expanded.

Deleted: Printrak

Should the database reorganization be required, fingerprint record entry can continue, as can review of already completed search results. Search results would simply be queued for the short period of time needed to reload data from magnetic disk into the adaptive match processors. Of course, any reorganization process can be performed during offline hours as well.

RFP OSI 2046
CURRENT SYSTEM

MOTOROLA/PRINTRAK AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AFIS)

Deleted: PRINTRAK

The heart of SFIS is the ability for capturing, storing, searching, and matching fingerprint images. The hardware and software acquired by the current Contractor from Motorola/Printrak is primarily responsible for delivering this functionality.

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

In the county offices, a remote capture PC workstation, an Identix TouchView scanner, and Motorola/Printrak software are required to capture the fingerprint image. Once the fingerprint image is captured, .bmp files are created. The Motorola/Printrak software manipulates the image to extract minutiae data to a FDP file, to create the thinned image file and to create the WSQ (Wavelet Scalar Quantization) compressed image file. The three (3) Motorola/Printrak files, the photo (.jpeg), and text file, are zipped together and sent to the Central Site. Later in the evenings, the raw bmp files are retrieved from the workstations.

Deleted: Printrak

Deleted: Printrak

Deleted: Printrak

With SFIS, fingerprint matching occurs two (2) ways, either through a Closed Search or through an Open Search. A Closed Search occurs when the Welfare applicant is believed to be known to SFIS (Not their first time to be imaged). The applicant's fingerprints are scanned and the Motorola/Printrak software on the Remote Input Workstation extracts the minutiae data. Using the recipient's CIN (Client Index Number), the Image Capture Workstation sends a request to the Central Site to locate the applicant's minutiae file stored in the DIRS database. The minutiae file is transmitted back to the workstation. Fingerprint matching occurs when the Motorola/Printrak software compares the two (2) minutiae files on the remote workstation. This is sometimes referred to as "one-to-one" matching. If a match is determined to exist (referred to as an "expected" result), the newly captured fingerprint image is reviewed for data quality, and if the newly captured image is of a higher quality than the file image, the file image at the Central Site is replaced with the new image. If the new image matches the old image, but is not of better quality, the file image will remain as it is. In either case, the photographic image is replaced on file in the Central Site database. A one (1) page-print out referred to as a "match response" is provided to the operator when the result is the expected result of Closed Search Match Found.

Deleted: Printrak

Deleted: Printrak

An Open Search occurs when the welfare client is not believed to be known to SFIS (First time to be imaged). The client's fingerprints are scanned and the images processed. The image files are transmitted to the Central Site where the Database Server coordinates the Open Search match process with the Motorola/Printrak subsystem. This is sometimes referred to as "one-to-many" matching.

Deleted: Printrak

At the Central Site, the Motorola/Printrak subsystem is comprised of three (3) main hardware components:

Deleted: Printrak

- Match Subsystem (CIC/ADS);
- Distributive Match Controller (DMC); and
- Expert Matcher (EM).

RFP OSI 2046 CURRENT SYSTEM

The Match Subsystem is a hardware and software combination that is responsible for storage, retrieval, and submitting searches of fingerprint images. The hardware is a redundant configuration of Compaq (now HP) Alpha 1200 servers and a Compaq StorageWorks disk subsystem. The two (2) Alpha systems are in a cluster configuration that allows for redundancy and workload sharing. Both systems have access to the fingerprint data stored on the StorageWorks disk subsystem. The two (2) Alpha systems are configured identically with:

- Dual Processor Alpha five hundred and thirty-three megahertz (533MHz) processors;
- One gigabyte (1GB) memory;
- One (1) twenty-seven gigabyte (27GB) disk drive;
- One (1) four millimeter (4mm) DAT tape drive;
- One (1) DLT 7000 tape drive;
- One (1) 10/100Mbps Ethernet NIC;
- Digital UNIX 4.0 (True64);
- Sybase Adaptive Server RDBMS version 11.9.2; and
- Motorola/Printrak Transaction Processor software.

Deleted: Printrak

The Match Subsystem runs two (2) software components, the ADS (Advanced Data Storage) responsible for storage and retrieval of fingerprint image information and the CIC (Civil ID Controller) responsible for submitting searches of the database.

Motorola/Printrak uses Sybase Adaptive Server version 11.9.2 as its database management systems. The fingerprint files managed by Motorola/Printrak are the minutiae data and thinned image files. The files are not stored within Sybase but are stored by the Tru64 file system on the StorageWorks disk subsystem. The Sybase database contains pointers to the fingerprint files.

Deleted: Printrak

Deleted: Printrak

The Motorola/Printrak StorageWorks subsystem uses RAID5 technology to protect the data. RAID5 spreads information across the disk drives such that the failure of any single drive will not result in a loss of data. If a disk drive fails, the information on the failed drive can be reconstructed from data on the remaining functional disk drives in the RAID5 set.

Deleted: Printrak

RFP OSI 2046 CURRENT SYSTEM

The StorageWorks subsystem contains eight (8) eighteen point one gigabytes (18.1GB) disk drives, seven (7) for production use and one (1) spare. That equates to one hundred and twenty-seven gigabytes (127GB) of raw disk space and ninety-five gigabytes (95GB) of usable disk space in a RAID5 configuration. Of the ninety-five gigabytes (95GB) usable, eighty-six gigabytes (86GB) are allocated for production. Of the eighty-six gigabyte (86GB) allocated for production, forty-three gigabytes (43GB), or fifty percent (50%), are currently utilized.

The Distributive Match Controller (DMC) manages the search and match transactions that are submitted to the AMPs. The SFIS system is configured with forty-five (45) AMPs plus two (2) spares. Each AMP is a Compaq 5500 server that is responsible for searching a portion of the minutiae data stored in the SFIS system. When each AMP server initializes, its portion of the minutiae database is read and loaded into memory. All searches are then performed against the data in memory.

The AMPs use geometric based matching to compare the location and orientation of the fingerprint minutiae between the search image and the in-memory image. The AMPs calculate a match score and return the results of their searches to the Distributive Match Controller. Potential matches, those with high match scores, are then forwarded to the Expert Matcher (EM).

The Expert Matcher is a hardware/software combination that simulates the verification process of a fingerprint expert. The Expert Matcher is a Compaq 5500 server running Windows NT and Motorola/Printrak Expert Matching software. The software uses the structural and graph based topological features of the minutiae and thinned image data to identify fingerprint matches.

Deleted: Printrak

The Distributive Match Controller, the Expert Matcher and all forty-seven (47) Adaptive Match Controllers are Compaq 5500 servers. With the exception of memory, all servers are identically configured as follows:

- 4-way five hundred and fifty megahertz (550MHz) processors;
- one gigabyte (1GB) memory (five hundred and twelve megabytes (512MB) in each AMP);
- nine gigabytes (9GB) disk drive;
- CD-ROM;
- 10/100Mbps Ethernet NIC; and
- Windows NT 4.0.

RFP OSI 2046 CURRENT SYSTEM

Accuracy

System Accuracy Requirements

SFIS met the accuracy requirements as defined by the initial RFP during the AFIRM Conversion. It appears that accuracy requirements defined by the initial RFP are also being met at this time.

Motorola/Printrak has developed a fingerprint image evaluation algorithm that automatically determines the quality of the fingerprint image captured by the Client Input Worker on the direct read fingerprint reader. If the fingerprint image is determined to be unacceptable, the software notifies the Client Input Worker, and also displays suggestions on improving the fingerprint image quality. The Client Input Worker must either capture an acceptable fingerprint or the system automatically exempts it. Because the system will not accept a fingerprint image that is determined to be unacceptable, the accuracy rate of the matching process is greatly improved.

Deleted: Printrak

Print-to-Print Search Accuracy Requirements

For all Open Search requests in which two (2) database fingerprint images correspond to the two (2) fingerprint images submitted for search, the SFIS produces a correct "Hit" indication at least ninety-seven point five percent (97.5%) of the time. This accuracy figure is met through a secondary matching process called EXPERT Matching which uses artificial intelligence techniques. EXPERT Matching replicates the process that a trained fingerprint technician would use to compare two (2) potentially matching fingerprints.

When both matching processes are used, the average accuracy rate for the automatic match/no match decisions is over ninety-seven point five percent (97.5%). These accuracy rates include both Type I (miss rate) and Type II (false match rate) errors.

In addition, Motorola/Printrak developed a fingerprint image evaluation algorithm that automatically determines the quality of the fingerprint image captured by the Client Input Worker on the direct read fingerprint reader. If the fingerprint image is determined to be unacceptable, the software notifies the Client Input Worker and also displays suggestions on improving the finger image quality.

Deleted: Printrak

RFP OSI 2046
CURRENT SYSTEM

For all Open Search requests in which there are no database fingerprint images that correspond to the two (2) fingerprint images submitted for search, SFIS produces a "No Match Found" indication ninety-eight point five percent (98.5%) of the time.

TWO-FINGER CLOSED SEARCH ACCURACY REQUIREMENT

For all Closed Search requests in which there are two (2) database fingerprint images associated with the search record and the correct database record was selected having two (2) useable fingerprint images corresponds to the fingerprint images submitted for search, SFIS produces a correct "Match Found" indication at least ninety-nine point nine percent (99.9%) of the time.

For all Closed Search requests made with two (2) fingerprint images and the database record selected for the match does not correspond to the search record, SFIS produces a "No Match Found" indication at least ninety-nine point nine percent (99.9%) of the time.

Single Finger Open Search Accuracy

For all Open Search requests in which there is one (1) database finger that corresponds to the one (1) finger submitted for search, SFIS produces a correct "Match Found" indication at least ninety-five percent (95%) of the time.

For at least fifty percent (50%) of all Open Search requests in which there are no database fingers that correspond to the one (1) finger submitted for search, SFIS produces a "No Match Found" indication or a candidate list with no more than one (1) candidate.

Single-Finger Closed Search Accuracy Requirement

For all Closed Search requests where the search request is made with one (1) fingerprint image and there is at least one (1) corresponding and useable fingerprint image record in the database, SFIS produces a correct "Hit" indication at least ninety-nine percent (99%) of the time.

For all Closed Search requests where the search request is made with one (1) fingerprint image and there is not a corresponding set of fingerprint image records in the database, SFIS produces a "No Match Found" indication at least ninety-nine percent (99%) of the time.

**RFP OSI 2046
CURRENT SYSTEM**

G. SYSTEM INSTALLATION

COUNTY SITE PREPARATION

County Site preparation for SFIS is furnished by the State. The State installs the equipment in such a manner as to ensure that the equipment operates correctly and efficiently, and to ensure that it is adequately protected from fire and water damage. The State requires that for each remotely located workstation that is installed, the following is available:

- Power - one (1) one hundred and twenty (120) vac/20 amp circuit with a four (4) plex receptacle;
- Communications - communication connection to the LAN/WAN is one (1) RJ45 receptacle; and
- Cable - CAT V.

Installation Sites

SFIS remote workstations are installed at approximately two hundred and seventy-five (275) county Sites. All installations are in accordance with applicable laws, codes, ordinances and industry standards and conform to existing electrical system and wiring of the remotely located sites.

Office Relocations and Additions

Office Moves

Currently, the State is responsible for de-installation, moving, and reinstallation of all Contractor supplied items when an office is moved from one (1) location to another.

New Office Setup

Currently, the State is responsible for installation of all Contractor supplied items when a new office is established.

**RFP OSI 2046
CURRENT SYSTEM**

FLOOR PLANS

Remote Site Floor Plan

The current Remote Site floor plan is representative of a Remote Input Workstation installation at a county site. The floor plan includes the equipment and a workspace (e.g. desk) and chair for the workstation operator and a chair for the applicant. The current Contractor assumes the following minimum dimensions in working with this floor plan:

The workspace dimension (e.g., desk used by the workstation operator) is five feet (5') wide by three feet (3') deep;

The chairs used by the workstation operator and applicant have a dimension of twenty-seven inches (27") wide by twenty-four inches (24") deep ; and

Both the workstation operator and applicant will be seated during SFIS processing.



Exhibit: Remote Site Installation

Central Site Floor Plan

The Central Site system is installed at the DTS South Annex (formerly known as HHSDC South Annex) location in Sacramento, California. The current Contractor installs, tests, and provides maintenance of all Central Site equipment at the SFIS Central Site. The current Contractor's floor plan for the Central Site includes all space and/or equipment needed by Central Site Contractor personnel.

RFP OSI 2046 CURRENT SYSTEM

The raised floor space occupied by the Central Site equipment includes seven hundred and seventy (770) square feet of space. The floor space for the Central Site equipment is shown in an additional Exhibit below.

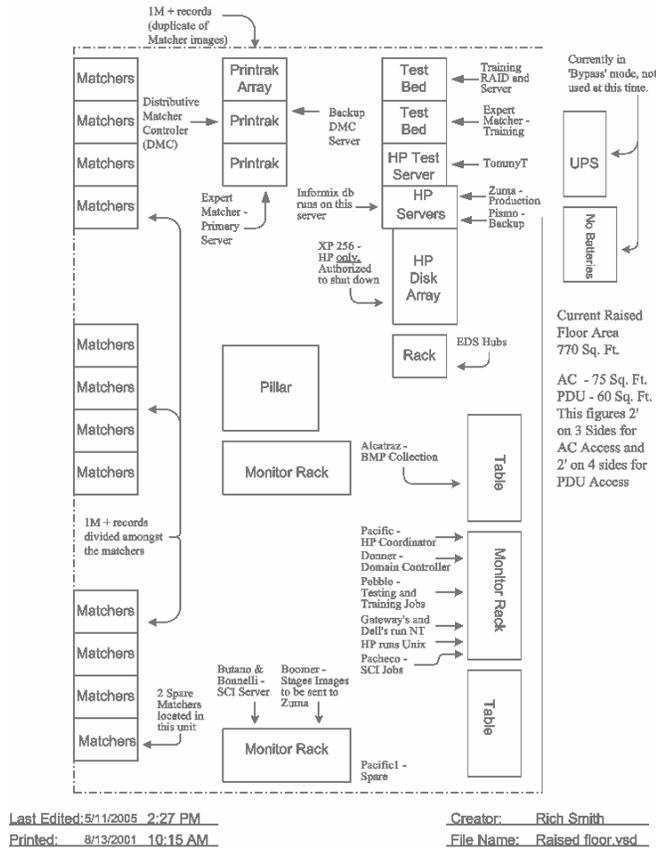


Exhibit: Central Site System Equipment Floor Plan

**RFP OSI 2046
CURRENT SYSTEM**

Environmental Requirements

The current Contractor complies with all federal, State, and local laws for the Central Site equipment and the county Site installations.

Qty.	Hardware	Location	Requirements by Unit				
			KVA	BTU/HR	Pounds	Temp.(°F)	% of Relative Humidity
2	RAID Cabinet (DSR 2000) ^a	Central Site	0.5	1,125	956	63° - 82°	50+-30%
11	AMP Cabinet (SP 2000) ^b	Central Site	0.8	2,730	723	63° - 82°	50+-30%
4	Match Server Cabinet (DSR, SP 2000) ^c	Central Site	0.5	1,125	613	63° - 82°	50+-30%
2	Motorola/Printrak Test Bed Cabinet^d	Central Site	0.85	2,955	615	63° - 82°	50+-30%
2	Database Server (HP9000/K460) ^e	Central Site	1.02	3,481	174	41° - 104°	15 - 80
1	Database Disk Cabinet ^f	Central Site	0.87	3,000	110	41° - 104°	15 - 80
1	Test Database Server	Central Site	0.8	2,730	110	41° - 104°	15 - 80
12	Process Coordinators	Central Site	0.3	1,023	223	41° - 104°	15 - 80
1	Test Process Coordinator ^h	Central Site	0.3	1,023	41	41° - 104°	15 - 80
1	Test Single Platter Optical ⁱ	Central Site	0.03	82	10	41° - 104°	15 - 80
1	DBA Workstation (HP9000/B132L+)	Central Site	0.3	1,023	41	41° - 104°	15 - 80
1	DBA Peripherals	Central Site	0.12	410	35	41° - 104°	15 - 80
2	Optical Jukebox ^j	Central Site	0.12	410	420	41° - 104°	15 - 80
2	Network Printer (Xerox DocuPrint N24)	Central Site	0.12	410	99	41° - 95°	15 - 85

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

Qty.	Hardware	Location	Requirements by Unit				
			KVA	BTU/HR	Pounds	Temp.(°F)	% of Relative Humidity
1	System Console (HP9000/B132L+)	Central Site	0.3	1,023	41	41° - 104°	15 - 80
1	Verification Workstation ^k	Central Site	0.2	683	35	35° - 104°	20 - 80
1	Test Remote Input Workstation	Central Site	0.2	683	35	35° - 104°	20 - 80
1	Test HP Laser Jet 2100	Central Site	0.12	410	17	41° - 95°	15 - 85
1	Test Identix Fingerprint Scanner	Central Site	0.0024	12	2	41° - 104°	15 - 80
1	Test Howard Enterprise Camera ^l	Central Site	0.0022	8	.3	41° - 104°	15 - 80
250	Remote Input Workstation ^m	Remote Site	0.2	683	35	35° - 104°	20 - 80
250	HP Laser Jet 2100 Printer	Remote Site	0.12	410	17	41° - 95°	15 - 85
250	Identix Fingerprint Scanner ^m	Remote Site	0.0024	12	2	41° - 104°	15 - 80
250	Howard Enterprise Camera ^m	Remote Site	0.0022	8	.3	41° - 104°	15 - 80

Exhibit: Environmental Requirements

^a The RAID Storage Cabinets (DIRS) contain the DSR server, as well as disk storage and tape backup for the DIRS. The cabinets hold the RAID Disks, and RAID Controller.

^b Each AMP Cabinet contains up to four (4) Adaptive Match Processors for the SP 2000 Matching Subsystem.

^c The Match Server Cabinets contain the Minutiae Match Controller, *EXPERT* Matchers, Transaction Processor, DIRS Server, and Minutiae Storage.

^d The Motorola/Printrak Test Bed Cabinets contain all the matching subsystem equipment, including the Minutiae Match Controller, *EXPERT* Matchers, Transaction Processor, DIRS Server, Adaptive Match Processor Spare, RAID Disks (DIRS) and RAID Controller.

^e The Database Servers include the Primary Database Server and the Secondary Database Server.

^f The Database Disk Cabinet is the dual ported disk attached to the Primary and Secondary Database Servers.

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

^g The Process Coordinator Cabinets contain the Image Coordinators, Match Coordinators, and Purge Coordinators.

^h The Test Process Coordinator runs the software designed as the Image Coordinator, Match Coordinator, and Purge Coordinator.

ⁱ The Test Single Platter Optical is attached to the Test Process Coordinator.

^j The Primary Optical Jukebox will be attached to one of the Purge Coordinators. The Spare Optical Jukebox acts as a backup production jukebox with a mirror image of the Primary Optical Jukebox.

^k The Verification Workstation listed here include the ongoing Verification Workstation to be located at DTS.

^l Howard Enterprise Camera environmental requirements include the rating for the lights.

^m Remote Input Workstations (and peripherals on lines following including the printers, Identix Scanners, and Photographic Cameras) include two hundred and forty-four (244) ongoing workstations, forty-two (42) initial load workstations, and six (6) additional workstations for Month sixty-five (65). The spare workstations and peripherals do not have environmental requirements at DTS or the County Offices, because they are stored at the EDS Maintenance Locations.

**RFP OSI 2046
CURRENT SYSTEM**

H. HARDWARE RELIABILITY

WORKSTATION RELIABILITY

Weekly Workstation Reliability

The workstation reliability is measured weekly (Monday through Friday) during actual in-use hours per workstation when the workstations are actually used by the State and/or counties. On a weekly basis, the system must achieve the following Workstation Reliability measurements:

- Each workstation' reliability is measured weekly (Monday through Friday) during operational hours when the workstations are actually used by the State and/or counties. The Average Workstation Reliability for all State and county-operated Workstations in SFIS is ninety-eight point five percent (98.5%);
- No more than five percent (5%) of the State and county-operated Workstations may have an individual average Workstation Reliability of less than ninety-five percent (95%); and
- No single State and county-operated Workstation may have a Workstation Reliability level below ninety percent (90%).

Workstation Key Components

Currently, the following conditions are considered as one hundred percent (100%) of the Workstation being down and count as one (1) Downtime Hour or fraction thereof for each hour that the condition continues:

- Failure or malfunction of any functionality normally available from the workstation.
- Failure or malfunction of any contractor-supplied communications equipment at the remote site workstation that causes the failure of communications between the workstation and the central site; This includes but is not limited to, any Live Scan Device that does NOT pass the Scanner Diagnostics Test or,
- Failure or malfunction of the Live Scan device (if one (1) is attached to the workstation). This includes, but is not limited to, the spotlight dimmer switch.
- Failure or malfunction of the Photo capture camera (if one (1) is attached to the workstation).

**RFP OSI 2046
CURRENT SYSTEM**

- Failure or malfunction of the workstation printer is considered as fifty percent (50%) of the Remote or Central Site Workstation being down and will count as one-half (½) Downtime Hour or fraction thereof for each hour that the condition continues.

Workstation Reliability Calculation

Currently, workstation Reliability is computed as follows:

Total Scheduled Hours - Total Adjusted Down time) / Total Scheduled Hours] x 100 = Workstation Reliability (expressed as a percentage)	Where Total Scheduled Hours = Sum of all scheduled operational hours for all State and county-operated SFIS workstations
Total Adjusted Down Time = Sum of all Adjusted Down Time hours for all State and county-operated SFIS workstations	

Total Scheduled Hours are Monday through Friday 7 a.m. to 7 p.m. Up time and down time must be calculated using these hours of operation, regardless of site operational hours.

Weekly Central Site Reliability

Central Site Reliability is measured weekly (Monday through Friday). Between the hours of 7 a.m. to 7 p.m. (or actual in-use hours when the system is used by the State outside of the period between 7 a.m. to 7 p.m.), Monday through Friday, during any given week, the average uptime percentage for the SFIS Central Site. The Average Uptime Percentage for the Central Site is ninety-eight point five percent (98.5%).

Central Site Primary (100%) Components

Currently, the following conditions are considered as one hundred percent (100%) of the Central Site being down and count as one (1) Central Site System Downtime Hour or fraction thereof for each hour that the condition continues:

- Failure or malfunction of the Central Site's contractor-supplied capability to maintain communications between the remote sites and the Central Site;

RFP OSI 2046 CURRENT SYSTEM

- Failure or malfunction of the Central Site's transaction log storage capability;
- Failure or malfunction of the RDBMS capabilities of the system;
- Failure or malfunction of the database management capabilities of the system;
- Failure or malfunction of the Central Site's capability to control the flow of transactions within the Central Site system; or
- Failure or malfunction of the Central Site's capability to support match verifications at the Central Site. If the system is configured with more than one (1) verification workstation at the Central Site and if one (1) (or more) of these workstations fail or malfunction, one (1) Central Site System Downtime Hour is computed as follows: (Number of Verification Workstations Failed / Total Number of Verification Workstations) x one hour = Central Site System Downtime Hour or fraction thereof for each hour that the condition continues.

Central Site Secondary (50%) Components

Currently, each of the following conditions is considered as fifty percent (50%) of the Central Site being down and counts as one-half ($\frac{1}{2}$) Central Site System Downtime Hour or fraction thereof for each hour that the condition continues:

- Failure or malfunction of the Central Site's capability to retrieve photo and/or fingerprint images; or
- Failure or malfunction of the Central Site's capability to perform image-to-image matching. If the system is configured with more than one (1) matching subsystem at the Central Site and if one (1) (or more) of these subsystems fail or malfunction, one (1) Central Site System Downtime Hour is computed as follows: (Number of Matching Subsystems Failed / Total Number of Matching Subsystems) x one-half ($\frac{1}{2}$) hour = Central Site System Downtime Hour or fraction thereof for each hour that the condition continues.

Central Site Reliability Calculation

The current Central Site Reliability is computed as follows:

**RFP OSI 2046
CURRENT SYSTEM**

Total Scheduled Hours - Total Adjusted Down time) / Total Scheduled Hours] x 100 = Central Site Reliability (expressed as a percentage)	Total Scheduled Hours = Sum of all scheduled operational hours for the Central Site
	Total Adjusted Down Time = Sum of all Adjusted Down Time hours for the Central Site

Test Bed System Reliability

Weekly Test Bed Reliability

Currently, the Test Bed System reliability is measured weekly (Monday through Sunday). The Average Uptime Percentage for the Test Bed System is ninety-eight percent (98%).

Test Bed Components

Currently, failure or malfunction of any system functionality in the Test Bed System is considered as one hundred percent (100%) of the Test Bed System being down and counts as one (1) Test Bed System Downtime Hour or fraction thereof for each hour that the condition continues.

Test Bed Reliability Calculation

Currently, the Test Bed System Reliability is computed as follows:

Total Scheduled Hours - Test Bed System Down Time) / Total Scheduled Hours] x 100 = Test Bed System Reliability (expressed as a percentage)	Where Total Scheduled Hours = Sum of all scheduled operational hours for the Test Bed System
Test Bed System Down Time = Sum of all Test Bed System Down Time Hours for the Test Bed System	

**RFP OSI 2046
CURRENT SYSTEM**

I. MAINTENANCE

The maintenance procedures that support SFIS ensure uninterrupted service to recipients of public assistance benefits. The current Contractor provides the SFIS maintenance support and procedures required by the State for the Central and Remote Sites (county and project management sites). This support includes:

- Software maintenance by phone, on site, and remotely managed through the SFIS Help Desk.
- Hardware maintenance by phone, on site, and remotely managed through the SFIS Help Desk.
- Maintenance reports.
- Preventive maintenance.
- Help Desk assistance.
- Personnel to coordinate with subcontractors and other providers.

As of June 2004, according to the Workstation Availability Summary Report (WAS), the average number of maintenance calls was twenty-three (23) calls per month, which is approximately one (1) call per workday. According to this report, the number of maintenance calls from users over the last two and one half (2½) years has decreased. A reported problem with the Remote Input Workstation scanner is the number one (1) call type.

Move, Add, Change (MAC's) requests occur at the rate of approximately one (1) per week, or approximately fifty (50) per year. The MAC requests may involve the current Contractor to configure a workstation, prepare the equipment for the install and/or update Contractor documentation (These requests do not include MAC calls that do not affect the Contractor such as router swaps, etc.).

MAINTENANCE AVAILABILITY

The current Contractor has maintenance service available twenty-four (24) hours a day, seven (7) days a week. A contact list has been provided to the State describing the process to access maintenance services both within and outside the principal period of maintenance.

**RFP OSI 2046
CURRENT SYSTEM**

PRINCIPLE PERIOD OF MAINTENANCE TIME-FRAME

The Principal Period of Maintenance (PPM) is defined as any twelve (12) consecutive hours per day, excluding holidays observed at the installation site. Service calls occurring within this period are covered by the current Contractor's basic monthly maintenance charges. The Principal Period of Maintenance time is from 7 a.m. through 7 p.m. Pacific Time, Monday through Friday on all regularly scheduled State workdays. The monthly maintenance charges for Maintenance Service Coverage are for this period. The Principal Period of Maintenance may be changed by the State upon thirty (30) days written notification.

Service calls initiated within the Principal Period of Maintenance are covered by the basic monthly maintenance charge. In this context, "initiated" is interpreted to mean that someone has placed a telephone call to the Help Desk telephone number and that either the Help Desk operator is reached or the person placing the Help Desk call is placed in the Help Desk queue. There are no additional charges for remedial maintenance during the Principal Period of Maintenance.

Currently, when remedial maintenance is required at any time other than during the PPM, response time is not normally any more than one (1) hour beyond the time allotted. The current Contractor is allowed to charge on an hourly basis for remedial maintenance outside of the Principal Period of Maintenance. There is no charge for remedial maintenance of a malfunction that occurred and was serviced within the previous forty-eight (48) hours, i.e. a "call back."

REMEDIAL MAINTENANCE (UNSCHEDULED)

The current Contractor provides remedial maintenance after notification by State staff, Help Desk staff, or county staff that hardware or software is inoperative, including replacement of failing remote or Central Site equipment. Qualified Maintenance Representatives who have the necessary tools and equipment maintain and provide repair or replacement of all installed hardware components when necessary, with the exception of State-owned equipment.

Remedial Maintenance Response Time Definition

The time for Maintenance Representatives to respond to a call for remedial maintenance is known as response time. This time is defined as the time interval between the time a trouble call is placed and the time Maintenance Representatives arrive at the site of the problem, exclusive of that time during which the Maintenance Representative is denied access to the equipment.

RFP OSI 2046 CURRENT SYSTEM

Off-line Maintenance Capability

An off-line maintenance capability is provided to allow the hardware to be tested for correct operation without the use of the central processing unit or its front-end controller.

When a workstation or server is turned on, the boot ROM (Read Only Memory) that contains general-purpose software that supports the operating system goes through several sequences to get the machine booted. The first thing it does is to perform the System Processing Unit (SPU) self-test. During this sequence, the boot ROM checks to see if the following components are functioning properly:

- RAM.
- Network Interface Card (NIC).
- Input/Output (I/O) subsystem including disk controllers and all ports.
- Display subsystem.
- Keyboard.

As a means of ongoing preventive maintenance, a camera calibration software module is initiated to check the fingerprint scanner's image quality. Whenever the scanner and Remote Input Workstation are booted, calibration software is used to adjust the scanner illumination to its required level. This calibration software automatically runs at startup and requires no operator intervention.

The laser printer includes off-line self-diagnostic routines internal to the printer. After the printer power is turned on, the printer goes through self-testing to ensure proper operation. This self-testing diagnostic may be used to perform off-line maintenance.

Maintenance Reports

The current Contractor documents all service calls and makes this documentation available to the State in the form of a Service Maintenance Activity (SMA) and Hardware Maintenance Report (HMR) illustrated in the Exhibits below. These reports list service calls and include the SMA and HMR Number.

RFP OSI 2046
CURRENT SYSTEM

The SMA lists the following:

- Problem tracking numbers (both the State and Contractor numbers).
- Date and time notified.
- Date and time of arrival.
- Site information.
- Problem description and resolution.
- Date and time repaired.

The HMR lists the following:

- Type, model, and serial number of equipment serviced.
- New equipment installed.
- Vendor assistance utilized.
- Time spent for repair.
- Description of malfunction.
- List of parts replaced.
- List of any outside repairs if needed.
- User certification, including date and time, of restoration of equipment to operational status.

The current Contractor delivers the SMA and HMR to the State upon completion of each service call.

**RFP OSI 2046
CURRENT SYSTEM**

Service Maintenance Activity (SMA)		SMA No.: <u>96</u>
Account: CA SIS: _____ (Enter location name)		
E D S 9300 Fair Drive, Suite 200, El Monte, CA 91731		
<i>Site Information:</i>		
Date: ____/____/____	Time: ____:____	Prepared By: _____
Address: _____		Contact: _____
City: _____	Floor: _____	Room: _____ Phone: (____) _____
Loc. ID: _____	Map Code: _____	Line ID: <u>L</u> <u>100</u>
Circuit ID: _____	-001	Switch 54: (____) _____
<i>Task Assignment:</i>		
Date/Time - Start: ____/____/____	:	End: ____/____/____
Islet No.: _____	PB Factor: _____	Phone: (____) _____
Seg/DAP No.: _____	GTE Factor: _____	Phone: (____) _____
<i>Problem Description:</i>		
YID: _____	RD: _____	Controller ID: <u>P</u> Notify CSD: <u>Yes / No</u>
		CSD Contact: _____
Time: _____		

<i>Resolution Description:</i>		
Time: _____		

<input type="checkbox"/> <u>Y/N</u> Equipment exchange (Log Serial Numbers on back of form)		<input type="checkbox"/> <u>Continued</u>
<i>Dispatch:</i>		
Dispatch Date: ____/____/____	Time Arrived: _____	Depart: _____
Check in with EDS Helpdesk: _____		System Up Time: _____
Customer Signature: _____		EDS Tech: _____
Customer Name (Print): _____		
<i>EDS Use Only:</i>		
Completed By: _____	Legal: _____	Inventory: _____ Manager Approval: _____

Exhibit: Service Maintenance Activity (SMA)

**RFP OSI 2046
CURRENT SYSTEM**

Hardware Maintenance Report (HMR)					HMR No.: 98 -	
<i>Hardware Exchange Inventory:</i>						
Device:	Term ID:	S/N of Device Removed:	S/N of Device Installed:	Inv. Update	Test:	
#1				Yes / No	Y / N	
#2				Yes / No	Y / N	
#3				Yes / No	Y / N	
Record AFIRM SPU S/N:			////////////////////////////////////			
<i>NOTE: HP SPU serial number also required for, Monitor, VideoLive Card, Keyboard & Mouse exchange.</i>						
Vendor Repair Assistance Device #1:						
Date/Time--Called: ____ / ____ / ____		: ____		Prepared By: _____		
Date/Time--Arrived: ____ / ____ / ____		: ____		Departed: ____ / ____ / ____		
Vendor: _____		Serial No.: _____		Phone: (____) _____		
Model: _____		New S/N: _____		Ticket No.: _____		
Date/Time:	Problem Description:					
Date/Time:	Resolution Description:					
	<input type="checkbox"/> Y / N <input type="checkbox"/> Tested					
Vendor Tech Signature:			Date:			
Outside Repairs:						
Date Shipped: ____ / ____ / ____		Returned: ____ / ____ / ____		Tested In-House: ____ / ____ / ____		
Vendor Repair Assistance Device #2:						
Date/Time--Called: ____ / ____ / ____		: ____		Prepared By: _____		
Date/Time--Arrived: ____ / ____ / ____		: ____		Departed: ____ / ____ / ____		
Vendor: _____		Serial No.: _____		Phone: (____) _____		
Model: _____		New S/N: _____		Ticket No.: _____		
Date/Time:	Problem Description:					
Date/Time:	Resolution Description:					
	<input type="checkbox"/> Y / N <input type="checkbox"/> Tested					
Vendor Tech Signature:			Date:			
Outside Repairs:						
Date Shipped: ____ / ____ / ____		Returned: ____ / ____ / ____		Tested In-House: ____ / ____ / ____		
EDS Use Only:						
Completed By: _____		Logged: _____		Inventory: _____		Manager Approval: _____

Exhibit: Hardware Maintenance Report (HMR)

**RFP OSI 2046
CURRENT SYSTEM**

Maintenance of Additional Equipment

The current Contractor maintains any and all Contractor supplied additional equipment that has been or will be ordered/installed during the term of the current SFIS Contract.

Equipment Replacement

Leased or purchased machines, which fail to function in the manner for which they were designed and contracted for such that the State's programs are adversely affected, are replaced at the State's request. Before requesting replacement, the State attempts to satisfactorily resolve the problem with the Contractor. The State is the sole judge as to the adverse impact upon State programs of non-functioning equipment requested for replacement; however, the State does not act in an arbitrary or capricious manner.

Reliability Improvement Notices

All reliability improvements that are released by the Contractor or manufacturer for the same type of equipment as being maintained under the terms of a maintenance contract are provided by contractor and made with the consent of and without additional charge to the State during the period of any maintenance contract.

CENTRAL SITE MAINTENANCE

Hardware and Software Maintenance

The current Contractor has maintenance and support contracts in place with all of the major vendors of the hardware and software in use at the Central Site. The current Contractor is responsible for working in cooperation with the representatives of hardware manufacturers or suppliers, software developers or suppliers, and the DTS Telecommunications Division to diagnose and resolve any problems.

Preventive Maintenance

Software maintenance occurs as upgrades are received from the various commercial off-the-shelf (COTS) software vendors and at the State's request and agreement.

**RFP OSI 2046
CURRENT SYSTEM**

The table below details the frequency and duration of the preventive maintenance procedures. The Exhibit describes the preventive maintenance procedures that are performed by current Contractor personnel.

<i>CENTRAL SITE - Servers and Coordinators</i>		
Check wiring and cable connections	Monthly	Two (2) minutes
Verify server labeling is visible	Daily	One (1) minute
Ensure equipment vents are dust free	Monthly	One (1) minute
Clean monitor screens	Monthly	Two (2) minutes
Clean mouse ball and buttons	Monthly	One (1) minute
Spray keyboard with compressed air	Monthly	One (1) minute
Ask database administrator for any recent occurrences of difficulties or problems	Daily	Five (5) minutes
Advise database administrator on any potential problems in the area (i.e. coffee, stickers covering vents, etc.)	Daily	Five (5) minutes
Perform file system check	Weekly	Sixty (60) minutes
Perform disk space-availability check	Daily	Five (5) minutes
Perform database space-availability check	Daily	One (1) minute
Run database utilities to determine if indexes are intact	Weekly	Sixty (60) minutes
Perform tape drive cleaning	Monthly	Ten (10) minutes
Perform number-of-database table-extent check	Weekly	Thirty (30) minutes
Perform defunct process removal	Weekly	Ten (10) minutes
Display database server process messages for warnings	Daily	Two (2) minutes
Monitor database server operation efficiency	Daily	Two (2) minutes
<i>CENTRAL SITE - Matching Subsystem</i>		
Back up MMC transaction log	Daily	Ten (10) minutes
View and purge system log files	Weekly	Ten (10) minutes
Verify adequate free disk space	Weekly	Five (5) minutes
Remove core dump files	Weekly	Five (5) minutes
Back up MMC RDBMS files	Weekly	Two (2) hours

**RFP OSI 2046
CURRENT SYSTEM**

Initialize all transaction processing queues	Weekly	Fifteen (15) minutes
Perform full backup of current writeable partition	Monthly	Five (5) hours
Verify integrity of RDBMS database tables	Monthly	Sixty (60) minutes
Clean all terminal screens	Monthly	Five (5) minutes
Clean all tape drives	Monthly	Five (5) minutes
Verify all fans are operational	Monthly	Ten (10) minutes
Verify CPU operation	Quarterly	Fifteen (15) minutes
Vacuum inside of computer chassis	Quarterly	Thirty (30) minutes
<i>CENTRAL SITE - Image Retrieval System</i>		
Back up Informix transaction log	Daily	Five (5) minutes
Perform incremental image file backup	Daily	Ten (10) minutes
Check integrity of new object additions by date	Daily	Ten (10) minutes
View and purge system log files	Weekly	Ten (10) minutes
Verify adequate free disk space	Weekly	Five (5) minutes
Remove core dump files	Weekly	Five (5) minutes
Back up Informix files	Weekly	Sixty-five (65) minutes
Initialize all transaction processing queues	Weekly	Fifteen (15) minutes
Synchronize minutiae and image databases	Weekly	Five (5) hours
Verify integrity of RDBMS database tables	Monthly	Sixty (60) minutes
Verify integrity of image objects	Monthly	Forty-five (45) minutes
Clean all terminal screens	Monthly	Five (5) minutes
Clean all tape drives	Monthly	Five (5) minutes
<i>CENTRAL SITE - Image Retrieval System</i>		
Verify all fans are operational	Monthly	Ten (10) minutes
Verify CPU operation	Quarterly	Fifteen (15) minutes
Vacuum inside of computer chassis	Quarterly	Thirty (30) minutes
Create complete archive backup every two (2) years/as needed using	Once every	Five (5)

**RFP OSI 2046
CURRENT SYSTEM**

new tape media	two (2) years	hours per partition
----------------	------------------	------------------------

Exhibit: Preventive Maintenance Procedures

Though the image and feature data are synchronized on a continuous basis, they reside on separate special-purpose subsystems allowing for the possibility that data in the databases could become unsynchronized. Although mis-synchronization of the databases is rare, the current Contractor runs the database synchronization program (DB_SYNCH) weekly in order to ensure that no problems exist. In the rare instance that such a problem may exist, the record is resynchronized with no loss of data.

In the event that a malfunctioning Motorola/Printrak matcher unit is discovered during preventive maintenance, the current Contractor personnel store replacement Matchers to be used to replace defective matchers.

Deleted: Printrak

Central Site Remedial Maintenance

Maximum response time for Central Site remedial maintenance to hardware or software does not normally exceed one (1) hour. Further, in the event of a malfunction within any component or components of the Central Site system, the Central Site system is normally restored to full operational status within two (2) hours of the time of the original system failure.

Spare equipment for Motorola/Printrak components at the Central Site are available to ensure that these malfunctioning components can be quickly replaced, returning the system to full use. These spare components are included on the floor plan description of this document.

Deleted: Printrak

Backup subsystems are available for the following subsystems:

- Database Server;
- Process Coordinators;
- Image Coordinators
- Match Coordinators
- Purge Coordinators
- DBA Workstation;
- Network Printers;
- System Console;

**RFP OSI 2046
CURRENT SYSTEM**

- Verification Stations;
- Motorola/Printrak Subsystems;
- Background Database Extraction Subsystem
- Matching Subsystem
- Digital Image Retrieval Subsystem.

Deleted: Printrak

Periodic System Checks

The current Contractor has created and implemented a set of procedures and a plan to ensure that all security measures are operational, and that all hardware and software is functioning correctly. Periodic system checks are performed at least daily; these procedures do not degrade system performance to the extent that the system cannot meet the current Contract requirements. A Periodic System Check Procedures checklist is illustrated in the Exhibit below, "Periodic System Check Procedures." This checklist is used by the System Operators daily to verify that all security measures are operational and that all hardware and software is functioning correctly. Each morning the System Operator performs each procedure on the checklist that is scheduled for that day, initialing the appropriate box to indicate completion of the task. The System Operator also performs each security procedure on the checklist to ensure that all workstations and servers are secure at the completion of on-line processing. Shaded boxes indicate that a particular task is not performed on that day.

In addition to tasks performed at the Central Site by the System Operators, Contractor Central Site workstation operators perform a variety of checks at their workstation. These tasks are described by workstation type in the Exhibit below.

<p>SPARE WORKSTATION Verify password protection during logon Verify multiple logon not possible Verify ability of SFIS application to access database server Verify ability of matchers to respond by entering a "no store" transaction SCI Interface is Available by Requesting a File Clearance Verify operation of DIRS by performing an Inquire transaction Verify that Spare Remote Workstation is secure after testing is complete</p>
<p>DATABASE SERVER Verify password protection during logon Database is Online Verify transaction logging is in progress Verify that queues are being processed Perform disk space availability check</p>

**RFP OSI 2046
CURRENT SYSTEM**

<p>Perform database space availability check Display database server process messages for warnings Monitor database server operation efficiency Verify that database terminal is secure and no user is logged in as root or Informix</p>
<p>PROCESS COORDINATORS Verify password protection during logon Verify Image Coordinators are Online Verify that Image Coordinator terminals are secure and no user is logged in as root Verify password protection during logon Verify Match Coordinators are Online Verify that Match Coordinator terminals are secure and no user is logged in as root Verify password protection during logon Purge Coordinators are Online Verify that Purge Coordinator terminals are secure and no user is logged in as root</p>
<p>VERIFICATION WORKSTATION Verify password protection during logon Verify that workstations are Operational and Verify Operators Present Verify that Unused Verification Stations are Secure and no user is logged in</p>
<p>SYSTEM CONSOLE Verify password protection during logon Verify that System Console is Operational Verify that System Console is Secure (if not currently in use by authorized personnel)</p>
<p>WORKSTATION Verify password protection during logon Verify that DBA Workstation is Operational Verify that DBA Workstation is Secure (if not currently in use by authorized personnel)</p>
<p>WORK CONNECTION Check network control monitor to verify communication to each sites</p>
<p>WORK PRINTERS Verify that network printers are Online and without error messages</p>
<p>MATCHING SUBSYSTEM Verify password protection during logon Back up MMC transaction log View and purge system log files Verify adequate free disk space Remove core dump files Verify that Matching subsystem terminals are Secure and no user is currently logged on</p>
<p>IMAGE RETRIEVAL SUBSYSTEM Verify password protection during logon Check integrity of new object additions by date View and purge system log files Verify adequate free disk space Remove core dump files Verify Image Retrieval terminals are Secure and no user currently logged on</p>
<p>AM MANAGEMENT WORKSTATION SFIS with user name and password If applicable, check optional printer paper supply; print test reports Maintain work area: ensure it is free of dust, cables are secured, no soft drinks, etc in the area</p>
<p>VERIFICATION WORKSTATION SFIS with user name and password If applicable, check printer paper supply; print test report Maintain work area: ensure it is free of dust, cables are secured, no soft drinks, etc in the area</p>
<p>REMOTE INPUT WORKSTATION SFIS with user name and fingerprint image Verify scanner lens is clear and free of debris before first fingerprint capture Verify photo image is clear and lens is free of lint and debris before first photo capture</p>

RFP OSI 2046 CURRENT SYSTEM

Run scanner diagnostic test (select Scanner button from Welcome Menu)
Check printer paper supply; print test report/response (Not on Portable)
Maintain work area: ensure it is free of dust, cables are secured, no soft drinks, etc in the area

Exhibit: Periodic System Check Procedures

In addition, the System Operation and Support Plan (SOSP) is updated as System Check processes and procedures change, and includes the periodic system check procedures along with other preventive maintenance procedures and regular tasks necessary to support the operation of SFIS.

Remote Site Maintenance

Preventative Maintenance

The remotely located SFIS workstation operator is expected to perform some preventive maintenance tasks to help maximize equipment performance including:

- Maintain a dust free work area (daily).
- Ensure a liquid free work area to prevent equipment from getting wet (daily).
- Keep the equipment vents open to allow cool air to ventilate equipment during operations (daily).
- Clean scanner platen with scanner cleaning wipes (daily – white wipes).
- Any hardware problems that a remote workstation operator may encounter are usually reported immediately by calling the Help Desk.
- Run Scanner Diagnostic tests (weekly).

**RFP OSI 2046
CURRENT SYSTEM**

Level of Maintenance Support

The current Contractor maintains a level of system operation during the Principal Period of Maintenance. The current Contractor provides services for those sites located within a forty (40) mile radius of City Hall in any Maintenance City, a maximum response time not to exceed two (2) hours. For those sites located outside of the forty (40) mile radius of City Hall in all other Maintenance Cities an extra one-half (½) hour is allotted for each additional twenty (20) mile increment. At no location shall the response time exceed eight (8) hours.

Contractor Maintenance Representatives have spare equipment available for remote sites in sufficient quantity to replace failing workstations with spare workstations so that the failing workstations can be brought back to the Maintenance Location for repair. The Representatives receive pre-configured workstations with the current application version from the current Contractor. The Representatives connect to the Central Site once the workstation is set up. After connectivity is established, the current Contractor ensures all files etc. are configured correctly and updates them if necessary. This replace-and-repair approach to hardware maintenance returns the remote workstation to normal operations instead of attempting a repair at the site while the workstation operator waits for a usable workstation. The current Contractor inventories the locations of all equipment when replaced to be able to locate any specific item. Help Desk personnel monitor SFIS to ensure availability and response to equipment problems.

The following current characteristics pertain to remedial maintenance of the SFIS equipment or software that is not contained within the Central Site system.

The maximum response time will vary depending on the problem site location distance from City Hall in the nearest city listed in the Table below.

Anaheim	Bakersfield	Fresno
Los Angeles	Marysville	Monterey
Oakland	Redding	Sacramento
San Bernardino	San Diego	San Francisco
Stockton	San Jose	Riverside

Exhibit: City Hall List

RFP OSI 2046
CURRENT SYSTEM

For those problem sites located within a forty (40) mile radius of City Hall in any city listed in the above Table, the maximum response time does not exceed two (2) hours. For those problem sites located outside of the forty (40) mile radius of City Hall in any city listed in the Table above, an extra one-half ($\frac{1}{2}$) hour is allowed for each additional twenty (20) mile increment. At no location does the response time exceed eight (8) hours.

Replacement Part Quantity

The current Contractor stocks at least ninety percent (90%) of replacements parts at all maintenance sites on an on-going basis for workstation components, and provides replacement parts within the required response time. Ninety percent (90%) of replacement parts” is defined as the greater of:

- Ninety percent (90%) of all replacement parts that are estimated to fail in all SFIS components serviced by a particular maintenance site within one (1) month, or
- Ninety percent (90%) of non-redundant unique equipment pieces that comprise SFIS components that are serviced by a particular maintenance site.

Replacement Part List

The current Contractor provides the State Project Manager with a list of replacement parts at each maintenance site on a quarterly basis. This list shows an inventory of at least ninety percent (90%) of replacement parts. At any time, the list of replacement parts includes all items that have failed at two percent (2%) or more of all SFIS workstations within the past twelve (12) month period.

**RFP OSI 2046
CURRENT SYSTEM**

J. SYSTEM WORKLOAD AND THROUGHPUT

DATABASE SIZE

SFIS was sized to support fourteen million (14M) sets (both the left and right index fingers) of fingerprint images and associated descriptor data. Currently, there are approximately three point five million (3.5M) sets in the database, which is roughly twenty-five percent (25%) of capacity.

AVERAGE MONTHLY WORKLOAD

The average monthly workload for CLOSED SEARCHES is approximately 60,000 and the average monthly workload for OPEN SEARCHES is approximately 30,000.

RESPONSE TIME

The system processes forty-five hundred (4.5K) to five thousand (5K) fingerprint transactions per day. That is an average of eighteen point five (18.5) transactions per Client Input and Multifunction Workstation. There are about one point five (1.5) times as many Closed Searches as Open Searches. In 2004, the average Open Searches equaled twenty-eight thousand three hundred and forty-two (28,342) per month and the average Closed Searches equaled forty-six thousand two hundred and nine (46,209) per month. Approximately one hundred and fifty (150) transactions per day are routed to the fingerprint verifiers.

In March to May of 2004, the Counties flagged the Open Searches for priority processing as follows:

- Priority = seventy-three point one percent (73.1%)
- Normal = twenty-six point eight percent (26.8%)
- Conversion = point one percent (.1%)

Priority fingerprint transactions including verification transactions are to be completed within fifteen (15) minutes. On average, these complete in two (2) minutes. The current system is well within the contract requirements for response time.

Normal searches are completed by 7 a.m. the next day. Normal searching is performed both after online hours and during online hours when there are no Priority transactions in the queue. The current system is well within contractual requirements for response time.

RFP OSI 2046
CURRENT SYSTEM

Conversion search transactions are completed by 7 a.m. the next business day one (1) calendar week after the search was received at the Central Site for processing. The current system is well within the contract requirements for response time.

Currently, all remote and Central Site activities are completed within the allotted time, including fingerprint processing, transmission of images and data, primary search processing, *EXPERT* (secondary) match processing, and returning of the match/no match response to the remotely located site printer.

Processing is done in a distributed environment with each Client Input, System Administration, and Multifunction Workstation accomplishing much of its own processing with local programs. The Client Input, System Administration, and Multifunction Workstations provide hardware and networking capability and are designed to optimize system reliability, storage, transmission capability and central processing unit (CPU) throughput. The Client Input, System Administration, and Multifunction Workstation processing includes quality verification that finger images captured at the workstation are of adequate quality for matching. These workstations also locally edit all biographical data, extract finger image-minutiae points, perform closed matching, and perform data compression. Once the local programs complete processing, each workstation connects to the Central Site for additional processing.

The Central Site includes design features that increase the speed of the matching process. The fingerprint image database is partitioned into multiple subsets so that matching can occur on each partition of the fingerprint image database simultaneously.

The system has five (5) minutiae match controllers (MMC) and forty-seven (47) Adaptive Match Processors (AMPs) (forty-five (45) active and two (2) hot spares). The MMC controls the AMPs and compiles lists of candidates being returned. The candidates are then forwarded to an additional matching process that utilizes neural network technology. This additional step, known as *EXPERT* Matching, emulates the verification process of a fingerprint expert.

When a search is submitted, the AMP uses geometric-based matching to compare the location and orientation of fingerprint minutiae (or feature points) between the search print and the file print. The AMP calculates a match score for each search print against file prints from the database. High match scores are candidates for the true match. The objective of the *EXPERT* Matcher is to apply a very detailed matching process to the search print and each of the top N number of file prints in the respondent (or candidate) list in order to boost the match score of the correct candidate and move it to the top of the list.

RFP OSI 2046 CURRENT SYSTEM

By incorporating the [Motorola/Printrak](#) proprietary *EXPERT* Matcher, the need for a Verification Technician to manually review post-search results has been reduced. The *EXPERT* Matcher process is based on cognitive theory and makes use of structural and graph-based topological features such as minutiae type, minutiae neighbor similarity, minutiae connectivity, minutiae constellation matching, distance-based ridge count similarity, ridge-trace similarity and ridge-flow similarity. These feature comparison processes are the same skills that the Verification Technician would use to visually compare two (2) side-by-side images. To accomplish these processes, the *EXPERT* Matcher requires the extracted minutiae as well as the thinned image (skeleton) for each print. This data is extracted by the [Motorola/Printrak](#) AFP and is stored as compressed data within the *EXPERT* Match RAID that allows rapid retrieval and processing. Adequate *EXPERT* Match processors are designed into the system in order to accomplish the required workload within the available time. Typically, candidates are compared by the matching subsystem within twenty (20) seconds.

Deleted: Printrak

Deleted: Printrak

The system has four (4) *EXPERT* Matching Processors, which provides a performance reserve of approximately ten percent (10%).

The design of the matching subsystem allows the peak load to be increased by adding individual matching components, thus increasing the number of matching database partitions.

The current Contractor actively monitors performance of the SFIS production environment. System operators and administrators have access to a number of online, real-time monitoring tools for the servers, Informix database and [Motorola/Printrak](#) subsystem. Upon review of the real-time monitor, the current Contractor stated that the HP Database Server is approximately ten percent utilized.

Deleted: Printrak

The current architecture of the Central Site provides for the expansion of capacity should it become necessary. The current Database Server can be scaled vertically by adding up to eight (8) processors. The current Process Coordinator Workstations can scale vertically by adding a processor. The [Motorola/Printrak](#) AFIS is also capable of vertical scaling within each server and horizontal scaling of the AMP servers.

Deleted: Printrak

Both disk storage subsystems are capable of adding capacity should it become necessary. The HP XP256 Disk Array can expand over nine (9) times to nine terabytes (9TB).

**RFP OSI 2046
CURRENT SYSTEM**

Simultaneous Entries

The current SFIS configuration is capable of responding to simultaneous entries from all workstations. The HP 9000 N4000 Database Server with four gigabytes (4GB) High Density SyncDRAM Memory is sufficiently sized to respond to all workstations simultaneously.

Concurrent Transaction Processing

SFIS processes other types of transactions including Image Retrieval and File Clearance concurrently with the Open and Closed Search workloads.

SFIS has been designed to handle the daily workload and if this workload should be exceeded, the system's modular design allows for expansion as the workload increases.

Though expandable, additional components would need to be added to the configuration once the system limitations shown in the Exhibit below are reached. For example, the configuration can support growth in the proposed database chassis or introduction of a multiple Database Server design should the system limitation of seven point six million (7.6M) clients be exceeded.

Subsystem	Capacity
Database Server	Fourteen million (14M) client records
Process Coordinators	Fifty-four hundred (5400) transactions per hour
Network Printers	Twenty-four pages per minute (24ppm)
Verification Stations	Fifty-four (54) match verifications per fifty (50) minute hour
Matching Subsystem	Fourteen million (14M) records Sixty-two (62) transactions per fifteen (15) minutes
EXPERT Matcher	Fifty (50) candidates per search at a rate of Five (5) seconds per search
DSR 2000 (Server/RAID)	Fourteen million (14M) records

Exhibit: System Limitations

RFP OSI 2046 CURRENT SYSTEM

The Database Server plays an integral role in the processing of SFIS transactions, including the receiving and responding to the remotely located workstations, transaction logging and queuing activities. The Database Server and process coordinators have an overall throughput of fifty-four hundred (5,400) transactions per hour. Because of this possible bottleneck, the central site configuration, as illustrated on the Exhibit below "SFIS CENTRAL SITE CONFIGURATION" diagram, includes process coordinators to off-load many of the functions from the Database Server. This off-loading is a component of handling incoming requests from the remotely located workstations.

The Database Server is configured for redundancy and consists of two (2) HP9000/N4000 systems. The two (2) systems are in a Primary (active) and Secondary (hot-standby) configuration. The HP9000/N4000 configurations are identical and include:

- Four (4) PA-8500, three hundred and sixty megahertz (360Mhz), sixty-four (64) bit processors (expandable to eight (8));
- Four gigabyte (4GB) memory (expandable to sixteen gigabyte (16GB));
- Eighteen gigabytes (18GB) internal disk drive;
- Four millimeter (4mm) DAT tape drive;
- CD-ROM;
- Dual 10/100Mbps Ethernet NIC (only one (1) used in production);
- Dual Fiber Channel adapters for connectivity to the HP XP256 storage array; and
- HP-UX 11.0 Operating System.

Process coordinators have the capability to handle fifty-four hundred (5,400) transactions per hour. Should the process coordinators become a bottleneck in the system, additional process coordinators may be placed into production to redistribute the workload and increase throughput capability.

RFP OSI 2046 CURRENT SYSTEM

For example, the matching subsystem processes Open Search transactions with minimal interaction from the Database Server because of the match coordinator. The Database Server maintains the queues that are accessed by the match coordinators. The match coordinator retrieves the top ten Priority searches from the queue and presents them to the matching subsystem, thus minimizing the number of database transactions by preventing each individual AMP from accessing the queue. Each AMP returns the candidates for the search as they complete to the match coordinator. The match coordinator compiles the various responses and posts the candidates on the appropriate verification queue as they are received. Again, only one (1) posting to the database per search is done to update the verification queue and status.

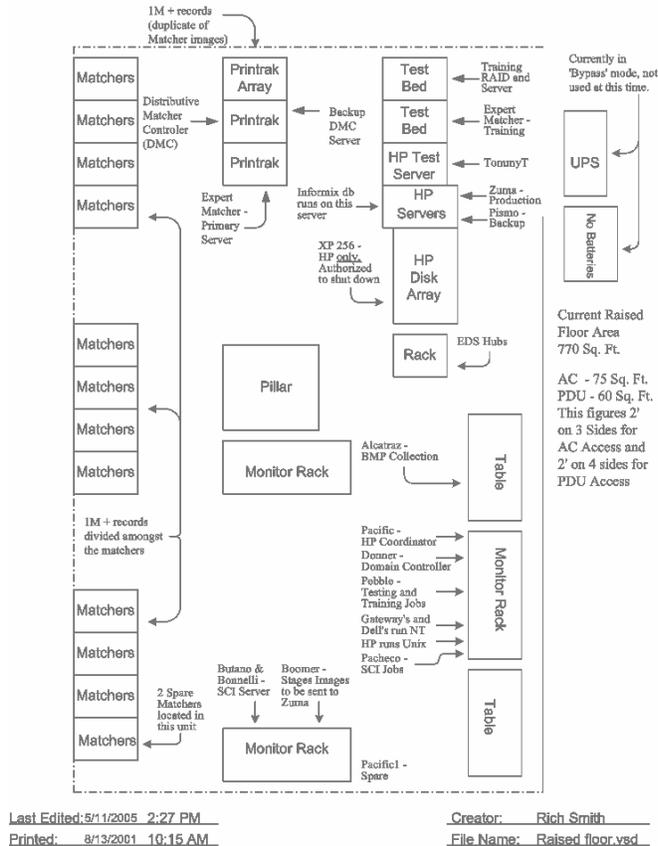


Exhibit: SFIS Central Site Configuration

RFP OSI 2046 CURRENT SYSTEM

Closed Search processing is performed at the System Administration, Multifunction, and Client Input Workstations. However, the process involves the Database Server because it retrieves the images connected to the CIN requested and it re-posts the results of the Closed Search to the verification queue. Since the bulk of the processing is transferred to SFIS workstations, the demand for processing is reduced on the Central Site.

As with the process coordinators, additional network printers may be placed into production should the print volume exceed the capabilities of the existing printers. The addition of network printers into the LAN and redistribution of the print jobs may be accomplished to expand the print capacity of SFIS.

Each Verification Workstation is capable of performing match verification on fifty-four (54) submissions per fifty (50) minute hour. Verification Workstations may also be added to the LAN should the transaction volume increase beyond the current capabilities of the existing Verification Workstations.

The Expert Match Processor has a minimum of ten percent (10%) spare processing capacity to help alleviate possible throughput problems. Another Expert Matcher may be added if the workload increases beyond the current specifications.

The SFIS Database and the Digital Image Retrieval System (DIRS) data both reside on an HP XP256 Disk array. The Database Server utilizes the process coordinators and the Informix relational database software to store SFIS and DIRS information on the HP XP256 Disk Array.

When a fingerprint image is captured at the remote workstation, the workstation generates the following files:

- WSQ – Compressed image of the fingerprint;
- THN – Thinned image of the fingerprint;
- FDP – Minutiae data of the fingerprint;
- DAT – Index and key data for the fingerprint;
- JPG – Photo of the recipient in JPEG format; and
- BMP – Raw fingerprint image bitmap.

The WSQ, THN, FDP, DAT, JPG are transmitted to the Central Site Database Server and, then stored in the DIRS on the XP256. At night, the BMP files are copied to the XP256 where it is temporarily held until it is written to DLT tape for long-term, off-site storage.

RFP OSI 2046 CURRENT SYSTEM

The XP256 disk array is based on a Hitachi storage engine with HP specific enhancements in firmware, performance, and Fiber Channel connectivity. The XP line of Disk Arrays provides:

- High availability, no single point of failure, non-disruptive upgrades;
- Continuous data availability and data storage protection with RAID1, RAID5 and battery-protected, mirrored write cache;
- Multi-terabyte scalability from seventeen gigabytes (17GB) to nine terabytes (9TB); and
- High performance with 100MBps Fiber Channel ports.

Currently, there are twenty-five (25) disk drives in the XP256, twenty-four (24) are in use with one (1) spare. At thirty-six point nine gigabytes (36.9GB) each, the total disk space is eight hundred and eighty-six gigabytes (886GB). The disk drives are configured for redundancy using RAID5. If a disk drive fails, the information on the failed drive can be reconstructed from data on the remaining functional disk drives in the RAID5 set.

The use of RAID5 reduces the eight hundred and eighty-six gigabytes (886GB) of disk space to six hundred and fifty gigabytes (650GB) of usable disk space. Of the six hundred and fifty gigabytes (650GB) of usable disk space, four hundred gigabytes (400GB), or sixty-two percent (62%), are allocated for production use. Of the four hundred gigabytes (400GB) allocated for production, only sixty-two gigabytes (62GB), or fifteen percent (15%), are currently utilized. The SIFS production data residing on the XP256 consumes only nine point five percent (9.5%) of the total usable disk space.

The storage capacity of the Matching Subsystem, like the DIRS storage capacity, is adequate. Each AMP can store between one hundred and thirty-four thousand (134K) and one hundred and seventy-five thousand (175K) SFIS records. The SFIS Matching Subsystem includes forty-seven (47) AMPs (forty-five (45) live, two (2) hot spares); each AMP stores one hundred and thirty-four thousand (134K) SFIS records. Thus, the Matching Subsystem as currently configured is capable of storing five point eight million (5.8M) SFIS records.

RFP OSI 2046 CURRENT SYSTEM

Overall throughput processing is designed such that the system recognizes priority transactions (As of June 2004, priority transactions that added to the SFIS database accounted for seventy-three point one percent (73.1%) of all adds) and returns match results within fifteen (15) minutes. All other transactions (As of June 2004, normal transactions that added to the SFIS database accounted for twenty-six point eight percent (26.8%) priority of all adds) are processed as Normal, which will return match results by 7 a.m. the next day. The SP 2000 processes priority transactions first; normal transactions are queued for processing during the evening or when the SP is idle during priority search time.

The SP 2000 has been configured to process sixty-two (62) transactions within any fifteen (15) minute period. The SP can be scaled to handle a larger database size by adding additional AMPs and, if necessary, additional MMCs.

Response Time Requirements

Retrieval Response Time

The system currently is able to retrieve photo or fingerprint images not associated with a search result in no more than five (5) seconds, excluding Wide Area Network transit time, at any workstation connected to the Central Site.

Closed Search Response Time

All Closed Search matches are performed at the System Administration, Multifunction, and Client Input Workstations as a background job. The process involves retrieving the minutiae data related to the requested CIN from the Database Server and returning this data to the remote workstation. Once the minutiae data has arrived at the workstation, the Closed Search match is performed in seconds. The calculation of capacity, Verification Technicians, and Verification Workstations have been sized to allow review of Closed Searches.

This process results in a response to the user on the Closed Search within an average of fifteen (15) minutes. The response is returned to the workstation transmitting the search data for display and/or print within an average of fifteen (15) minutes from the time the operator selects the Transmit button, indicating the end of input, to the time the match is complete and the system has submitted the match result to the print queue at the site that has requested the search.

RFP OSI 2046 CURRENT SYSTEM

Response Times

Priority search responses are returned in fifteen (15) minutes. The response is returned to the workstation transmitting the search data for display and/or print within fifteen (15) minutes from the time the operator selects the Transmit button, indicating the end of input, to the time the match is complete, and the system has submitted the match result to the print queue at the site that has requested the search.

The remaining twenty-six percent (26.8%) of the "Daily Application" (Normal) workload is returned by 7 a.m. the next State workday. The "Existing Caseload" (Conversion from AFIRM) returns by 7 a.m. on the seventh calendar day following the receipt of the request at the Central Site. The response is returned to the workstation transmitting the search data for display and/or print within seven (7) calendar days from the time the operator selects the Transmit button, indicating the end of input, to the time the match is complete and the system has submitted the match result to the print queue at the site that has requested the search.

Remote Workstation Throughput

Remote Input Workstations are capable of processing a minimum of twenty-four (24) clients per hour.

Verification Throughput

The Current Contractor performs verification on all Open Search Matches, which are approximately five percent (5%) of all Open Searches. The rate at which verification can be accomplished is fifty-four (54) per fifty (50) minute hour, per Verification Workstation. Each of these search verifications assumes the Verification Technician examines the matches on the candidate list. The Expert Matching Processor produces high probability match scores that reduce the size of the candidate list. The long candidate list (twenty (20) to fifty (50) non-AFIRM candidates plus all matched AFIRM candidates) is available for the Verification Technician to view, if desired; however, the Expert Matcher is designed to reduce the need to view this large quantity of candidates. Verification is performed on all single finger Open Searches, with the top five (5) on the candidate list being displayed.

RFP OSI 2046 CURRENT SYSTEM

The number of Closed Searches that produce a No Match requires search verification by an operator at the Central Site. These verifications are assumed to be required during Priority time so as to return a response within the indicated fifteen (15) minute time.

With the inclusion of the Expert Matching Processor, the system was designed to eliminate low confidence search matches. The Expert Matching Processor performs various cognitive matching techniques that a Verification Technician (expert) would employ in performing search verification. These techniques eliminate low confidence match scores and very clearly define candidates as search matches (five percent (5%) which must be reviewed by the operator) and search no-matches (ninety-five percent (95%) which need not be reviewed by the operator).

By incorporating the [Motorola/Printrak](#) proprietary Expert Matcher, the need for Verification Technicians to manually review post-search results is reduced. The Expert Matcher process is based on cognitive theory and makes use of structural and graph-based topological features such as minutiae type, minutiae neighbor similarity, minutiae connectivity, minutiae constellation matching, distance-based ridge count similarity, ridge-trace similarity and ridge-flow similarity. These feature comparison processes are the same skills that the Verification Technician would use to visually compare two (2) side-by-side images. One (1) Verification Workstation, with two (2) six (6) hour shifts per day, can meet the required workload and coverage time needed (currently 7 a.m. to 7 p.m.).

Deleted: Printrak

Search Queues

Separate processing queues are currently utilized to facilitate transaction prioritization. Each processing queue handles records on a first-in, first-out basis. Records in the "priority" queue process before records in the "non priority" queue. The existing workload queue is processed when all other queues have been cleared. SFIS allows only county or State operators with the appropriate permission to modify record priority status. Users with the required security level have the ability to change the priority of individual transactions that are listed as pending in the queue, if, for instance, a match request is submitted with an incorrect priority code. A brief description of this functionality is presented in the following paragraphs. Additional detailed information, including screen layouts can be found in the System Administration Workstation User Guide.

RFP OSI 2046
CURRENT SYSTEM

PRIORITY QUEUE AUTHORIZATION

The State System Administrator and the County System Administrators are able to assign priority queue authorization to a user or a classification of users via the Permission Table. The authority to assign any given priority level is restricted to the State and County System Administrators. Users or user classifications invested with the authority to assign a particular priority level are assigned by the State System Administrator.

DYNAMIC QUEUE DISPLAY

The Central Site dynamically updates the transaction activity of the system queues each time the status has changed ensuring that the database tables always reflect the current processing activity of the queues. Each process running on a remotely located SFIS workstation will post to the appropriate database tables, any change in transaction status. For example, data related to matching subsystem transactions is continuously sent from the MMC to the Database Server.

SFIS provides a dynamic, real-time display of the transaction activity of the system queues. The system queue transaction activity display automatically updates by the system at the time interval set by the State System Administrator. Once initiated, the system queue transaction activity display is automatically updated by the system at a set interval. The set interval for automatic update may occur at a minimum of five (5) seconds. The system queue transaction activity display is available for display at any time on any workstation in the system.

**RFP OSI 2046
CURRENT SYSTEM**

K. MANAGEMENT PROCEDURES AND POLICIES

CHANGE MANAGEMENT

Change Management is a process or discipline of controlling the introduction of change into the production environment. Any change that could possibly affect the production environment is subject to the Change Management process. This includes new equipment installations/de-installations, software upgrades, application enhancements/maintenance, and configuration updates. Changes to computing components such as, application code, servers, storage subsystems, operating systems, LANs, WANs, or data center facilities follow this process. In summary, the process includes the following steps:

- Change request submission;
- Review the impact of the change;
- Validate (or void) the requested change;
- If validated, analysis is completed;
- State signs off analysis;
- Determine other system components requiring alteration because of the change; and change of those components;
- Schedule implementation of the change;
- Communicate the impact of the change to affected stakeholders;
- Test the change (and remove or back-out the change if necessary);
- Implement the change into the production environment; and
- Review the implementation for future improvements.

The SFIS Project Management Office (PMO) has developed and documented a Change Request/Change Order (CR/CO) Process that accommodates change request submission, tracking, analysis and approval. Changes requested by the current Contractor, County, SFIS staff member, etc. are analyzed and then reviewed and approved by the SFIS Change Control Board (CCB).

The State and the current Contractor developed and documented the Change Control (CR/CO) process that uses the Project Administration and Control System (PACS) to track changes to the SFIS production environment from time of Change Request (CR), to time of State accepted Change Order (CO) to implementation. In addition to the CR process, the current Contractor follows a Change Request Implementation Process that includes the following phases:

**RFP OSI 2046
CURRENT SYSTEM**

- Planning Phase;
- Development Phase;
- Testing Phase;
- Release Phase, if appropriate; and
- Monitor/Close Out Phase.

Change Acceptance and Validation Procedures

These above mentioned procedures were designed to be compatible with and have been integrated into, the current Contractor's Configuration Management Plan. Items addressed by these procedures include the Configuration Items listed in the following table:

Formal Configuration Items	Responsibility
6,000 Record Sample Dataset	State
Application Software – Back-End	EDS
Application Software – GUI	EDS
Communication Plan	EDS
Configuration Management Plan	EDS
Database	EDS
Disaster Recovery Plan	EDS
Hardware – Remote and Central Site	EDS
Help Desk Plan	EDS
Help Desk Knowledge Base	EDS
OSI SFIS Web Site	State
Implementation Plan	EDS/State
Portable Input Workstations	EDS
Project Release Workplan	EDS
Regression/System Test Scripts and results	EDS
Release Notice	EDS
Requirements Document	State
Software in Escrow	EDS
Source Code	EDS
System and Utility Software (COTS)	EDS
System Design Document	EDS
System Operation and Support Plan	EDS
System Test Report	EDS
Training Database	EDS

**RFP OSI 2046
CURRENT SYSTEM**

Formal Configuration Items	Responsibility
Training Materials	State
Transfer Plan	EDS
User Communication	EDS/State
User Guides	State
Workstations Online Help	State

Acceptance of a CR by the State is valid when the State signs off on the Change Request Analysis form. Acceptance of a CO by the State is valid when all Configuration Items have been signed off, and validated by the State on the CO form. Only when these written confirmations occur, can changes be considered to be complete and Change Orders closed. CCB approval is tracked through the periodic CCB meeting minutes and the PACS.

The State does not accept a change as being completed until all Configuration Items associated with a change have also been inspected and approved by the State. This is documented in the CM Plan throughout the CR/CO process.

It is important to note that many changes are not stand-alone; a change may require a prerequisite or a co-requisite. Because of these relationships as well as for convenience, changes may be batched together such as in a new software version. This has an affect on the acceptance and validation strategy, since often several changes are reviewed for acceptance and validation at the same time.

The following bullet points describe various aspects of the State's acceptance and validation process for changes to SFIS:

RFP OSI 2046
CURRENT SYSTEM

- The SFIS' team's acceptance and validation procedures for changes to SFIS vary depending on the nature and scope of the change. For example, if a change is software oriented, the acceptance and validation procedure might be to request a demonstration of the change, accompanied by inspection of relevant configuration items. If the change is hardware oriented the team may opt to conduct their own independent testing that leads to acceptance and validation (also accompanied by inspection of relevant Configuration Items). Another possibility is to view a demonstration provided by the Contractor but still conduct independent testing. If the change is to documentation only, the acceptance and validation procedure might be inspection only. There are no hard and fast rules concerning what acceptance and validation processes should be followed. The acceptance and validation procedure to be followed for a particular Change Request/ Order, however, is always defined and agreed upon by the Contractor and added by the State to the Change Request's/ Order's test plan.
- Just as the processes for acceptance and validation vary based on the nature and scope of changes, so too can the make-up of the State's Acceptance and Validation Team vary. A change with an extremely broad scope might entail including representatives from OSI, CDSS, and the counties on the Acceptance and Validation Team. On the other hand, a minor change to a computer room process or document may only require a single representative from the State be on the Acceptance and Validation Team. Again, there are no hard and fast rules regarding Acceptance and Validation Team composition. The acceptance and validation procedure to be followed for a particular Change Request/ Order, however, is defined and agreed upon by the Contractor and added by the State to the Change Request's/Order's test plan.
- The PACS is used to house acceptance and validation information. The updating of PACS is included in the CR/CO Process.
- For purposes of accountability, only one (1) organization is responsible for a change.
- The steps described below may be used not just to support acceptance and validation of SFIS hardware and software changes but may also be applied to other items such a document deliverables or procedural changes.

**RFP OSI 2046
CURRENT SYSTEM**

Formal Acceptance and Validation

Step	Action	Description
1	Change Request / Change Order Review	<p>The CCB will review each Change Request to determine the change's nature and scope. Analysis forms can be used to assist in determining the scope of the change(s) with respect to configuration items. Implementation plans can also be used to support this review.</p> <p>The CCB will also be responsible for addressing possible management concerns associated with the change(s).</p>
2	Create Acceptance and Validation Team	<p>CCB review of the change determines the composition of the Acceptance and Validation Team, if required. In many cases this is handled informally and only one (1) person comprises the Team. If the CCB determines that the change(s) are such that they can be reviewed by OSI's SFIS resources only, the State System Administrator or his/her designee will create the Acceptance and Validation Team, subject to the SFIS Project Manager's approval; typically the Project Manager delegates this to the SFIS Program Operations Manager. If resources are required for the Team that are outside OSI's SFIS staff, the SFIS Program Operations Manager will escalate to the SFIS Project Manager who will then secure the necessary Team resources. This is most likely to occur if CDSS or county resources are required, but the Team could also require a resource such as DTS Telecomm.</p> <p>The CCB review will also establish if the SFIS Project Manager is the correct level of authority to complete the acceptance of the change(s) by the State. In some cases, it may be appropriate that CDSS management has this authority.</p> <p>A fundamental aspect of the Team is that the SFIS Program Operations Manager or his designee will appoint a Team Leader. The Team Leader will be accountable for the Team's activities, including</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		recommending rejection or acceptance to the SFIS Project Manager. This leadership assignment is documented in the PACS.
3	Determine Acceptance and Validation Process	<p>The Acceptance and Validation Team will determine, with input from the parties (Contractor, OSI etc.) responsible for the change(s), how to best accept and validate the change(s). This step could result in a change to the composition of the Team.</p> <p>For each change or set of changes a documented Acceptance and Validation Plan will be developed by the Team. This plan is housed in the PACS and added to the changes test plan.</p>
4	Evaluate and Approve the Contractor's Test Plan	<p>This step may not be required if the scope of the change(s) is small. This step also assumes the SFIS Contractor is responsible for executing the change(s). In actuality, entities other than the Contractor could be responsible for a change.</p> <p>This procedure is executed when the Contractor notifies the State that their Test Plan is ready for approval. The Test Plan must be reviewed by the Acceptance and Validation Team and approved by the CCB, or their designee. The Test Plan will include all related CIs, release date(s), and end user notifications.</p>
5	Review and Approve the Contractor's Test Plan Results	<p>The Acceptance and Validation Team may review and evaluate test results including:</p> <ul style="list-style-type: none"> • Regression/System Test Scripts and results. • System Test Report. <p>The Team will approve the results or recommend corrective action.</p>
6	Create Test(s) Package(s)	The Acceptance and Validation Team will create test package(s) by assembling all Configuration Items from all responsible parties.

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
7	Conduct Acceptance and Validation Test(s)	<p>The Acceptance and Validation Team will perform the Acceptance and Validation Test(s) as defined in the Acceptance and Validation Plan. These tests may or may not include the Contractor.</p> <p>Deviations will be documented and provided to the Contractor or other party, if appropriate. Recommendation for approval or rejection will be provided to the SFIS Project Manager.</p>
8	Deviation Correction	<p>The responsible party will correct deviations. The Acceptance and Validation Team will ensure that deviations have been corrected.</p>
9	Acceptance of Change(s)	<p>The SFIS Project Manager or his/her designee will accept the change(s) in writing, and notify the Contractor, if required. The Change Request(s) / Change Order(s) will be closed.</p>
10	Change(s) Included in Production SFIS	<p>The change(s) will be included in the SFIS production environment.</p>
11	Tracking	<p>The status of the Change Request / Order is maintained so that the current acceptance status (Open, Closed, Void) and status date is available. Each time a change in status occurs, the Change Request / Change Order in the PACS shall reflect the new status.</p>

RFP OSI 2046 CURRENT SYSTEM

Examples

Below is an example of an Analysis Form from PACS.



Change Request For Analysis

Control Number: SF-C-0463 Status: Closed
 Initiated By: Lorol de Mola, Enrique Date Initiated: 04/06/04
 Title: Help Desk Ticketing Tool Migration Priority: High

Release Number: NA Build Release Number:
 Target Release Date: Date To Production:
 Change Type: Technical Category:

Description: EDS is migrating its REM's online help desk tool to a new offering called "Digital Workflow". As part of this migration the REM's online editing tool will be migrated to a new tool from Paraglyph. This effort includes the following tasks: the transfer of REM data to the new tool, new data requirements, reports conversion, application and network access, user training and project documentation updates. The SFIS help desk is scheduled to be included in Phase I of the project. Phase I completion is to be completed by August 2004.

Requirements Affected? Yes No TBD
 Functions: Help

Analysis Information

Analysis Assigned To: Scott Sean Date Assigned: 05/12/04
 Analysis Due Date: 05/13/04 Date Analysis Returned: 05/12/04
 Estimated Effort: 120+ hrs. Confidence Level: High
 Technical Solution: Install new program, create necessary access to the tool through the State and EDS network; establish new access for transfer data from REM to new tool; train all users; update documentation (HD Document and knowledge base)
 Programs Affected: REM's online
 Cost Of Change: No Change Estimate of Change: \$0
 Proposed One-Time Costs: \$0.00 Proposed On-Going Costs: \$0.00

Milestones Affected? Yes No TBD

- Configurables Affected? Yes No TBD
- 6,000 Record Sample Dataset
 - Configuration Management Plan
 - EDS Internal Documentation
 - Help Desk Plan
 - Portable Input Workstations
 - Requirements Document
 - System and Utilities Software (COTS)
 - Test Scripts and Results
 - Training Materials
 - User Communication
 - Workstations On-line Help
 - Application Software - Back-End
 - Database
 - Hardware - Remote and Central Site
 - HMSDC's SFIS Web Site
 - Regression Testing
 - Software in Escrow
 - System Design Document
 - Toolbars/Shortcut
 - Transfer Plan
 - User Guide
 - Application Software - GUI
 - Disaster Recovery Plan
 - Help Desk Knowledge Base
 - Implementation Plan
 - Regression Testing Scripts
 - Source Code
 - System Operation and Support Plan
 - Training Database
 - User Acceptance Testing
 - User Input

Project Plan Required? Yes No TBD

Resources:	Name	Hours	Position	Rate	Total
	Scott, Sean	120	Application Analyst	\$80	\$9,600
Total Resource Cost:					\$9,600

Analysis Comments: No cost to the State.
 State Approval: Signature: _____ Date: _____

RFP OSI 2046 CURRENT SYSTEM

Below is an example of a Change Request form from the PACS.



Change Request

Change Request Identification

Control Number: SF-C-0463 Status: Closed
 Initiated By: Lorel de Mola, Enrique Date Initiated: 04/06/04 Phase: CO opened
 Project Manager: Christina, George PM Validation: Yes No TBD Priority: High
 PM Comments:

Change Request Description

Title: Help Desk Ticketing Tool Migration
 Description: EDS is migrating its REM/Anthro help desk tool to a new offering called "Digital Workflow". As part of this migration the REM/Anthro existing tool will be migrated to a new tool from PerotSystems. This effort includes the following tasks: the transfer of REM data to the new tool, new data requirements, reports conversion, application and network access, user training and project documentation updates. The SFPS help desk is scheduled to be included in Phase 1 of the project. Phase 1 conversions to be completed by August 2004.

Change Type: Technical Change Category:
 Is CR due to Risk Event? Yes No TBD If yes, Risk Control Number?:
 Is Change Mandated? Yes No TBD Explain:
 Requirements Affected? Yes No TBD

Catalyst For Change:
 Justification For Change:

Status Date/Desc.: 05/12/04 State, Dave Sakayya, signed off on 5/12/04. Closed and opened CO #SF-C-0253. I manage document #14,271 v1. Scanned copies e-mailed to Henry Lorel de Mola on 5/12/04 and originals to be hand-delivered on 5/20/04.
 05/12/04 Per Henry Lorel de Mola's telephone conversation with Melanie Coups on 5/12/04 - Analysis completed.
 05/12/04 Added and opened per the 5/6/04 CCB meeting and Henry Lorel de Mola's e-mail dated 5/11/04.

Analysis Information

Analysis Assigned To: Scott Swan Date Analysis Assigned: 05/12/04
 Analysis Due Date: 05/13/04 Date Analysis Returned: 05/12/04
 Estimated Effort: 120+ hrs. Confidence Level: High
 Technical Solution: Install new program; create necessary access to the tool through the State and EDS networks; establish new access; migrate data from REM to new tool; train all users; update documentation (HD Document and knowledge base)
 Programs Affected: REM/Anthro Estimate of Change: \$0.00
 Cost Of Change: No Change Proposed One-Time Costs: \$0.00 Proposed On-Going Costs: \$0.00
 Milestones Affected? Yes No TBD
 Configurables Affected? Yes No TBD

Approval Cycle

Project Configuration Control Board Action		
Board Action: <input checked="" type="radio"/> Approved <input type="radio"/> Disapproved <input type="radio"/> TBD	Project CCB Status: <input type="radio"/> Forward to Program CCB <input type="radio"/> Cancel <input type="radio"/> Hold <input checked="" type="radio"/> Unknown	
Board Chair Name: Sakayya, Dave	Signature:	Date: 05/12/04

RFP OSI 2046 CURRENT SYSTEM

Below is an example of a Change Order form from the PACS.



Change Order

Change Request/Order No.: SFC-04638F-C-0253 **Date Initiated:** 05/12/04
Change Type: **Status:** Open
Title: Help Desk Ticketing Tool Migration

Description:
EDS is migrating its REM/Varithe help desk tool to a new offering called "Digital Workflow". As part of this migration the REM/Varithe ticketing tool will be migrated to a new tool from Paragins. This offer includes the following tasks: the transfer of REM data to the new tool, new data requirements, setup, configuration, application and network access, user training and project documentation updates. The SFD help desk is scheduled to be included in Phase 1 of the project. Phase 1 conversions to be completed by August 2004.

Configurables:

Help Desk Knowledge Base	
<i>Assigned To:</i> Arndt, MaryJane	<i>Status:</i> Not Started
<i>Checked By:</i> _____	<i>Date:</i> _____
<i>Comments:</i> _____	
Help Desk Plan	
<i>Assigned To:</i> Barkon, Lori	<i>Status:</i> Not Started
<i>Checked By:</i> _____	<i>Date:</i> _____
<i>Comments:</i> _____	

Status Description:
10/06/04 Per Henry Lord de Mold's e-mail dated 10/06/04. The State firewall team is reviewing the change submitted to allow the State GPS location access the EDS DW IP. That we know of the change has not been scheduled.

Approved By: <input checked="" type="checkbox"/> Project CCB <input type="checkbox"/> Program CCB <input type="checkbox"/> Org. Level CMB
Date: 05/12/04 Date: Date:

Stipulations

General Stipulations:
Cost not to exceed: \$0.00 **Schedule not to be extended more than:**

CONFIGURATION MANAGEMENT

Application Development Environment

The following describe the languages and tools used to construct the SFIS applications. The SFIS applications are built using a mixture of 'C' language programs for batch, data service utilities, and reporting and the PowerBuilder Development Tool for the end-user application.

Overview

As part of the SFIS application, services for data storage and manipulation are written in 'C'. These services provide data storage and manipulation in the SFIS database and file system. 'C' programs also provide the bulk of the batch processing for the SFIS system. 'C' programs generate daily, weekly, and monthly reports. In addition, various 'C' programs provide operational support and monitoring services.

The SFIS project uses the PowerBuilder Development Tool from Sybase Corporation. PowerBuilder is a client / server application development tool that has been on the market for over ten years. PowerBuilder supports two-tier, n-tier and web based client / server application development. The SFIS application architecture calls for a two-tier implementation, with PowerBuilder being used to develop the client tier application.

PowerBuilder is a Rapid Application Development (RAD) tool that concentrates on easing the interaction of user interface with the data source. In the PowerBuilder tool, these functions are blended together using a control called DataWindows. DataWindows allow the developer to graphically create data access commands and tie the results to the on-screen display.

RFP OSI 2046 CURRENT SYSTEM

Application Coding Standards

The SFIS application coding standards are included as part of the Configuration Management Plan (CMP) document. They are found in Appendix A of that document. The standards included in the CMP for SFIS include standards for PowerBuilder, 'C', database, and documentation. The PowerBuilder standards include information for the developers. Instructions for naming variables and functions are present as well as the basic structure for source code in-line documentation. Also included are some basic dos and don'ts for PowerBuilder coding and displays.

The 'C' standards section contains a brief summary of rules for variable and function naming as well as instructions for formatting comments and source code. Also included are a brief code sample and some additional items for consideration when using the embedded SQL calls for the Informix database.

Application Software Configuration Management

The SFIS project has a Configuration Management Plan document that contains detail on the mechanics of configuration management. It contains definitions of common CM terms and a prescribed flow of Configuration Items (CI).

'C' Source Code

Configuration management of the 'C' source code uses an internal project tool called SFISPMTS. This tool was developed internally for use by the SFIS project. Currently, all of the source files are under configuration management control.

PowerBuilder

The PowerBuilder application uses an integrated tool called "Object Cycle" for configuration management. The Object Cycle tool comes as part of the PowerBuilder application tool. Object Cycle is a tool for the management of PowerBuilder code using a specific configuration management server that the developer must connect to prior to altering source code. The tool keeps track of who checks out / in source code, revisions of the code, as well as providing a repository for developer's comments.

**RFP OSI 2046
CURRENT SYSTEM**

Configuration Management Specialist

The current Contractor Project Manager, or a Systems Engineer (SE) assigned as backup, fill the role of Configuration Management Specialist and performs configuration management activities for which the current Contractor is responsible. The responsibilities include control of the project directory as gatekeeper, change control for documentation, and placement of escrow code into the project directory. The State performs configuration management activities on items for which the State is responsible.

Formal Configuration Management Activities

Formal configuration management is a strict process that requires a CR to make changes to any of the Formal configuration items. The CR is reviewed by the CCB and approved or denied. After changing a Formal CI, approval of the change is required by the CCB.

Configuration Item Identification

The objective of configuration identification is to identify a system and the components to be configured. It is the process of defining and documenting the configuration of a system throughout its life cycle. The first step in this process is the identification of the system level configuration item. Baselines and releases are established in accordance with the project plan.

Formal Configuration Items	Responsibility
6,000 Record Sample Dataset	State
Application Software – Back-End	EDS
Application Software – GUI	EDS
Communication Plan	EDS
Configuration Management Plan	EDS
Database	EDS
Disaster Recovery Plan	EDS
Hardware – Remote and Central Site	EDS
Help Desk Plan	EDS
Help Desk Knowledge Base	EDS
OSI SFIS Web Site	State
Implementation Plan	EDS/State
Portable Input Workstations	EDS
Project Release Workplan	EDS

**RFP OSI 2046
CURRENT SYSTEM**

Formal Configuration Items	Responsibility
Regression/System Test Scripts and results	EDS
Release Notice	State
Requirements Document	State
Software in Escrow	EDS
Source Code	EDS
System and Utility Software (COTS)	EDS
System Design Document	EDS
System Operation and Support Plan	EDS
System Test Report	EDS
Training Database	EDS/State
Training Materials	State
Transfer Plan	EDS
User Communication	EDS/State
User Guides	State
Workstations Online Help	State

Version Control Standards

For source code, configuration management tools are used (one (1) for PowerBuilder and one (1) for C) to manage and store previous versions of code. However, when a new release is deployed to production, the Configuration Management Specialist will place a copy of the escrow code into the project directory for Formal configuration management control. This directory will be located in \\Jade\CM_documents\. Additionally, all Formal Configuration Items related to the release will also be stored in this directory. This will allow all items for a particular release to be stored in one (1) directory. For example, the next release of SFIS will include all changed documentation, all of the source code deployed to production, and a copy of the schema of the database and any other Formal CIs. Only the Configuration Management Specialist and a backup will have write access to this directory. Any hard copies of CIs will be stored by the Contractor Project Manager.

RFP OSI 2046 CURRENT SYSTEM

VERSION NUMBERING STANDARDS

A sequential number containing an integer and decimal portion will be used for version numbering of both software and documentation. For each new release of SFIS software, the decimal portion of the version number is incremented. For example, the decimal portion would increase from 5.02 to 5.03. If the change is great enough (for example, a new version of PowerBuilder is implemented), the version is incremented to the next highest integer. For example, the version would increase from 5.03 to 6.0.

Similarly, for documentation, each change to a document will increment the decimal portion of the version number, such as from 1.0 to 1.1. Major changes to the document or a complete rewrite will increment the integer portion of the number, for example, from 1.6 to 2.0. The version number will be recorded in the document's Amendment History. If the document's changes are related to a release, the corresponding release number will also be recorded in the document's Amendment History. For those documents that currently do not have an Amendment History, the next time the document is changed via a CR, the Amendment History will be added.

CHANGE REQUEST IDENTIFICATION

When a CR is entered into PACS, a control number is assigned to the CR, which will be the unique identifier for that particular CR. The same control number will be used to identify the CR in the current Contractor's Project Control Database (PCD).

CM TOOLS

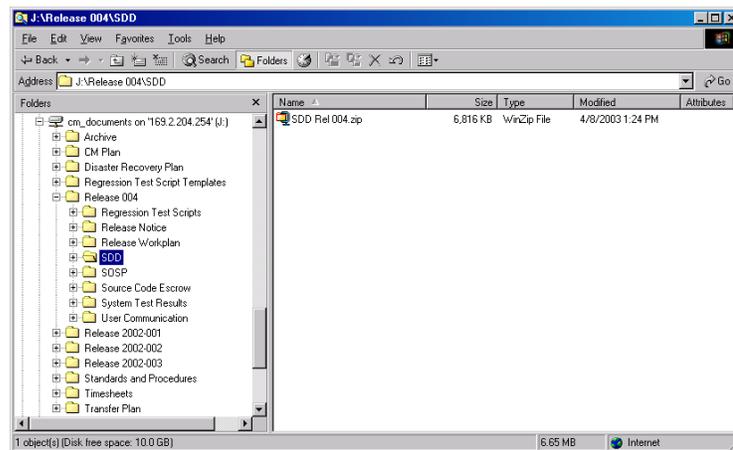
CM Tools	Baseline
PowerBuilder Object Cycle	PowerBuilder Source Code
SFISPMTS	C Source Code
Change System Request (CSR) Checklist	PACS checklist for changes to a CI in response to a CR or CO
Project directory structure on Jade	Documentation and source code deployed to production

RFP OSI 2046 CURRENT SYSTEM

JADE SERVER

The Jade server will be used to store all files and documentation related to configuration management. The folders used for CM are the CM_documents folder for Formal CIs, and the CM Supporting Documents folder for use as a working directory. The CM_documents folder is protected and only the Configuration Management Specialist and a backup has access. The CM Supporting Documents folder is open to everyone on the project to use as a work-in-progress area. Each directory is shown below along with an explanation of its sub-folders.

CM_DOCUMENTS FOLDER



The CM_documents folder is used to store all Formal CIs. It is also used to store other important document, including some that are managed and controlled. The contents of each sub-folder are described below.

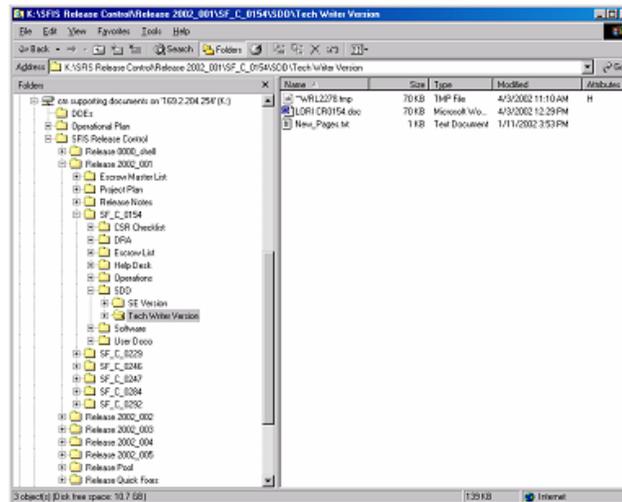
- Archive – Old versions of documentation before configuration management was put into place, and versions not related to a specific release.
- CM Plan – All versions of the Configuration Management Plan.
- Disaster Recovery Plan – All versions of the Disaster Recovery Plan.

RFP OSI 2046 CURRENT SYSTEM

- Regression Test Script Templates – Test case templates used for regression testing.
- Release ccy-### – Each Release folder contains all the formal CIs that were created or changed for that release, including the LA User Guide, Regression Test Scripts, Release Notice, Release Workplan (the project schedule in MS Project), System Design Document (SDD), System Operation Support Plan (SOSP), Source Code Escrow, System Test Results, and any User Communication. A backup copy of the working documents from the CM Supporting Documents folder may also be stored here.
- Standards and Procedures – Internal procedures used by the current Contractor team including documentation standards for the SDD and SOSP, the SOSP template, and the current Contractor Style Guide.
- Transfer Plan – All versions of the Transfer Plan.

CM SUPPORTING DOCUMENTS FOLDER

The CM Supporting Documents folder is used mainly as a working directory for CIs created during the release. The contents of each sub-folder are described below.



- DDEs – Copies of State provided DDEs.

RFP OSI 2046 CURRENT SYSTEM

- Operational Plan – MS Project files.
- SFIS Release Control – Folders created for each release number are used to store working documents. Items in each release folder include (but are not limited to) the Escrow Master List, the Project Plan, Release Notes, and documentation for each CR. Each CR folder may contain the following sub-folders:
 - CSR Checklist – CSR Checklist filled out by the SE assigned to the CR.
 - DRA – Not currently used, but created for any Disaster Recovery Action (Plans).
 - Escrow List – Escrow lists of the programs, tables, and data affected by the change.
 - Help Desk – Documentation of any needed changes to the Help Desk Plan, Knowledgebase, or online help files.
 - Operations – Documentation of any needed changes to Operations (SOSP).
 - SDD (SE Version) – Documentation of any needed changes to the SDD.
 - SDD (Tech Writer Version) – Documentation of the SDD related changes as completed by the Technical Writer.
 - Software – Objects, GUI, tables, files, and related walkthrough forms.

Other folders included under SFIS Release Control are:

- Release Pool – CRs that have not yet been assigned to a release.
- Quick Fixes – CRs that identify known problems that can be quickly and safely included whenever the user requests them.

BASELINES

Baselines are established for Formal Configuration Items. When a Review is required, participation from current Contractor, the PMO, and the State must be present so that approval and sign-off can be achieved.

**RFP OSI 2046
CURRENT SYSTEM**

Configuration Item	Control	When Baselined
6,000 Record Sample Dataset	Formal	At initial implementation
Application Software – Back-End	Formal	At promotion to Regression Testing
Application Software – GUI	Formal	At promotion to Regression Testing
Configuration Management Plan	Formal	After Walkthrough/Review of Plan and approval
Database	Formal	At promotion to Regression Testing
Disaster Recovery Plan	Formal	After Walkthrough of plan and approval
Hardware – Remote and Central Site	Formal	After deployment
Help Desk Plan	Formal	After Walkthrough of document and approval
Help Desk Knowledge Base	Formal	After Walkthrough of content to be added
OSI SFIS Web Site	Formal	After the initial online publication
Implementation Plan	Formal	After Walkthrough/Review of Plan and approval
Portable Input Workstations	Formal	After deployment
Project Release Workplan	Formal	After scope sign-off, and review and approval of Workplan
Regression/System Test Scripts and results	Formal	Ongoing
Release Notice	Formal	Production turnover and after deployment
Requirements Document	Formal	After review of Requirements Documentation and approval
Software in Escrow	Formal	After placement in Escrow
Source Code	Formal	At promotion to Regression Testing
System and Utility Software (COTS)	Formal	At promotion to Regression Testing
System Design	Formal	After review of Requirements

**RFP OSI 2046
CURRENT SYSTEM**

Configuration Item	Control	When Baselined
Document		Documentation and approval
System Operation and Support Plan	Formal	Production turnover
System Test Report	Formal	Ongoing
Training Database	Formal	At promotion to Regression Testing
Transfer Plan	Formal	After Walkthrough/Review of Plan and approval
User Communication	Formal	Ongoing
User Guides	Formal	Ongoing
Workstations On-line Help	Formal	After deployment

CM REPORTING

Report	Timing	Contents	Responsible	Audience
Baseline Verification Report	After baseline verification	Baseline Audit Date	Configuration Management Specialist	Current Contractor Project Manager Project Team
Deployment Plan	As needed - prior to a release or implementation	Application name and acronym Version number Installation date Description of the release Contact personnel Installation instructions	Current Contractor Project Manager	Affected Groups

BASELINE VERIFICATIONS

CM Baseline Verifications examine baselines and supporting documentation to ensure:

RFP OSI 2046
CURRENT SYSTEM

- Changes to CIs are properly documented both in the CI itself, and in supporting documentation.
- All CIs identified for a given baseline are present and that there are no extraneous CIs in the baseline.
- Actual structure and facilities of the CM control system (manual or automated) are the same as those documented in the project CM Plan.

A single verification may cover multiple control libraries and baselines. The baseline verification is conducted by the Configuration Management Specialist and is done every six (6) months with a baseline verification report being the outcome of the baseline verification.

Configuration Management Procedures

Formal Change Request Procedure

Step	Action	Description
1	Initiate Change Request	Any person with sufficient access and knowledge of the situation can request a CR. Initiation of a CR can consist of completion of a hard copy or electronic form, or memo sent to the appropriate person identified in the Communication Plan. It may not be possible at this point in time in the life cycle of the request for work to have a definitive determination whether an issue is an enhancement or a defect.
2	Record Change Request	The CCB reviews the request. If the CCB review determines that the request can be processed, the submitter is notified of the receipt of the CR, the request is captured and logged, and tracking and reporting of the status begins in PACS. If there are errors in the request that prevent further processing, it is returned to the submitter with information indicating the cause for the return. In this case, the receipt is not

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		<p>logged and it is expected that it will be resubmitted. When a change is received that results in a change to an existing CR, there are two (2) options:</p> <p>Option 1: Cancel the existing CR, consolidate the CR information (new plus old), and document a new CR.</p> <p>Option 2: Document changes on the existing CR and update the status and status change date for the existing CR.</p> <p>Current Contractor will determine who will perform the analysis.</p>
3	Prioritize and Assign Change Request for Analysis	<p>A report is generated from PACS for the current list of CRs. Each CR is prioritized and assigned as part of the CCB and the assignee evaluates the CR and develops a recommendation and proposed solution, with input from Subject Matter Experts (SME) and affected groups. Analysis will include time, resources, and costs. The CSR Checklist will be used. Following are the steps to evaluate a CR in the CCB:</p> <ul style="list-style-type: none"> • Prioritize • Determine who will evaluate • Address possible management concerns
4	Evaluate Change Request	<p>This procedure is executed when a CR is assigned by the CCB, as well as periodically for existing CRs. Following are the steps to evaluate a CR:</p> <ul style="list-style-type: none"> • Develop recommendation (concerning the request) to proceed, place on hold, or cancel • Identify all affected work products (including documentation) • Estimate State resources and costs

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		<ul style="list-style-type: none"> • Include change in State project plan <p>If the assignee is a member of the current Contractor team, the current Contractor team member will fill out the above information in the PCD. The current Contractor Project Manager will then generate a report from the PCD by Tuesday at noon for delivery to the State so that the PMO can update PACS.</p>
5	If Decision is to Proceed	<p>Obtain CCB Approval</p> <p>For all CRs, the current Contractor Project Manager and CCB approval is required. The CR is updated to reflect the status change:</p> <ul style="list-style-type: none"> • Obtain SFIS Project Management Approval • Tentatively plan which release the change would be part of <p>The current Contractor Project Manager communicates the approved changes to the project team. The CCB communicates the approved changes to the State, affected groups and the CR originator.</p>
6	Tracking	<p>The status of the CR is maintained so that the current status (New, Review, Approved, Rejected, Completed) and status date is available. Each time a change is made, an entry is made into both PACS and the PCD with the changed information to provide an audit trail.</p> <p>For approved CRs, ensure that all work products identified in the impact analysis are updated prior to showing the status of the CR as complete.</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		Once CCB approval is obtained, the CR becomes a Change Order.

Formal Configuration Item Control

Step	Action	Description
1	Authorize CI Changes	<p>The Contractor Project Manager determines who will be changing CIs impacted by the CR.</p> <p>Verify approval by reviewing authorizing document.</p> <p>Verify that the CI is not already being updated by someone else. If a new CI is being created, verify that the name is not already in use. If an existing CI is to be updated, verify that the CI has not been changed since the last authorized change.</p> <p>Update the authorizing document (Change Order), recording the assignee and assigned date information.</p>
2	Sign Out CIs	<p>Team member assigned to work on the Change Order obtains the change control identifier (CCID) from PACS to be used to tie the CI changes to the CR that authorized the change.</p> <p>For documents, the Configuration Management Specialist will move a copy of the CI from the Controlled Environment (project directory) to a work environment.</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
3	Change / Create CIs	<p>The authorized team member edits the CI in the work environment.</p> <p>The Modification Log in the CI should be updated when changes are made. This should include the date, a brief description of change, the CCID, and the name of the person making the change.</p> <p>For documents, the Amendment History should include the CR#, version number, approval date, modified by name, and revision description.</p> <p>Unit test CIs.</p> <p>Walkthroughs should be performed for CIs changed or created. Depending on the organization standards, multiple CIs may be covered in the same walkthrough. Suggested changes should be documented and there should be verification that the changes were completed as required.</p>
4	Add CIs	<p>Make sure no prior activity (such as emergency fixes) has occurred, which will be lost when the CI is returned to the controlled environment.</p> <p>The CI is returned to the CM-controlled environment. For documents, the Configuration Management Specialist will return the CI to the Controlled Environment (project directory).</p>
5	Verify CI Testing	<p>The test plan must be reviewed and approved by the State. The Test Plan will include all related CIs, release date(s), and end user notifications.</p> <p>Complete integration, regression, and user acceptance testing.</p> <p>The results of the test must be reviewed and approved by the State, with the date</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		and time of the approval recorded.
6	Update Technical Documentation	The current Contractor Technical Writer reviews the CSR Checklists to identify the technical documentation to update. Update the identified documentation. Obtain approval of completed documentation from the current Contractor, the State, and the PMO.

Formal Release Control

Step	Action	Description
1	Create Release Package	Create release package by identifying work products to be included, specifying action(s) to be performed, and indicating when the release package should be executed. Notify end users of the planned implementation date and impact of release.
2	Process Release Package	Review the release package with the CCB. Approve release package if the requested actions are appropriate. Execute release package takes place when the CM-Controlled Library is updated such that the CIs in the release package are acted upon as designated in the release package. This includes the tasks of validating the release package, ensuring the execution is in the execution window, and ensuring that the CIs have not been modified since the release package was validated. Validate the baseline and update the status of the Change Order in PACS and the CR in the PCD to completed.

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		<p>Commit release package once the CCB is sure that there will no longer be a need to do a back out or back in and the associated back-out/back-in data can be deleted.</p> <p>Notify end users that the release package has been implemented and provide instructions to implement, if required.</p>
3	Create Release Notice	<p>The current Contractor Technical Writer creates the Release Notice. When a software version is released to the State, an entry must be made in the Release Notice identifying the release number, date released, version ID, and a description of the changes. A complete history is necessary for audit purposes and to plan future releases.</p> <p>Obtain approval of the completed documentation from the current Contractor, the State, and the PMO.</p>
4	Deliver Documentation	<p>The current Contractor Technical Writer delivers the updated technical documentation and the Release Notice to the State and the current Contractor Help Desk Supervisor.</p>
5	Update User Guides and Training Materials	<p>The State reviews the CSR Checklists, updated technical documentation, and the Release Notice to identify the User Guides and training materials to update.</p> <p>Update the User Guides and training materials.</p> <p>Obtain approval of the completed documentation from the State and the PMO.</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
6	Ship Release Package	<p>Release package shipment utilizes data transmission or some type of manual distribution process to send release package outputs from one (1) site to another site.</p> <p>Once a software product has been installed at a remote site, the CM Administrator verifies with the State that the release package was complete and satisfactorily addresses the associated CRs.</p>
7	Deliver User Guides and Training	The State delivers the Release Notice, User Guides, training, and training materials to the end users.

Formal Baseline Verification

Step	Action	Description
1	Prepare for CM Baseline Verification	<p>Define scope of the verification including systems(s) and CIs to be reviewed.</p> <p>Define selection criteria for CIs, for example:</p> <ul style="list-style-type: none"> • CIs which have never been audited • CIs with the oldest audit date • CIs changed since the last CM baseline audit <p>The CM Baseline Verification History Log can be used to determine which system(s) and CIs have been previously verified and when the verification occurred. The CM Baseline Verification History Log is updated with the latest information from the selection of system(s), baseline(s), and CIs.</p> <p>Gather materials (such as the project CM Plan and the Release Notice) and also</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		<p>ensure that access to the on-line baselines/libraries to conduct the verification is available.</p> <p>Develop the Introduction and Scope sections of the CM Baseline Verification Report.</p>
2	Assess Baseline Integrity	<p>Determine if all CIs associated with a baseline actually exist within the baseline, and that all existing CIs in the baseline are documented as belonging in the baseline. This must be done for each baseline to validate each baseline, and done for each baseline to validate the baseline contents. If a tool is used for CM activities, the tool may also be used to perform this step.</p> <p>List current CM baseline contents. If an automated tool is used, an inventory report can be generated by the system to obtain the current CM baseline contents.</p> <p>Create an (expected) CM baseline contents report by combining the baseline contents reports from the prior CM Baseline Verifications with the changes identified in the Release Notice(s).</p> <p>Search for missing CIs by comparing the current baseline contents with the (expected) baseline contents report.</p> <p>Search for additional CIs by identifying any CIs on the (expected) baseline content report but are not in the actual baseline content.</p> <p>Verify CIs in progress. Verify that all the CIs currently "checked out" for updates are still legitimately being updated. Any CIs that no longer need to be checked out must be documented as an issue in</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		<p>the CM Baseline Verification Report.</p> <p>Update the CM Baseline Verification Report to include the findings from the Assess Baseline Integrity step.</p>
3	Verify Baseline Correctness and Completeness	<p>Ensure selected CIs within the CM baseline reflect all the documentation describing them, and ensure that all documentation that describes the CI exists.</p> <p>Generate listings of selected CIs from the baseline. The CM tool may be used to generate this listing.</p> <p>Obtain all CR reports for the selected CIs.</p> <p>Verify the CI is documented according to CM standards. Note any discrepancies for reporting.</p> <p>Verify the CI reflects all documentation from the CR reports, which affected the CI. Note any discrepancies for reporting.</p> <p>Verify that all documentation identified within the CI exists. Note any discrepancies for reporting.</p> <p>Verify approvals occur after changes, by comparing the date/time stamp on the CI to the date/time stamp on the Release Notice. Note any discrepancies for reporting.</p> <p>Update the CM Baseline Verification Report, documenting any discrepancies, and update the Baseline Verification History Log with the verified CIs.</p>
4	Review Structure and Facilities	<p>Ensure that the actual configuration and construction of each baseline is consistent with the description of the baseline as defined in the project CM Plan. Verify that the security structure</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		<p>and access defined in the project CM Plan is consistent with the security authorizations to the baseline.</p> <p>Document the actual physical configuration of the baseline and the actual security structure. An automated CM tool may be used.</p> <p>Compare the documented actual information with the information contained in the project CM Plan.</p> <p>Document any discrepancies in the CM Baseline Structure - Findings and Issues of the CM Baseline Verification Report.</p>
5	Verify Compliance to CM Standards and Procedures	<p>Verify that the project is following the CM standards and procedures documented in the project CM Plan. A checklist may be developed and used which lists the standards and procedures defined in the project CM Plan. Document any discrepancies found in the appropriate section of the CM Baseline Verification Report.</p> <p>Verify that the project is following the CM standards and procedures documented in the project CM Plan. This should be verified for each standard and procedure defined in the project CM Plan. Document any discrepancies found in the appropriate section of the CM Baseline Verification Report.</p>
6	Conclude Verification	<p>Complete the verification by documenting any conclusions in the Conclusions Section of the CM Baseline Verification Report.</p> <p>Make any final entries to the CM Baseline Verification History Log and file it for use during the next CM Baseline Verification.</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		<p>Attach to the CM Baseline Verification History Log any directory listings, inventory reports, configuration reports, and so forth that describes each current baseline. This accumulation of reports documents each baseline, which serves as the basis for future development and future verifications.</p> <p>Distributes the CM Baseline Verification Report to the audience defined in the project CM Plan.</p>
7	Resolve Verification Issues	<p>Generate and act on action items to address non-conformance issues in the CM Baseline Verification Report. Typically this task is performed by the person(s) who conduct(s) the Baseline Verification, but the issues may be passed onto the Contractor Project Manager to monitor and resolve.</p> <p>Review the CM Baseline Verification Report.</p> <p>Generate action items to address verification issues and assign them to an owner. The assigned owner conducts a root cause analysis of the verification issue(s) and a determination is made to see what caused the issue(s). The action items could be documented in the CM Baseline Verification Report or in the project's Action items list. Expected target date for closing of the action items should also be agreed upon and documented.</p> <p>Assigned owner(s) work(s) on completing the action items.</p> <p>If there are non-resolvable issues, they should be escalated according to documented escalation procedure.</p>

**RFP OSI 2046
CURRENT SYSTEM**

Step	Action	Description
		When the action items are completed, review completed action items with participant so that they may be documented as closed. This normally happens in internal team meetings.
8	Track Action Items	Monitor all action items, (addressing non-conformance issues documented in the CM Baseline Verification Report and generated by the Resolve Verification Issues task) until the action items have reached closure. The Contractor Project Manager will monitor these action items until they are closed.

Records Retention / Disaster Recovery / Archival

A plan was created for Disaster Recovery.

Managed and Controlled Work Products

Managed and Controlled is a level of configuration management applied to work products that are not part of a baseline, and are therefore not placed under Formal Configuration Management. However, these work products are important to project success and must still be maintained appropriately. Changes to these work products must be made in a controlled fashion, and steps should be taken to ensure the correct version of the work product is used. These work products are the responsibility of the current Contractor team.

The current Contractor Project Manager ensures these work products are controlled by designating someone as responsible for maintaining each work product.

- Any changes to the work products are forwarded to the designated person, who makes the changes as appropriate.
- The designated person assigns a version number to the work product, and increments the version number when changes are made.
- A formal, documented procedure is not required.

**RFP OSI 2046
CURRENT SYSTEM**

The following work products have been identified as Managed and Controlled, indicating that updates can be made by anyone on the current Contractor team and version control must be used.

Managed and Controlled Configuration Items
Baseline Verification History Log
Baseline Verification Report
Integration Test results
Operational Project Plan
Planning/replanning data
Project Standards and Procedures
Regression Test Plans, Procedures, and Cases
Statement of Work
Statement of Work for Subcontracts
Unit Test Plans, Procedures, and Cases

CI Naming Standards

PowerBuilder Standards

A variable name is of the following format:

<scope>[constant indicator]<type>_<name>

<scope>:

Scope	Prefix
Local	l?_
Instance	i?_
Shared	s?_
Global	g?_
Argument	a?_

[constant indicator]:

c constant

**RFP OSI 2046
CURRENT SYSTEM**

<type>:

Data Type	Prefix
Window	w_
MenuItem	m_
DataWindow	dw_
User object	uo_
Integer	i_
Unsigned integer	ui_
Long	l_
Unsigned long	ul_
Boolean	b_
String	s_
Double	db_
Real	r_
Decimal	c_
Blob	bb_
Character	ch_
DragObject	do_
Nonvisual	nv_
PowerObject	po_
DataWindowChild	dwc_
Mail session	ms_
Structure	str_
Transaction object	to_
Date	d_
Time	t_
DateTime	dt_

<name>:

lower-case-first capitalization; e.g.: variableName, workstationID

A pbl name is of the following format:

sfis<name>.pbl

Where name is a short one (1) or two (2) word description of the focus of the pbl; e.g., sfisaddupdate, sfisprint, sfissecurity, sfismain.

A PowerBuilder function has a name of the following format:

RFP OSI 2046 CURRENT SYSTEM

of_<name>

Where name is the name of the function. name should contain no underscores.

Although function names are entered in all-lowercase when created, they should be called from scripts with a first-letter-capitalization convention, with each successive word capitalized and acronyms fully capitalized; e.g., of_Print, of_DeleteFile, of_GetClientDOB.

A PowerBuilder function header has the following format:

```
//////////////////////////////////////////////////////////////////  
//  
// Statewide Finger Imaging System - SFIS  
//  
// Function: int of_ProcessPrint (as_fileName, ai_minutiae)  
// Object: n_cst_functions  
//  
// Processes the given print and returns a minutiae count.  
//  
// Arguments:  
// string as_fileName      Filename of print  
// ref int ai_minutiae     Reference variable in which to insert  
//                          minutiae count  
//  
// Returns:  
// int    1 Processing successful  
//        -1 Processing unsuccessful, unspecified error  
//        -2 Processing unsuccessful, print file does not exist  
//        null Necessary argument is null  
//  
// History:  
// 11.12.99/WC: Created as n_cst_functions.of_ProcessPrint  
// 03.05.01/WC: Modified for CSR 3.1-12  
// Added "file does not exist" return code.  
//-----  
//  
// Copyright (c) 1999-2001 State of California  
// ALL RIGHTS RESERVED  
//  
//////////////////////////////////////////////////////////////////
```

A PowerBuilder event header has the following format:

```
//////////////////////////////////////////////////////////////////  
//  
// Statewide Finger Imaging System - SFIS  
//  
// Event: Open  
// Object: w_printqueue  
//  
// Performs window initialization functions.  
//  
// History:  
// 04.17.01/DB: Created as w_printqueue.activate  
// 06.18.01/CA: Modified for CSR 4.2-9  
// Moved to open event and added initial SetFocus to cb_start.  
//-----  
//  
// Copyright (c) 2001 State of California  
// ALL RIGHTS RESERVED  
//  
//////////////////////////////////////////////////////////////////
```

**RFP OSI 2046
CURRENT SYSTEM**

////////////////////////////////////
OBJECT NAMING CONVENTIONS

Type	Prefix	Example
Window	w_	w_frame
Window function	wf_	wf_save_order()
Window structure	str_	str_kits
Menu	m_	m_frame
Menu function	mf_	mf_close_sheet()
Menu structure	str_	str_menu_stuff
Standard user object	u_	u_dw
User object function	uf_	uf_change_data_object()
User object structure	str_	str_columns
DataWindow object	d_	d_order_header
DataWindow control	dw_	dw_header_edit
Structure object	str_	str_keys
Query	q_	q_get_kits
Function object	f_	f_get_next_number()

OTHER POWERBUILDER STANDARDS

- Single spaces are placed before and after all operators and the assignment verb (-), and after each comma in a function parameter list.
- Tabs rather than spaces should be used to indent code to show inclusion in loops and other compound statements.
- Function calls and variables are coded in both upper and lowercase.
- Database commands (for example, INSERT, SELECT, and DECLARE CURSOR) should be coded in all capitals, with field names in lowercase and PowerBuilder bind variables using the same convention as normal PowerBuilder variables. PowerScript functions and commands should be coded with the first letter of each work capitalized (for example, If, RightTrim()). User-defined objects should be in all lowercase (for example, f_clear_mdi_children()).

RFP OSI 2046 CURRENT SYSTEM

- Line continuation should leave connecting tokens (for example, AND, +) at the end of the line, rather than at the beginning of the next line.
- One-line structures should be broken into multiple lines: (If ll_rows > 6 Then dw_report.Retrieve()) is incorrect.
- All objects used on a window or in construction of a user object are ideally inherited. This ensures consistency throughout development of the application and of future applications. Ideally, all windows are also inherited.
- In the search pbl path, the developer's private pbl comes first, followed by shared pbls, then ancestor pbls, and finally the application-specific pbls. A developer should check out objects into his/her private work library. All modifications to an object occur there, and once finished and tested, the objects are checked back into the originating library.
- Window size - w_main.resize(3658, 2401) // 800x600.
- Edit field – black text on white – 3d lowered.
- Column heading in grid – black text on silver – 3d raised – centered.
- Field label – black text on silver – no border – right justified.
- Default window background color – silver.
- Do not use buttonface as a replacement for silver on any control – it's helpful to set your development machine buttonface color to something other than silver to help identify when this might be occurring.
- Main window toolbar – aligned top – show text.
- Sheet window toolbar – aligned left – show text.
- Development libraries are located under p:\development, p:\production, and p:\test.
- Categorizing Objects in Libraries – functional groups or by database theme.
- Reference of bitmaps or icons using a relative path, for example - ..\resource\bitmap.bmp.

RFP OSI 2046

CURRENT SYSTEM

Note that the comment blocks in the legacy code look like:

```
/******  
/*  
/*This is a sample of a comment block used to draw attention to */  
/*the next batch of code. This is the 'old' way */  
/*  
/******
```

This style of commenting requires extra work for the developer, and does not produce a significant advantage in terms of drawing attention to the code block.

INLINE COMMENTING

The convention for inline commenting is:

```
int i; /* This is a sample of inline commenting */
```

WHITE SPACE

There is no need to add a lot of white space before or after the text. Again, this just creates extra work for the developer. One (1) space will be used. For example, compare this next sample with the previous one (1):

```
int i; /* This sample uses a lot of unneeded white space. */
```

INDENTATION

A common mistake is inconsistency when using indentation. SFIS standards for using indentations are to use two (2) spaces. This rule is for backward compatibility to legacy code. Examples of indentation are in the next code snippet:

```
{  
    :  
    :  
    int i; /* generic counter used in this example */  
    /* this is a sample of indentation in the main function block */  
    :  
    :  
    {  
        /* code within the block statement should be indented 2 spaces */  
        if ( i == 1 )  
        {  
            /* further example of indenting inside block */  
            printf( "\nNo argument used\n" );  
            break;  
        }  
        else  
        {  
            break;  
        }  
    }  
}
```

RFP OSI 2046 CURRENT SYSTEM

```
    }  
    :  
}
```

The above example is a rather simplistic demonstration, but underscores the samples of indenting in code.

Informix Considerations

Because there are embedded SQL calls in SFIS C code, there are special conventions used when declaring variables. Variables used by the Informix libraries are preceded by a '\$', for example:

```
$char TimeStamp[10];          /* dddhmmss */
```

Instead of using "#include" in the standard fashion (C), use '\$include':

```
$include datetime;  
$include sqlca;  
$include sqlstype;  
$include sqltypes;
```

In addition, when calling header files to be included at compile time, the include statement is preceded by the 'EXEC SQL' command:

```
EXEC SQL include comdbdef.h;
```

Database Standards

- All triggers in the database begin with the table name followed by an underscore and either insert or update depending on the function of the trigger. For example: tablename_update.
- All one-to-one temporary tables in the database begin with an "I".
- All data/lookup tables begin with a "T".
- All trigger tables begin with a "B".
- All indexes begin with an "I" followed by the table number and then the column being indexed. For example: i_tablenumber_columnname.

RFP OSI 2046 CURRENT SYSTEM

Documentation Standards

The naming standards for documentation are as follows:

- A descriptive name will be used, followed by the release number and/or the last updated date.
- The date format will be mmddyy.
- The first letter of each word will be capitalized.
- A spaced will be used to separate each component of the name.
- Example: SDD Release 003, CM Plan 101501.doc.
- Special naming standards for the System Operation and Support Plan (SOSP) are defined below:
- Each procedure will be given an identifier consisting of a number and a capital letter, followed by a dash, and a descriptive name.
- The number will correspond to the functional area in the Overview document and the letter will be the next sequential letter available.
- The first letter of each word will be capitalized.
- A space will be used to separate each component of the name.
- The name of the folder containing the SOSP procedures will include the release number and/or the last updated date.
- Examples: 3A - Production Batch Procedure.doc, SOSP 080602.

PROBLEM MANAGEMENT

The current Contractor and the SFIS Project Management Office (PMO) have developed and documented a problem management process built on a three (3) tiered Help Desk and a problem tracking software tool entitled Peregrine Systems ServiceCenter (ServiceCenter). The three (3) tiers of the Help Desk operates Monday through Friday from 7 a.m. to 7 p.m. Pacific Time, except for designated State holidays and include:

- SFIS Help Desk Support Team staffed by the current Contractor's Help Desk Agents;
- Advanced Help Desk Coordinators, SFIS Project Team members and the workstation maintenance vendor; and
- DTS network support and vendor support from HP, [Motorola/Printrak](#),
Informix and others.

Deleted: Printrak

RFP OSI 2046 CURRENT SYSTEM

Problems are reported to the Help Desk and entered into the ServiceCenter problem tracking system. This tool is utilized to track, escalate and report SFIS related problems. An online knowledge base is used to assist problem diagnosis and resolution.

Help Desk Ticket

All Help Desk calls received from the county sites are logged and given a reference number or logged with the reference number provided by the State, if available. Each incident is resolved by the Help Desk staff member receiving the call, unless escalation to the next level of System Operator or Systems Engineer is required. The staff member resolving the problem reports the resolution to the Help Desk staff member receiving the call for addition to the Help Desk log, which is given on a monthly basis to the State. Please refer to the Help Desk paragraphs of this document or to the Help Desk Document for a thorough description of the current Help Desk.

Outage Analysis

Outage Analysis is a detailed analysis of a production problem situation. The objective is to determine exactly what caused the problem and what can be done to prevent recurrence of the problem. Outage analysis requires a formal review or de-briefing of the problem situation with all involved parties. In this de-briefing, details of what happened, when it happened, how it happened and how the problem impacted the production environment are determined. A written report is created documenting the pertinent information about the incident. Most importantly, recommendations are developed that, when implemented, will prevent problem recurrence. The recommendations are converted into action items, issues, or change requests that are assigned to appropriate personnel for implementation and follow-up.

The current Contractor has documented an Incident Report process that is used for all major system outages. An overview of the incident is documented followed by detailed chronology of events. The Issues, Action Item, and Change Management processes are used to track and report on SFIS project related Issues, Action Items and changes.

The following example illustrates the incident report process.

Incident Reports – OPEN STATUS

Unknown/CIC process Froze: 09/10/2003 and continuing with no discernable pattern

**RFP OSI 2046
CURRENT SYSTEM**

DURATION: five (5) – ten (10) mins./ Occurrence

Incident Highlights:

Motorola/Printrak matching system stops processing matches and the current Contractor staff is required to restart the processes in order to get the Motorola/Printrak system to continue processing. This incident is currently being researched. Motorola/Printrak has staff investigating the issue and is working with the SFIS/current Contractor staff to solve the issue. Currently, when the CIC process freezes, match responses stop processing. The current Contractor staff restarts the process within five (5) minutes and end-users are normally not affected.

Deleted: Printrak

Deleted: Printrak

Deleted: Printrak

Lessons Learned:

- Motorola/Printrak has already ruled out caci01 and caci02. The do not believe they are causing the issue.
- Operators are using monitoring tools to help identify the issue and restart the process as soon as they freeze.
- Motorola/Printrak is looking into a possible corrupt .exe file.

Deleted: Printrak

Deleted: Printrak

Incident Details:

- The incident is occurring randomly and the system is being tracked to help resolve the issue.
- Motorola/Printrak has Nariz Oveja, Burro Boca, and Cerdo Oido assigned to the issue and they have been accessing the system via dial-up or coming into the site.

Deleted: Printrak

Follow-up Work:

- Incident is still being researched. Detailed report will follow.

Personnel Involved:

- Personnel involved include the current Contractor Staff and the current Motorola/Printrak Staff.

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

PROJECT POLICIES AND PROCEDURES

This section identifies program and project level policies, procedures, and standards including the following topics:

- Administrative policies, procedures, and arrangements.
- Work Standards.

Administrative Policies, Procedures, and Arrangements

The State currently provides the following:

- A full time Project Manager who will manage the project in terms of the State's responsibilities and deliverables as well as the Contractor's responsibilities and deliverables. The Project Manager may perform the following activities on behalf of the State:
 - Inspection of deliverables.
 - Verification of test results, staffing, Contractor activity in accordance with this Contractor's proposal and plan, and schedule and progress report accuracy.
 - Validation of certifications by Contractor; validation of cost results; validation of claims submitted to the State.
- A project team of approximately three (3) full-time equivalent individuals including the State's Project Manager (this number may be changed, at the State's discretion, at any time).
- Access to the work site during normal business hours, with a provision for twenty-four (24) hour, seven (7) day access during the critical project periods.
- Issue resolution and sufficient access to appropriate levels of State management to facilitate the decision making process.

Work Standards

The following are work standards for the current SFIS project:

- The Contractor uses the standard word-processing, relational database management product, project management, and spreadsheet products used by the State (Microsoft Word, Microsoft Access, Microsoft Project, and Microsoft Excel) at the version levels specified by the State, in the preparation of all project correspondence and deliverables. The Contractor supplies at least one (1) electronic copy of each deliverable.

RFP OSI 2046
CURRENT SYSTEM

- Deliverables and their updates are prepared by the scheduled dates for their completion. State personnel are responsible for reviewing and approving each deliverable; all deliverables and deliverable updates require a negotiated State turn-around time. Should revisions to the document be required by the State, the contractor provides revised versions of these deliverables in most cases.
- Deliverables contain the following certification: "I certify that this deliverable has been prepared in accordance with the relevant terms and conditions of the contract and that all related steps have been followed in its preparation." The SFIS Project Manager or his/her designee signs contracted Deliverables as complete. Completion of deliverables and their updates are managed through the State's Issue Management process using the PACS.
- An Issue Tracking Database (part of the PACS) is used and maintained by the State through the life of the project to record and track relevant issues and decisions that are made about areas of concern to the Project Team members, system end users, and the Contractor. The Contractor assists in tracking each issue's progress and advises the State if a delay in resolution will impact the project schedule. The current Contractor can view the PACS' contents through a workstation located at the DTS South Annex. All updates to the PACS are performed by the Project's PMO.
- The Contractor stores the project work papers by task numbers that have been assigned to the project tasks corresponding to the Project Plan. In addition, Project Workbooks store work papers not related to specific task numbers; these are stored in the Contractors' workspace at the Central Site. All project work papers and Project Workbooks stored by the Contractor are made available to the State with a one (1) hour notice to the Help Desk. Project work papers and Project Workbooks developed in connection with the SFIS project are the property of the State.

**RFP OSI 2046
CURRENT SYSTEM**

L. DOCUMENTATION AND REPORTS

BROCHURES AND OTHER MATERIALS

The current Contractor is responsible for making updates, printing, storing, and distributing the existing SFIS publication materials:

- Brochures;
- Video; and
- Posters.

The SFIS publication materials were initially distributed to all counties. Now, only SFIS brochures are available by request to the Contractor. SFIS brochures are available in the following languages:

- English;
- Spanish;
- Chinese;
- Cambodian;
- Russian; and
- Vietnamese.

Design Publication Materials

The Contractor developed, implemented, and supported a comprehensive public information campaign that supported the State's conversion needs at the beginning of the project. State and Contractor personnel identified the specific materials to be produced during system design. In support of this campaign, the Contractor team designed brochures, pamphlets, and other materials, such as bulletins, posters, and short videos, for distribution to public and private agencies in order to announce the implementation of SFIS and in order to inform the public of the positive benefits of the system.

**RFP OSI 2046
CURRENT SYSTEM**

Provide Publication Materials

The current Contractor is responsible for providing brochures in sufficient quantity for the life of the SFIS Contract. This material became State property and has been in circulation during the entire term of the current contract to help gain public support and acceptance of SFIS. SFIS videos were provided to all counties; the State also provided written permission to the counties to copy the videos. Videos are no longer available from the current Contractor. Both the State and the contractor have archival copies of all materials. Brochures are available for printing from the CDSS website.

Languages For Publication Materials

It is currently a contract requirement for brochures to be provided in the following six (6) languages:

Cambodian	Chinese	English
Russian	Spanish	Vietnamese

Deliver Publication Materials

Currently, the Contractor must deliver brochures to the requesting site within ten business days of the date the order was received. The current Contractor initially delivered materials ordered by the State in the specified types and quantities to the specified locations throughout California.

Approach to Public Information Campaign

Since SFIS was implemented, the project has not had a Public Information Campaign. The initial public information campaign used a multi-part strategy aimed at addressing the concerns of the advocacy groups, educating the general public and potential social services clients on the benefits of the program, and easing concerns of the social services clients related to finger imaging.

DOCUMENTATION REQUIREMENTS

Complete Set of Reference Materials

Currently, all county user reference materials are created and maintained by the State and distributed via the SFIS website. The current reference materials are as follows:

RFP OSI 2046 CURRENT SYSTEM

- User Guides (Client Input, Fraud Investigation, System Administration and Portable Input Workstation);
- Resolution Guide;
- Training Presentations (Client Input, Fraud Investigation, System Administration and Portable Input Workstation);
- Training Checklists (Client Input, Fraud Investigation, System Administration and Portable Input Workstation);
- Training Workbooks (Client Input, Fraud Investigation, System Administration and Portable Input Workstation);
- Web Based Training Modules;
- County Coordinator List; and
- Release Materials (Instructions, Description and Presentations).

Each county workstation was initially given a complete set of user guides and training workbooks pertaining to that workstation's training and operations.

Documentation Updates

The current Contractor provides State and county users updates (the latest available to their other commercial customers) to COTS hardware, firmware, software, and internal documentation at no additional cost.

The State currently provides all updates to the State-created user reference materials and the On-Line Help text.

Documentation

The current Contractor provides and maintains the following system documentation:

- Help Desk Document – A contract deliverable that details the ongoing operations and characteristics of the SFIS Help Desk. Topics include:
 - Objectives and Functions;
 - Help Desk Structure;
 - Help Desk Implementation;
 - Help Desk Processes;
 - Information Sources and Reports; and
 - Telephone Numbers.

RFP OSI 2046
CURRENT SYSTEM

- System Operation and Support Plan (SOSP) – A contract deliverable that details the ongoing Central Site operations of SFIS. The manual describes batch cycle schedules, report distribution, online system response, uptime monitoring, and other day-to-day activities needed to support SFIS. Topics include:
 - Staffing;
 - Scheduled Production Operating Procedures;
 - Production Software Recovery Procedures;
 - Test and Training Operating Procedures;
 - Test Software Recovery Procedures;
 - Maintenance and Repair;
 - Configuration Management Procedures;
 - Verification Procedure;
 - Help Desk Operations;
 - Documentation Procedures;
 - Grayscale Extraction; and
 - Who to Call.
- Transfer Plan – A contract deliverable that details the tasks, responsibilities, and timeframes for transferring the system operation from the current Contractor to a new contractor without disruption of service. Topics include:
 - Transfer Management;
 - Project Schedule;
 - Hardware;
 - Functional Areas;
 - Vendors;
 - Sample Replacement Schedule Letter;
 - Sample Implementation Install Checklist; and
 - Sample Project Schedule.
- Disaster Recovery Plan – A contract deliverable that details the plan for the recovery of the system in the event of a disaster. Designed to conform to SAM requirements. Topics include:
 - Administrative Information;
 - Recovery Strategy;
 - Damage Recognition;
 - Damage Assessment;
 - Mobilization of Personnel;
 - Recovery Plan Implementation;
 - Primary Site Restoration/Relocation;
 - Emergency Contact Lists;

RFP OSI 2046 CURRENT SYSTEM

- Recovery Operations Center Assignment Checklists; and
- Damage Assessment and Disaster Classification Forms.
- Configuration Management Plan (CMP) — Defines configuration management activities and organization for the SFIS project. Topics include:
 - Configuration Management Organization;
 - Formal Configuration Management Activities;
 - Managed and Controlled Work Products; and
 - Configuration Item Naming Standards.
- All Source Code (placed in escrow) – A contract deliverable that includes copies of all SFIS application software source code including all fixes to custom software held in escrow, by a third party (DSI Technology Escrow Services, Inc), for the life of the system.
- System Design Document (SDD) — A contract deliverable that describes detailed software processing logic and workflow. Describes the programs, tables, reports, and files that comprise SFIS, inputs and outputs, the security package, and maintenance methods. Topics included in the SDD include:
 - SFIS Architecture;
 - Central Site Database Design;
 - Online Functional Design;
 - Security;
 - SCI/SFIS Interface;
 - Batch Processing; and
 - Backup and Recovery.

SFIS GENERATED REPORTS

Report Listing

The following paragraphs list SFIS generated and mandatory (under the current contract) reports produced during the Daily, Weekly, and Monthly Batch Cycle. After the reports are created during the batch cycle, they will be available for printing at the county site, CDSS, and OSI. Operators with the appropriate security level will be able to print the reports within their site by accessing the Print function. Please refer to the User Guides for a description of how to use the Print function.

**RFP OSI 2046
CURRENT SYSTEM**

Daily Reports

Report Name: CCW
Program Number: caap4100

Description:

The Case Carrying Worker (CCW) report gives the status of all open cases for a particular site and Eligibility Worker. This daily report lists the name, CIN, LIN, and program type (CalWORKs, Food Stamp, and/or GA/GR), sorted by name.

REPORT: CS4100D
SITE ID: 9802
WORKER: 3672

STATEWIDE FINGERPRINT IMAGING SYSTEM
CCW REPORT
DAILY

PROCESSING DATE: 04/06/2000
PAGE: 1

NAME	CIN	LIN	CalWORKs	FOODSTAMP	GA/GR
FORTZ, MONTAG	74736791H	98-32-8542159-2-02			Y
TIBURON, JIMMY	73601022H	98-32-8542159-2-02			Y

RFP OSI 2046 CURRENT SYSTEM

Report Name: Activity Summary

Program Number: caap4102

Description:

The Activity Summary report is generated from the Workstation Transaction table and gives a summary of daily operational activities per site ID. It lists the operator ID, number of queries, adds, updates, and exemptions, sorted by operator ID.

REPORT: CS4102D
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
ACTIVITY SUMMARY
DAILY

PROCESS DATE: 03/04/2000
PAGE: 1

OPERATOR ID	TOTAL QUERIES	TOTAL ADDS	TOTAL UPDATES	TOTAL EXEMPTIONS
98AASO	0	0	0	0
98ABOV	0	0	0	0
98ADUR	0	0	0	0
98AGSP	0	0	0	0
98AHNL	0	0	0	0
98ALFI	0	0	0	0
98AREA	4	1	0	0
98AWGG	0	0	0	0
98AWQA	0	0	0	0
98EJJI	0	0	0	0
98ELOL	0	22	0	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: Stored Transactions 21 Days or Older

Program Number: caap4124

Description:

The Stored Transactions twenty-one (21) Days or Older report is generated from the Stored Transaction Expire table (t999_st_expire) and shows all stored transactions that exist on the county's workstations that are twenty-one (21) days or older. The report is sorted by workstation ID and identifies the operator ID, name of client, CIN, DOB, create date and the number of days old. The report is used by the SFIS Help Desk staff and the State (OSI) to ensure that stored transactions are processed in a timely manner.

REPORT: C34124D STATEWIDE FINGERPRINT IMAGING SYSTEM PROCESS DATE: 05/16/2003
 SITE ID: 9802 STORED TRANSACTIONS ON HARD DRIVE (21 DAYS OR GREATER) PAGE: 1
 RAILY

WRST ID	OPER ID	NAME	CIN	DOB	CREATE DATE	DAYS OLD
9802A	98AYCM	CLEAVER, JUNE		01/02/1966	01/30/2003	35
9802A	98AYLP	HOOVER, APRIL		01/02/1944	03/20/2003	36
9802B	98AYOU	BOGGER, JOSE		01/02/1966	03/20/2003	36
9802C	98AACH	CLASS, CLONE		01/02/1966	10/29/2002	178
9802C	98AASJ	JOHNSON, DICK		01/02/1966	03/20/2003	36
9802D	98ACH	THIB, CAROL		01/02/1966	01/30/2003	35
9802D	98ACH	APT, JENNIE		01/02/1966	03/20/2003	36
9802U	98ABOV	GLASS, TIFFANY	75811602H	01/02/1966	11/19/2002	157
9802T	98ABOV	CUPPES OUP, TEA		01/02/1966	11/19/2002	157
9802T	98ABOV	THOUSE, ROCK		01/02/1966	11/20/2002	156
9802T	98ADUR	SEEKER, RUSE	74102202H	01/02/1966	03/28/2003	28

**RFP OSI 2046
CURRENT SYSTEM**

Weekly Reports

Report Name: CCW

Program Number: caap4200

Description:

The Case Carrying Worker (CCW) report is generated from the PCN, Print, and LIN tables and gives weekly status for all open cases by site ID. It lists name, CIN, LIN, and program type (CalWORKs, Food Stamp, or GA/GR), sorted by name.

REPORT: CS4200W
SITE ID: 9802
WORKER: NONE

STATEWIDE FINGERPRINT IMAGING SYSTEM
CCW REPORT
WEEKLY

PROCESSING DATE: 03/04/2000
PAGE: 1

NAME	CIN	LIN	CalWORKs	FOODSTAMP	GA/GR
FISCAL, SHYLOCK	85219291H	36-46-4278976-1-31	Y		
PREZ, CIO	45977251H	36-41-2032365-4-87		Y	

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Closed Search Misses

Program Number: caap4201

Description:

The Closed Search Misses report is generated from the Matched, PCN, and Temp Case Master tables and summarizes by site ID the daily Closed Search verification failures returned by SFIS. This weekly report lists the workstation ID, CIN, LIN, name, verify date, and verify ID, sorted by workstation ID.

REPORT: CS4201W
SITE ID: 9802
WORKER: NONE

STATEWIDE FINGERPRINT IMAGING SYSTEM
CLOSED SEARCH MISSES REPORT
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

WORKSTATION ID	CIN	LIN	NAME	VERIFY DATE	VERIFY ID
98022	75218881H	49-49-4879976-1-31	ALGER, HORATIO	03/04/2000	
98022	75111402H	46-46-5666789-7-13	MUDD, POPSICLE	03/04/2000	

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Conversion Detail

Program Number: caap4203

Description:

The Conversion Detail report is generated from the Print, LIN, and PCN tables and shows a detail compilation of case records converted by each Eligibility Worker per site ID. This weekly report identifies the CIN, LIN, name, sex, date of birth, and program type (CalWORKs, Food Stamps, GA/GR).

REPORT: CS4203W
SITE ID: 9802
WORKER:

STATEWIDE FINGERPRINT IMAGING SYSTEM
CONVERSION DETAIL REPORT
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

CIN	LIN	NAME	SEX	DOB	CalWORKs	FOODSTAMPS	GA/GR
90833377A	16-09-5982461-7-23	JOHNSON, BEN	M	10/13/42	Y		

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Opened Search Duplicate Record

Program Number: caap4204

Description:

The Open Search Duplicate Record report is generated from the PCN, Matched, and LIN tables and summarizes by site ID duplicate record matches received, processed for administrative clearance, and referred to Fraud Investigators. This weekly report identifies the name, CIN, LIN, match date, resolution code, and verify ID.

REPORT: CS4204W
SITE ID: 9802
WORKER: NONE

STATEWIDE FINGERPRINT IMAGING SYSTEM
OPENED SEARCH DUPLICATE RECORD
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

NAME	CIN	LIN	MATCH DATE	RESOLUTION	VERIFY ID
MARLOWE, CHRISTOPHER	75439992H	19-34-SB5A22F-1-05	03/04/2000	PF	
WILDER, SCHRAG	71677791H	64-64-377764-8-79			

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Fingerprint Exemptions

Program Number: caap4205

Description:

The Fingerprint Exemptions report is generated from the Case Master table and summarizes by site ID the weekly temporary and permanent exemptions by exemption type. This weekly report lists the operator ID, temporary exemptions, and permanent exemptions, sorted by operator ID.

REPORT: CS4205W
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
FINGERPRINT EXEMPTIONS REPORT
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

OPERATOR ID	TR FINGERPRINT	TL FINGERPRINT	PR FINGERPRINT	PL FINGERPRINT
01A001	6	6	0	1

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Fraud Investigation Status

Program Number: caap4206

Description:

The Fraud Investigation Status report is generated from the Matched, PCN, and LIN tables and gives weekly status for referred cases per county. It lists the match date, site ID, name, CIN, LIN, fraud ID, fraud disposition and date, sorted by match date.

REPORT: CS4206W
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
FRAUD INVESTIGATION STATUS
WEEKLY

PROCESS DATE: 03/05/2000
PAGE: 1

MATCH DATE	SITE ID	NAME	CIN	LIN	FRAUD ID	FRAUD DISPOSITION	DISPOSITION DATE
03/04/2000	9802	WAYNE, BRUCE	77659991H	46-46-4899976-1-31			
	9802	KENT, CLARK	75888991H	46-46-4877776-1-31			

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Operator Input Activity

Program Number: caap4207

Description:

The Operator Input Activity report is generated from the Workstation Transaction table and reported by site and operator ID. It lists the name, LIN, CIN, date, hour, fingerprint exemptions, function type, and program type (CalWORKs, Food Stamps, or GA/GR), sorted by name.

REPORT: CS4207W
OPERATOR ID: 98ELOL
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
OPERATOR INPUT ACTIVITY REPORT
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

NAME	LIN	CIN	DATE	HOUR	RIGHT FINGER	LEFT FINGER	FUNCTION TYPE	CalWORKs	FOOD STAMPS	GA/GR
BATSON, BILLIE	98-76-6464654-5-49	78787802H	03/04/2000	12:30			ADD		Y	
MARVEL, MARY	98-77-6469694-2-66	71510061H	03/04/2000	12:33			ADD			Y

RFP OSI 2046 CURRENT SYSTEM

Report Name: Query

Program Number: caap4208

Description:

The Query report is generated from the Workstation Transaction and Security Transaction tables and shows weekly Operator database queries per site. It lists the operator ID, workstation ID, operator name, query, date, and item sorted by operator ID.

REPORT: CS4208W
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
QUERY REPORT
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

OPERATOR ID	WKST ID	OPERATOR NAME	QUERY	DATE	ITEM
98AREA	98021	CLIENT-INPUT, TRAINING	FC	03/04/2000	RUSSELL, RUSS
98AREA	98021	CLIENT-INPUT, TRAINING	FC	03/04/2000	RUSSELL, RUSTY
98AREA	98021	CLIENT-INPUT, TRAINING	FC	03/04/2000	RUSSELL, RUSS
98AREA	98021	CLIENT-INPUT, TRAINING	SI	03/04/2000	76388061H
98AREA	98021	CLIENT-INPUT, TRAINING	SI	03/04/2000	90001713H
98AWGG	98021	CLIENT-INPUT, TRAINING	FC	03/04/2000	JACOBS, SETH
98AWGG	98021	CLIENT-INPUT, TRAINING	FC	03/04/2000	JACOBS, SETH

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: SFIS Opened Search Match

Program Number: caap4210

Description:

The SFIS Opened Search Match report is generated from the Matched and PCN tables and summarizes by site ID daily verified fingerprint matches returned by SFIS. This weekly report identifies the CIN, LIN, name, match date, disposition code and verify ID, sorted by CIN.

REPORT: CS4210W
WORKER: NONE
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
SFIS OPENED SEARCH MATCH REPORT
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

CIN	LIN	NAME	MATCH DATE	DISPOSITION	VERIFY ID
75168851H	98-76-6523422-1-11	HUACHINANGO, MARY	03/04/2000		
75375502H	98-76-7866699-8-65	ANGUILA, PETER			
75651502H	19-30-CAAK203-1-04	PERCA, NINA	03/04/2000		
75603502H	55-65-6798786-1-02	LUCIO, MARI			

RFP OSI 2046 CURRENT SYSTEM

Report Name: Operators Login and Logout

Program Number: caap4212

Description:

The Operator Login and Logout report is generated from the Operator Transaction table and tracks Operator login and logout times per site. This weekly report lists operator ID, operator name, workstation ID, date, login time, and logout time.

REPORT: CS4212W
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
OPERATORS LOGIN AND LOGOUT
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

OPERATOR ID	OPERATOR	WKST ID	DATE	LOG-IN	LOG-OUT
98AHJQ	CLIENT-INPUT, TRAINING	98021	03/04/2000	13:18	P
98ALHN	CLIENT-INPUT, TRAINING	98021	03/04/2000	19:03	P
98AREA	CLIENT-INPUT, TRAINING	98021	03/04/2000	10:43	10:44
			03/04/2000	13:20	13:37
			03/04/2000	13:38	P
			03/04/2000	13:38	P
			03/04/2000	14:05	14:12
			03/04/2000	14:40	P
			03/04/2000	14:41	P
			03/04/2000	14:41	15:02
98AUGD	CLIENT-INPUT, TRAINING	98021	03/04/2000	20:27	21:33
			03/04/2000	21:59	P
			03/04/2000	22:18	22:45
98AWGG	CLIENT-INPUT, TRAINING	98021	03/04/2000	15:26	16:01
98ALHN	CLIENT-INPUT, TRAINING	98022	03/04/2000	20:28	21:33
			03/04/2000	21:59	P

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Unacceptable Quality Prints
(30 to 59 Days Old)

Program Number: caap4215

Description:

The Unacceptable Quality Prints (thirty (30) to fifty-nine (59) Days Old) report is generated from the LIN, Case Master, PCN and Print tables. It compiles by site ID unacceptable quality (UQ) prints on the SFIS database that are thirty (30) to fifty-nine (59) days old. This weekly report identifies the name, LIN, CIN, date, and actual number of days old.

REPORT: CS4215W
WORKER:
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
UNACCEPTABLE QUALITY PRINTS (30 TO 59 DAYS OLD)
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

NAME	LIN	CIN	DATE	DAYS OLD
HIPOGLOSO, SYDNEY	38-90-9094566-0-12	978904837A	10/04/1999	45

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Temporarily Exempted Fingerprints
(Over 60 Days Old)

Program Number: caap4216

Description:

The Temporarily Exempted Fingerprints (Over sixty (60) Days Old) report is generated from the LIN, Case Master, PCN and Print tables. It compiles by site ID temporarily exempted fingerprints on the SFIS database over sixty (60) days old. This weekly report identifies the name, LIN, CIN, and date.

REPORT: CS4216W
WORKER:
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
TEMPORARILY EXEMPTED FINGERPRINTS (OVER 60 DAYS OLD)
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

NAME	LIN	CIN	DATE
CANGREJO, ADOLPH	24-90-9066686-0-12	99222237A	12/04/1999

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Unacceptable Quality Prints
(Over 60 Days Old)

Program Number: caap4217

Description:

The Unacceptable Quality Prints (Over sixty (60) Days Old) report is generated from the LIN, Case Master, PCN, and Print tables. It compiles by site ID unacceptable quality (UQ) prints on the SFIS database over sixty (60) days old. This weekly report identifies the name, LIN, CIN, and date.

REPORT: CS4217W
WORKER:
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
UNACCEPTABLE QUALITY PRINTS (OVER 60 DAYS OLD)
WEEKLY

PROCESS DATE: 03/04/2000
PAGE: 1

NAME	LIN	CIN	DATE
MEJILLON, DALE	24-90-9009887-0-12	99765837A	12/15/2000

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Photo Retake
(Over 60 Days Old)

Program Number: caap4219

Description:

The Photo Retake (Over sixty (60) Days Old) report is generated from the LIN, Photo, PCN, Print, Case Master, and Batch Date tables and compiles by site ID all photo retakes on the SFIS database over sixty (60) days old. This weekly report identifies the name, LIN, CIN, and date.

REPORT: CS4219W
WORKER:
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
PHOTO RETAKE (OVER 60 DAYS OLD)
WEEKLY

PROCESS DATE: 03/24/2000
PAGE: 1

NAME	LIN	CIN	DATE
AUTRY, CHAMPION	24-90-9975387-0-12	99552837A	12/15/2000

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Open Search Transaction

Program Number: caap4220

Description:

The Open Search Transaction report summarizes weekly Open Search transactions, and identifies the number of records with fingerprints added during the month either through SFIS or Automated Fingerprint Imaging Reporting and Match system (AFIRM) Conversion. It also indicates the number of clients removed via the Remove Images process.

REPORT: CS4220W

STATEWIDE FINGERPRINT IMAGING SYSTEM
OPEN SEARCH TRANSACTION REPORT
WEEKLY

PROCESS DATE: 03/05/2000
PAGE: 1

Total Clients With Fingerprint (start of period)	=	85
Clients Added With Fingerprint (during period)	=	68
Online SPIS (68)		
AFIRM's OPEN SEARCH (0)		
Total Clients With Fingerprint (end of period)	=	258
Removed Client(s)	=	0

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: AFIRM Images Converted to SFIS

Program Number: caap4221

Description:

The AFIRM Images Converted to SFIS report weekly summarizes AFIRM images converted to SFIS captured images. It identifies the number of records with fingerprints added through AFIRM Conversion and the number replaced by SFIS images. It also indicates the total number of each type of case.

REPORT: CS4221W

STATEWIDE FINGERPRINT IMAGING SYSTEM
AFIRM IMAGES CONVERTED TO SFIS
WEEKLY

PROCESS DATE: 03/05/2000
PAGE: 1

Subtotal AFIRM images		=	0
AFIRM right images	(0)		
AFIRM left images	(0)		
Subtotal SFIS images		=	0
SFIS right images	(0)		
SFIS left images	(0)		
Total AFIRM Images		=	0
AFIRM cases		=	0
SFIS cases		=	0
Total AFIRM Cases		=	0

**RFP OSI 2046
CURRENT SYSTEM**

Monthly Reports

Report Name: Fraud X-County Mismatch

Program Number: caap4222

Description:

The Fraud X-County Mismatch report summarizes by county ID the fraud mismatches for the month. It identifies the match date, site ID, name, CIN, LIN, fraud ID, fraud disposition, and disposition date.

REPORT: CS4222M
COUNTY: 38

STATEWIDE FINGERPRINT IMAGE SYSTEM
FRAUD X-COUNTY MISMATCH
MONTHLY

PROCESS DATE: 03/31/2000
PAGE: 1

MATCH DATE	SITE ID	NAME	CIN	LIN	FRAUD ID	FRAUD DISPOSITION	DISPOSITION DATE
-----	-----	-----	-----	-----	-----	-----	-----
03/30/2000	3801 4203	CAMARON, JEFFREY ALMEJA, BILLY	92228715A 71531502H	38-54-5654654-6- 04 42-54-6546546-5- 06			
03/30/2000	3802 1910	VENERA, JOHN OSTRA, BERT	75904602H 72005302H	38-98-4546546-5- 06 19-65-4654654-6- 04			

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: CCW
Program Number: caap4300

Description:

The CCW report is generated from the PCN, Print, and LIN tables and gives monthly status for all open cases by site ID. It lists name, CIN, LIN, and program type (CalWORKs, Food Stamp, or GA/GR), sorted by name.

REPORT: CS4300M
SITE ID: 3403
WORKER: Y3M

STATEWIDE FINGERPRINT IMAGING SYSTEM
CCW REPORT
MONTHLY

PROCESSING DATE: 04/30/2002
PAGE: 1

NAME	CIN	LIN	CalWORKs	FOODSTAMP	GA/GR
-----	-----	-----	-----	-----	-----
HOWARD, SHEMP	74079758D	34-30-0567654-1-34	Y		
NESSELRODE, CLEOPATRA	70672568D	34-07-0432884-0-34		Y	

RFP OSI 2046 CURRENT SYSTEM

Report Name: Closed Search Misses

Program Number: caap4301

Description:

The Closed Search Misses report is generated from the Matched, Temp Case Master, and LIN tables, and summarizes by site ID the daily Closed Search verification failures returned by SFIS for the month. It lists the workstation ID, CIN, LIN, name, verify date, and verify ID, sorted by workstation ID.

REPORT: CS4301M
SITE ID: 9802
WORKER: NONE

STATEWIDE FINGERPRINT IMAGING SYSTEM
CLOSED SEARCH MISSES REPORT
MONTHLY

PROCESS DATE: 03/22/2000
PAGE: 1

WORKSTATION ID	CIN	LIN	NAME	VERIFY DATE	VERIFY ID
98022	75000851H	46-41-2042165-4-87	FLYWHEEL, RUFUS	03/05/2000	
98022	73571502H	65-41-6546820-0-19	LAPONG, CARL	03/05/2000	

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Activity Summary

Program Number: caap4302

Description:

The Activity Summary report is generated from the Activity Count table and summarizes by site ID operational activities for the month. It identifies the operator ID, total queries, total adds, total updates, and total exemptions, sorted by operator ID.

REPORT: CS4302M
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
ACTIVITY SUMMARY
MONTHLY

PROCESS DATE: 03/22/2000
PAGE: 1

OPERATOR ID	TOTAL QUERIES	TOTAL ADDS	TOTAL UPDATES	TOTAL EXEMPTIONS
98AASO	0	0	0	0
98ABOV	0	0	0	0
98ADUR	0	0	0	0
98AGSP	0	0	0	0
98AHNL	0	0	0	0
98ALFI	0	0	0	0
98AREA	4	1	0	0
98AWGG	0	0	0	0
98AWQA	0	0	0	0
98EJJI	0	0	0	0
98ELOL	0	22	0	0

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Conversion Detail

Program Number: caap4303

Description:

The Conversion Detail report is generated from the LIN, Print, and PCN tables and compiles the number of case records converted for the month. It identifies the CIN, LIN, name, sex, date of birth, and program type (CalWORKs, Food Stamps, and GA/GR).

REPORT: CS4303M
SITE ID: 9802
WORKER:

STATEWIDE FINGERPRINT IMAGING SYSTEM
CONVERSION DETAIL REPORT
MONTHLY

PROCESS DATE: 03/22/2000
PAGE: 1

CIN	LIN	NAME	SEX	DOB	CalWORKs	FOODSTAMPS	GA/GR
90877177A	38-09-5975761-7-23	LANGOSTA, JOSE	M	10/13/42	Y		

RFP OSI 2046 CURRENT SYSTEM

Report Name: Conversion Summary

Program Number: caap4303s

Description:

The Conversion Summary report is generated from PCN table and summarizes by county ID the monthly Conversion cases grouped by the program type (GR/GA, CalWORKs, FS, GR/CalWORKs, GR/FS, CalWORKs/FS, and CalWORKs/FS/GR).

REPORT: CS4303S
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
CONVERSION SUMMARY
MONTHLY - CDSS

PROCESS DATE: 03/31/2000
PAGE: 1

GR/GA	CalWORKs	FS	GR/CalWORKs	GR/FS	CalWORKs/FS	CalWORKs/FS/GR
23	37	60	83	60	97	54

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: Opened Search Duplicate Record Summary

Program Number: caap4304

Description:

The Opened Search Duplicate Record Summary report is generated from the PCN table and summarizes by county ID the duplicate record hits received for the month. It lists the number of duplicate record matches by program type (GR/GA, CalWORKs, FS, GR/CalWORKs, GR/FS, CalWORKs/FS, and CalWORKs/FS/GR).

REPORT: CS4304S
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
OPENED SEARCH DUPLICATE RECORD SUMMARY
MONTHLY - CDSS

PROCESS DATE: 03/31/2000
PAGE: 1

GR/GA	CalWORKs	FS	GR/CalWORKs	GR/FS	CalWORKs/FS	CalWORKs/FS/GR
41	32	73	0	0	3	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: Fingerprint Exemption

Program Number: caap4305

Description:

The Fingerprint Exemption report is generated from the Workstation Transaction table and summarizes by site ID temporary and permanent exemptions, by exemption type, for a given month. It identifies the operator ID, temporary exemptions, and permanent exemptions.

REPORT: CS4305M
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
FINGERPRINT EXEMPTION REPORT
MONTHLY

PROCESS DATE: 03/22/2000
PAGE: 1

OPERATOR ID	TR FINGERPRINT	TL FINGERPRINT	PR FINGERPRINT	PL FINGERPRINT
01A001	6	6	0	1

RFP OSI 2046 CURRENT SYSTEM

Report Name: Fraud Investigation Status

Program Number: caap4306

Description:

The Fraud Investigation Status report is generated from PCN, Matched, and LIN tables and summarizes status for referred cases showing investigation status (pending, in-progress, complete). It lists the match date, site ID, name, CIN, LIN, fraud ID, fraud disposition and date, sorted by match date.

REPORT: CS4306M
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
FRAUD INVESTIGATION STATUS
MONTHLY

PROCESS DATE: 03/31/2000
PAGE: 1

MATCH DATE	SITE ID	NAME	CIN	LIN	FRAUD ID	FRAUD DISPOSITION	DISPOSITION DATE
03/04/2000	9802	DUMONT, MARGARET	75789991H	46-46-4874476-1-31			
	9802	DUMONT, MARGARET	75789991H	46-46-4874476-1-31			
03/04/2000	9802	JEEVES, MAHATMA	75269402H	46-46-5462789-7-13			
	9802	JEEVES, MAHATMA	75269402H	46-46-5462789-7-13			

RFP OSI 2046 CURRENT SYSTEM

Report Name: Newly Added Person

Program Number: caap4307s

Description:

The Newly Added Person report is generated from the PCN table and summarizes by county ID the total number of new records added, grouped by the program type (GR/GA, CalWORKs, FS, GR/CalWORKs, GR/FS, CalWORKs/FS, and CalWORKs/FS/GR).

REPORT: CS4307S
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
NEWLY ADDED PERSON
MONTHLY - CDSS

PROCESS DATE: 03/31/2000
PAGE: 1

GR/GA	CalWORKs	FS	GR/CalWORKs	GR/FS	CalWORKs/FS	CalWORKs/FS/GR
41	32	73	0	0	3	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: Permanent Exemptions

Program Number: caap4308s

Description:

The Permanent Exemptions report is generated from the Case Master and PCN tables and summarizes by county ID the number of permanent fingerprint exemptions for each program type (GR/GA, CalWORKs, FS, GR/CalWORKs, GR/FS, CalWORKs/FS, and CalWORKs/FS/GR).

REPORT: CS4308S
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
PERMANENT EXEMPTIONS REPORT
MONTHLY - CDSS

PROCESS DATE: 03/31/2000
PAGE: 1

FINGERPRINT	GR/GA	CalWORKs	FS	GR/CalWORKs	GR/FS	CalWORKs/FS	CalWORKs/FS/GR
PR	0	0	0	0	0	0	0
PL	0	0	1	0	0	0	0
PR/PL	0	0	0	0	0	0	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: SFIS Opened Search Match

Program Number: caap4310

Description:

The SFIS Opened Search Match report is generated from the Matched and PCN tables and summarizes by site ID total verified fingerprint matches returned by SFIS for a given month. It lists the CIN, LIN, name, match date, disposition, and verify ID, sorted by CIN.

REPORT: CS4310M
WORKER: NONE
SITE ID: 9802

STATEWIDE FINGERPRINT IMAGING SYSTEM
SFIS OPENED SEARCH MATCH REPORT
MONTHLY

PROCESS DATE: 03/22/2000
PAGE: 1

CIN	LIN	NAME	MATCH DATE	DISPOSITION	VERIFY ID
75651502H	19-30-CAAK203-1-04	TRUCHA, NINA	03/04/2000		
75603502H	55-65-6798786-1-02	CARPA, MARI			
75237402H	45-45-4878787-4-85	PULPO, DINA	03/04/2000		
75232502H	44-54-5489798-7-89	CALAMAR, SOPIE			

RFP OSI 2046 CURRENT SYSTEM

Report Name: SFIS Response Time Summary

Program Number: caap4312

Description:

The SFIS Response Time Summary report works with the PCN table to summarize Central SFIS response time performance by county ID. It lists the site ID, priority level, minimum time, maximum time, average time, and maximum exceed requirement count, sorted by site ID.

REPORT: CS4312M
COUNTY: 01

STATEWIDE FINGERPRINT IMAGING SYSTEM
SFIS RESPONSE TIME SUMMARY REPORT
MONTHLY

PROCESS DATE: 03/31/2000
PAGE: 1

SITE ID	PRIORITY LEVEL	MINIMUM TIME	MAXIMUM TIME	AVERAGE TIME	MAXIMUM EXCEED REQ
0101	1	0 00 : 00	0 00 : 00	0 00 : 00	0
0101	3	0 00 : 00	0 00 : 00	0 00 : 00	0
0101	7	0 00 : 00	0 00 : 00	0 00 : 00	0
0102	1	0 00 : 00	0 00 : 00	0 00 : 00	0
0102	3	0 00 : 00	0 00 : 00	0 00 : 00	0
0102	7	0 00 : 00	0 00 : 00	0 00 : 00	0
0103	1	0 00 : 00	0 00 : 00	0 00 : 00	0
0103	3	0 00 : 00	0 00 : 00	0 00 : 00	0
0103	7	0 00 : 00	0 00 : 00	0 00 : 00	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: Temporary Exemptions

Program Number: caap4314s

Description:

The Temporary Exemptions report is generated from the Case Master and PCN tables and summarizes by county ID the number of temporary fingerprint exemptions for each program type (GR/GA, CalWORKs, FS, GR/CalWORKs, GR/FS, CalWORKs/FS, and CalWORKs/FS/GR).

REPORT: CS4314S
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
TEMPORARY EXEMPTIONS REPORT
MONTHLY - CDSS

PROCESS DATE: 03/31/2000
PAGE: 1

FINGERPRINT	GR/GA	CalWORKs	FS	GR/CalWORKs	GR/FS	CalWORKs/FS	CalWORKs/FS/GR
TR	0	0	1	0	0	0	0
TL	0	0	1	0	0	0	0
TR/TL	0	0	0	0	0	0	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: Open Search Transaction

Program Number: caap4320

Description:

The Open Search Transaction report summarizes Open Search transactions during the month. It identifies the number of records with fingerprints added during the month either through SFIS or AFIRM Conversion, and also indicates the number of clients removed via the Remove Images process.

REPORT: CS4320M

STATEWIDE FINGERPRINT IMAGING SYSTEM
OPEN SEARCH TRANSACTION REPORT
MONTHLY

PROCESS DATE: 03/31/2000
PAGE: 1

Total Clients With Fingerprint (start of period)	=	85
Clients Added With Fingerprint (during period)	=	68
Online SPIS (68)		
AFIRM's OPEN SEARCH (0)		
Total Clients With Fingerprint (end of period)	=	258
Removed Client(s)	=	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: AFIRM Images Converted to SFIS

Program Number: caap4321

Description:

The AFIRM Images Converted to SFIS report summarizes the AFIRM images converted to SFIS captured images during the month. It identifies the number of records with fingerprints added through AFIRM Conversion, the number replaced by SFIS images, and the total number of each type of case.

REPORT: CS4321M

STATEWIDE FINGERPRINT IMAGING SYSTEM
AFIRM IMAGES CONVERTED TO SFIS
MONTHLY

PROCESS DATE: 03/31/2000
PAGE: 1

Subtotal AFIRM images		=	0
AFIRM right images	(0)		
AFIRM left images	(0)		
Subtotal SFIS images		=	0
SFIS right images	(0)		
SFIS left images	(0)		
Total AFIRM Images		=	0
AFIRM cases		=	0
SFIS cases		=	0
Total AFIRM Cases		=	0

RFP OSI 2046 CURRENT SYSTEM

Report Name: Fraud Statistics

Program Number: caap4900

Description:

The Fraud Statistics report summarizes statistics related to potential and actual fraudulent cases. It identifies the number of records resolved with three specific resolution codes, the referrals for possible fraud, and the referrals with various disposition codes.

REPORT: CS4900M	STATEWIDE FINGERPRINT IMAGING SYSTEM FRAUD STATISTICS Monthly	PROCESSING DATE: 01/31/2001 PAGE: 1
TOTAL OPEN SEARCH HITS	= 930	
Total Resolved 01	= 45	
Total Resolved 02	= 155	
Total Resolved 03	= 242	
TOTAL RESOLVED	= 442	
Open Search Possible Fraud	= 26	
Closed Search Possible Fraud	= 13	
TOTAL REFERRALS FOR POSSIBLE FRAUD	= 39	
Total No Fraud Found	= 278	
Total Fraud Found Aided	= 4	
Total Fraud Found Not Aided	= 5	
Total Pending Investigation	= 2	
Total Under Prosecution	= 1	
TOTAL FRAUD REFERRALS WITH DISPOSITION	= 290	

**RFP OSI 2046
CURRENT SYSTEM**

Report Name: CS4223

Description: Appointment Notice Listing report.

REPORT: CS4223W
SITE ID: 1901

STATEWIDE FINGERPRINT IMAGING SYSTEM
APPOINTMENT NOTICE LISTING
DISTRICT: L0002

PROCESS DATE: 04/11/2002
PAGE: 1

APPT DATE	APPT TIME	LAST NAME	FIRST NAME	CIN	LIN	2 ND APP T	AUT O RES APP T	NEW APPT DATE	NEW APPT TIME
04/29/2002	07:00A M	BALLENA	GREG	9427774A	1909B0744431 04				
REMARK:									
04/29/2002	07:00A M	TORADO	VIVIANA	92522208A	1169SA6AC11 02				
REMARK:									

RFP OSI 2046 CURRENT SYSTEM

REPORT: CS4515A

STATEWIDE FINGERPRINT IMAGING SYSTEM
LEADER TO SFIS INTERFACE FILE
CINS ADDED THROUGH INTERPACE - DAILY

PROCESS DATE: 06/01/2001
PAGE: 1

CIN	LIN	SYST KEY	FIRST NAME	LAST NAME	DATE OF BIRTH	SEX
-----	-----	-----	-----	-----	-----	---
90567847D	19-09-B02VB02-1-02	1999901159170452	HUGO	MONTENEGRO	11161959	F
92183013D	19-09-B02WC05-1-03	1999901159170457	NELSON	RIDDLE	10081961	M
92120357D	19-09-B02Y513-1-06	1999901159170509	LUSINE	SQUIDWARD	11061982	F

RFP OSI 2046 CURRENT SYSTEM

REPORT: CS4515E

STATEWIDE FINGERPRINT IMAGING SYSTEM
LEADER TO SFIS INTERFACE FILE
REJECTED INTERFACE - DAILY

PROCESS DATE: 06/01/2001
PAGE: 1

CIN	CASE NUMBER	CHK DGT	SEP FAM	PID	FIRST NAME	LAST NAME	ERROR MESSAGE
95666645C	B026B50	4	1	01	PATRICK	KRABBYPATTIES	Participant under 18
95199345C	B016B50	4	1	01	AVRIL	SPEARS	Participant under 18
92433884C	B02F190	3	1	02	ANGELICA	SPONGEBOB	Participant under 18

RFP OSI 2046 CURRENT SYSTEM

REPORT: CS4323M
COUNTY: 98

STATEWIDE FINGERPRINT IMAGING SYSTEM
AGING RESOLUTION REPORT
MONTHLY

PROCESS DATE: 05/05/2003
PAGE: 1

SITE ID	APPLICANT NAME	APPL CIN	SEARCH FILE NAME	FILE CIN	MATCH DATE	DAYS OLD
9802	BLACK, JANE	75454991H	C BLACK, JANE	75454991H	03/04/2000	1157
9802	ANGEL, IRENE	75451502H	C ANGEL, IRENE	75451502H	03/04/2000	1157
9802	ALVAREZ, NICHOLE	75430502H	C ALVAREZ, NICHOLE	75430502H	03/04/2000	1157
9802	WILDER, LOTUS	75397791H	C WILDER, LOTUS	75397791H	03/04/2000	1157
9802	BEY, WELLA	75382502H	C BEY, WELLA	75382502H	03/04/2000	1157
9802	HANOVER, ESPERANZA	75375991H	C HANOVER, ESPERANZA	75375991H	03/04/2000	1157
9802	ROCHA, ISRAEL	75371502H	C ROCHA, ISRAEL	75371502H	03/04/2000	1157
9802	BEY, TEY	75282502H	O BE, HUALA	75281502H	03/04/2000	1157
9802	ANDERSON, ADA	75378851H	C ANDERSON, ADA	75378851H	03/04/2000	1157
9802	AKILO, JAYNE	75259402H	C AKILO, JAYNE	75259402H	03/04/2000	1157
9802	BEY, TEY	75282502H	C BEY, TEY	75282502H	03/04/2000	1157
9802	BE, HUALA	75281502H	C BE, HUALA	75281502H	03/04/2000	1157
9802	BE, HUALA	75281502H	C BE, HUALA	75281502H	03/04/2000	1157
9802	SMITH, GABRIELLE	75268791H	C SMITH, GABRIELLE	75268791H	03/04/2000	1157
9802	AYALA, DINA	75237402H	C AYALA, DINA	75237402H	03/04/2000	1157
9802	BENSON, MARSHANA	75248991H	C BENSON, MARSHANA	75248991H	03/04/2000	1157
9802	BEAR, BRIANNA	75252502H	C BEAR, BRIANNA	75252502H	03/04/2000	1157
9802	APE, JAMES	75541502H	C APE, JAMES	75541502H	03/05/2000	1156
9802	JOHNSON, MICHELLE	75671502H	C JOHNSON, MICHELLE	75671502H	03/05/2000	1156
9802	APPLE, NINA	75651502H	C APPLE, NINA	75651502H	03/05/2000	1156
9802	LEWIS, MARI	75603502H	C LEWIS, MARI	75603502H	03/05/2000	1156
9802	JORDAN, ABRAHAM	76023991H	C JORDAN, ABRAHAM	76023991H	03/05/2000	1156
9802	JONES, MARISA	75529991H	C JONES, MARISA	75529991H	03/05/2000	1156
9802	ARIAS, JOSE	76042502H	C ARIAS, JOSE	76042502H	03/05/2000	1156
9802	BALL, RINA	75488991H	C BALL, RINA	75488991H	03/05/2000	1156
9802	JORDAN, ELISA	75471502H	C JORDAN, ELISA	75471502H	03/05/2000	1156
9802	BOYLE, JEANE	75462502H	C BOYLE, JEANE	75462502H	03/05/2000	1156
9802	PHILLIPS, JOSEPH	76017991H	O BENTON, BENJAMIN	76016991H	03/05/2000	1156
9802	JOHNSON, JACK	75797991H	O GONZALEZ, MARIO	75796391H	03/05/2000	1156
9802	BOLD, ROBERT	75781502H	O MICHAELS, JOHN	75778402H	03/05/2000	1156
9802	PHILLIPS, JOSEPH	76017991H	C PHILLIPS, JOSEPH	76017991H	03/05/2000	1156
9802	BENTON, BENJAMIN	76016991H	C BENTON, BENJAMIN	76016991H	03/05/2000	1156
9802	ABRIL, LEONCIO	75977851H	C ABRIL, LEONCIO	75977851H	03/05/2000	1156
9802	AGUILAR, ARMANDO	75951502H	C AGUILAR, ARMANDO	75951502H	03/05/2000	1156
9802	AGUILAR, JOAQUIN	75929991H	C AGUILAR, JOAQUIN	75929991H	03/05/2000	1156
9802	HOPKINS, ANTHONY	75891502H	C HOPKINS, ANTHONY	75891502H	03/05/2000	1156
9802	HERNANDEZ, PABLO	75879891H	C HERNANDEZ, PABLO	75879891H	03/05/2000	1156
9802	GONZALEZ, MIGUEL	75841502H	C GONZALEZ, MIGUEL	75841502H	03/05/2000	1156
9802	SANDOVAL, MARCOS	75815851H	C SANDOVAL, MARCOS	75815851H	03/05/2000	1156
9802	BROOKINS, TYRONE	75812502H	C BROOKINS, TYRONE	75812502H	03/05/2000	1156
9802	JOHNSON, JACK	75797991H	C JOHNSON, JACK	75797991H	03/05/2000	1156
9802	GONZALEZ, MARIO	75796391H	C GONZALEZ, MARIO	75796391H	03/05/2000	1156
9802	BOLD, ROBERT	75781502H	C BOLD, ROBERT	75781502H	03/05/2000	1156
9802	MICHAELS, JOHN	75778402H	C MICHAELS, JOHN	75778402H	03/05/2000	1156
9802	NELLETT, ERIC	75541402H	C NELLETT, ERIC	75541402H	03/05/2000	1156
9802	HERNANDEZ, JULIET	74371502H	O DOE, JANE	74298402H	03/15/2000	1146
9802	BIRMINGHAM, MORRIS	74350991H	O BYRD, LADY	74295991H	03/15/2000	1146
9802	CONRAD, NEAL	90005214D	O AEBLEX, PAUL	90005171G	03/15/2000	1146
9802	AIREDALE, THOMAS	74337402H	O BEY, NEY	74282502H	03/15/2000	1146
9802	ADAMS, GREGORY	90006785E	O CROSBY, KYLE	90006768E	03/15/2000	1146

Appendix 7 - 10/05/2001

RFP OSI 2046
CURRENT SYSTEM

Operator Audit Reports

The existing system stores all relevant operator information, such as operator ID, time, date, data input, date revised, and transaction information, for all add, update, and delete transactions in the Informix database, as currently required. This data is utilized to create various ad hoc State-defined audit reports.

**RFP OSI 2046
CURRENT SYSTEM**

M. PERSONNEL

STATE APPROVAL OF STAFF

Contractor Personnel

The current Contractor is required to maintain the skill and experience levels of personnel throughout the contract. In the event that Contractor personnel vacancies occur, the Contractor must provide replacement personnel with skills and experience equivalent to those specified in the initial Bidder's proposal, and subject to State approval. The Contractor agrees to notify the State of personnel vacancies and provide resumes of replacement staff. Such notification and proposed replacement must be furnished to the State within seven (7) calendar days prior to the replacement personnel beginning work on the project.

AVAILABILITY OF STAFF

The current Contractor must dedicate the people and resources required to ensure successful operation of the project. The on-site staff and resources are fully dedicated to the SFIS project and are not shared with other projects. Contractor personnel assigned to SFIS must be located within the State of California. The current Contractor's subcontractor that provides replacement and repair services at those SFIS sites not maintained by the current Contractor personnel ensure adequate personnel and coverage throughout the State.

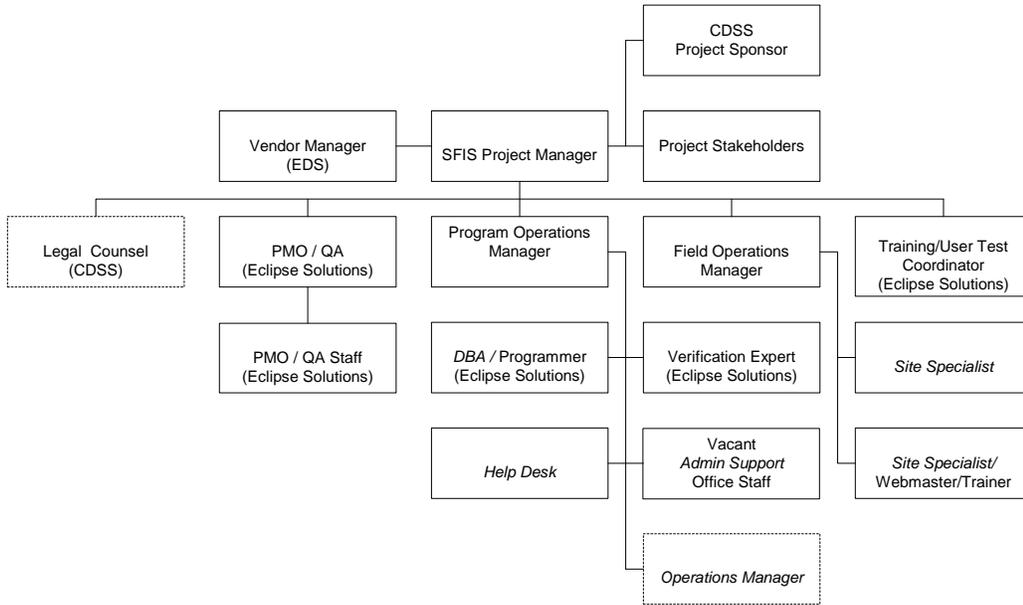
SFIS ORGANIZATION STRUCTURE

The current State SFIS organization is documented in the chart below.

**RFP OSI 2046
CURRENT SYSTEM**

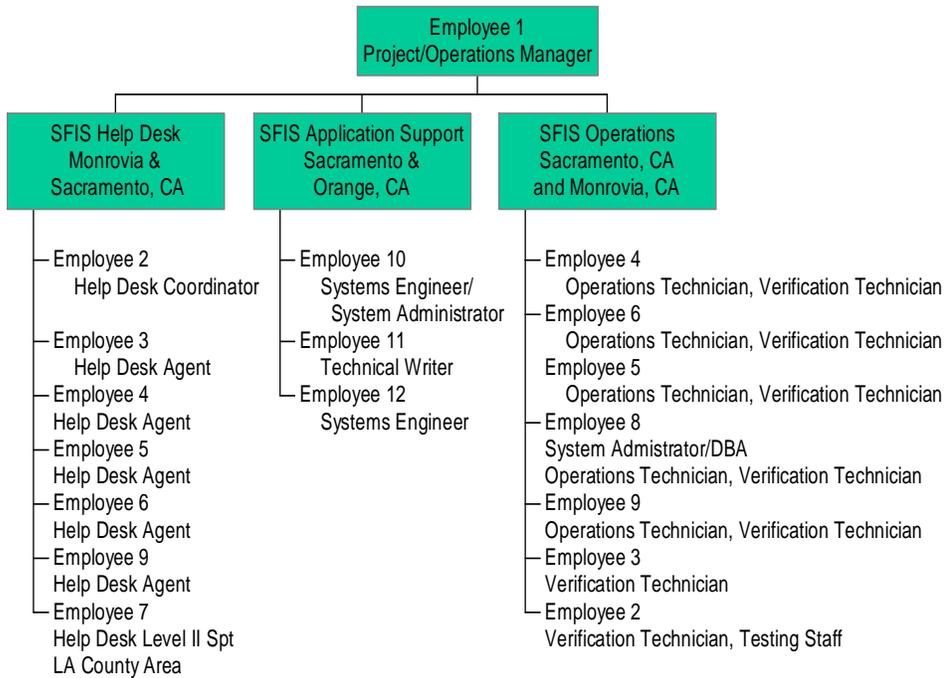
SFIS – CURRENT CONTRACTOR ORGANIZATION

The current Contractor's organization supporting SFIS is documented in the table below.



RFP OSI 2046
CURRENT SYSTEM

The SFIS Account's Organization Chart



RFP OSI 2046 CURRENT SYSTEM

Current Contractor Roles and Responsibilities

As the prime contractor, the current Contractor assumes all responsibility for coordination, control, and performance of subcontractors that make up their team. Furthermore, the current Contractor is the single point of contact with respect to subcontractor questions or problem resolution.

The current Contractor coordinates tasks with all subcontractor managers. In addition to overall coordination and integration of subcontractors, the current Contractor performs the following high-level tasks:

- Provide overall project management services and coordinate closely with the State in operating SFIS.
- Provide and/or coordinate maintenance for all procured and installed hardware.
- Integrate components provided by subcontractors and vendors into SFIS.
- Maintain SFIS application software.
- Test, under review of the State, of all software, hardware, communications hardware configuration, on-line and batch processing, including Acceptance and Pilot Tests.
- Provide full and complete system documentation.
- Provide a Help Desk to SFIS users.
- Provide ongoing Central Site operations and maintenance of SFIS.

The current contractor staff's responsibilities include:

- Software maintenance by phone and on site.
- Software enhancement.
- Hardware maintenance by phone and on site.
- Maintenance reporting to State staff.
- Preventative maintenance to the imaging equipment.
- Help Desk level I, II, and III support services.
- "Participate in weekly Project Change Control Board meetings."
- Manage subcontractor activities including Motorola/Printrak.

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

For more detail about the current contractor's' roles and responsibilities, see table below.

Name	Help Desk Coordinator	Help Desk Agents	Hardware & Connectivity	Application Support	Break/Fix	Inventory Control	Verification	Operations	Application Development	External Interfaces	System Administration	Database Support	System Documentation	Testing & QA	Management	Administration
Help Desk Coordinator	X						X							X		
Technical Writer													X	X		X
Operator1		X					X	X								
System Engineer1									X							
Monrovia Staff					X											
Help Desk Agent1		X					X	X								
Help Desk Agent2		X					X	X								
Project Manager															X	X
Operator2		X					X	X								
Help Desk Agent3		X					X	X								
System Engineer2				X					X						X	
System Administrator/ Database Administrator			X			X	X			X	X	X				

**RFP OSI 2046
CURRENT SYSTEM**

Motorola/Printrak Roles and Responsibilities

Deleted: Printrak

Motorola/Printrak is a subcontractor to EDS that provides the SFIS AFIS. Motorola/Printrak high-level roles and responsibilities are as follows:

Deleted: Printrak

Deleted: Printrak

- Provide program management services in support of the overall Contractor and SFIS effort.
- Assist in the integration of Motorola/Printrak fingerprint processing and one to one (1:1) matching software in the SFIS workstations.
- Provide Central Site fingerprint matching and storage equipment and software that meet SFIS requirements.
- Assist in the integration of Central Site fingerprint matching and storage equipment and software with other Central Site equipment and software.
- Provide fingerprint subsystem training to Contractor personnel.
- Provide Verification Technicians as required.
- Provide engineering and maintenance assistance as required.

Deleted: Printrak

Other Subcontractor Roles and Responsibilities

Other subcontractor high-level roles and responsibilities are as follows:

- Repair hardware returned to the maintenance location from the remote offices.
- Warehouse replacement equipment for maintenance dispatches.

Personnel Requirements

Contractor Project Manager

The Contractor currently provides a Project/Operations Manager whose project management responsibilities include:

- Planning and monitoring project activities.
- Working with the State Project Manager to resolve actual and/or potential problems.
- Reporting on project status.

RFP OSI 2046
CURRENT SYSTEM

- Providing analytical and technical expertise as required by the project.
- Obtaining and scheduling the use of required Contractor resources.

Verification Technicians

CERTIFIED FINGERPRINT EXAMINER

The State currently supplies a Certified Fingerprint Examiner for the verification process. When called upon, the Examiner is available to appear in court and is qualified to testify on fingerprint-related matters.

VERIFICATION TECHNICIANS

The current Contractor provides trained personnel for the verification process. The Contractor certifies that each individual is proficient in the knowledge and skills necessary to their functions. The Contractor's obligation is not satisfied without written certification.

QUALITY CONTROL OF VERIFICATION STAFF

The current State Certified Fingerprint Examiner monitors and reviews all Verification Technician staff members. The Certified Fingerprint Examiner reviews all procedural logs and checklists to ensure that documented procedures are executed and quality control procedures are followed. A process of randomly choosing transactions performed by the Verification Technicians has been implemented to provide quality control to the verification process. The Certified Fingerprint Examiner also verifies that the implemented procedures result in an efficient and effective SFIS.

Help Desk Personnel

HELP DESK PERSONNEL

The current Contractor provides personnel trained on all Help Desk functions. The SFIS Training Coordinator provides written certification that each individual trained is proficient in the knowledge and skills necessary to use SFIS.

RFP OSI 2046
CURRENT SYSTEM

QUALITY CONTROL OF HELP DESK PERSONNEL

The current Contractor's Project/Operations Manager reviews the implemented Help Desk function to verify structural and procedural completeness. Periodic quality reviews are performed to maintain the highest level of service delivered by the Help Desk staff. The Project/Operations Manager also monitors the work of all Maintenance Representatives dispatched to the remote locations to perform remedial maintenance. The Project/Operations Manager is responsible for ensuring that all quality control procedures are followed and produce effective results.

Central Site System Operators

CENTRAL SITE SYSTEM OPERATORS

The current Contractor provides trained personnel for computer operation functions at the Central Site. The Contractor certifies that each individual is proficient in the knowledge and skills necessary to perform their functions. The Contractor's obligation is not satisfied without written certification. These System Operators handle daily procedures to include monitoring of the system console including matching, diagnostic testing, and backup. Supervising the staff, the Contractor Project/Operations Manager also monitors system operation and performance, and monitors compliance with the SFIS contract and State objectives.

QUALITY CONTROL OF CENTRAL SITE OPERATORS

The Contractor monitors Contractor's staff trained in the operation of the system and is responsible for the quality control of the Contractor's operators. Periodic quality reviews are performed to maintain the highest level of service delivered by the system operators. The Project Manager reviews all turn-over logs and problems to ensure that all quality control procedures are followed and produce effective results.

Security Clearance

The current Contractor is responsible for obtaining security clearances for all employees, subcontractors, or materialmen requiring access to restricted areas at the Central Site or in the counties for work on SFIS.

**RFP OSI 2046
CURRENT SYSTEM**

Background Checks

The current Contractor has granted the right to the State to conduct background checks of all employees, subcontractors, and materialmen entering designated restricted areas. The background checks are conducted prior to any employee, subcontractor, or materialmen entering in a restricted area and are based upon information provided to the State including, but not limited to, name and date of birth. The information is provided only to the State's representative at least twenty-four (24) hours in advance of the need for access. The State of California may in its sole discretion refuse to allow an employee, subcontractor, or materialmen access to a restricted area for any of the following reasons:

- Conviction of a felony.
- Conviction of a misdemeanor (not including traffic or parking violation and petty offenses).
- A person under current criminal investigation or pending trial.
- Any outstanding warrants (including traffic and parking violations).
- A person currently on parole or probation.

Contractor Staff's Qualifications

Project/Operations Manager

The Contractor provides Project/Operations Manager(s), with the following qualifications:

- Either a Bachelor's degree plus three (3) years managing a variety of IT projects or five (5) years managing a variety of IT projects.
- Two (2) years managing the delivery of application maintenance or development services to a large scale automated system similar in size and complexity to SFIS as described in Section III, Current System.
- System Development Life Cycle (SDLC) knowledge and experience in implementation and use of SDLC standards.
- Managing a large-scale system maintenance or development staff.

RFP OSI 2046
CURRENT SYSTEM

- The following skills and knowledge are desirable:
 - Welfare system experience with automated Eligibility Determination/ Benefits Calculation (ED/BC).
 - Welfare Program Knowledge.
 - Managing a project with industry certification or assisting a project in achieving certification (e.g. ISO, CMM).
 - Must have a minimum of twelve (12) years experience in operations and operational support.
 - Experiences should include WAN support, customer service, Help Desk management, and systems maintenance.
 - Should have held support positions such as Customer Service Representative, Operations Technician/Scheduler, and Computer Operations Supervisor.

Help Desk Coordinator

The contractor provides Central Help Desk Coordinator(s) with the following qualifications:

- Five (5) years experience as a Manager with experience, including, but not limited to:
 - Minimum of two (2) years managing a Help Desk.
 - Supervision/management of staff.
 - Development of administrative processes to ensure customer service objectives are met.
 - Process and workflow analysis and improvement.
 - Development and Maintenance of databases from tracking and reporting.
- Knowledge of:
 - Techniques to improve customer relations.
 - System Development Lifecycle processes.
 - Change control principles and procedures and the ability to apply them when appropriate to minimize the impact of system and application modifications on customer service.
 - Welfare Program knowledge (desirable).
 - Familiarity with diagnostic tools (desirable).

Help Desk Agents

The contractor provides Help Desk Agents with the following qualifications:

RFP OSI 2046
CURRENT SYSTEM

- A minimum of one (1) year help desk experience and passed SFIS examination.
- Six (6) months of experience with Help Desk ticket system is desirable.

Help Desk Level II Support

The contractor provides Level II Help Desk Agent(s) with the following qualifications:

- A minimum of two (2) years experience on a project similar to SFIS, familiar with software that allows the control of a workstation remotely and six (6) months experience with a Help Desk ticket system.
- Experience providing support on a large object oriented application (statewide).
- Experience providing support for Windows NT.

Systems Engineer

The contractor provides two (2) Level II Systems Engineer(s) with the following qualifications:

- Each engineer has over nine (9) years of data processing experience.
- Expertise includes systems analysis, monitoring and maintenance support.
- Proficient in C and PowerBuilder programming languages.
- An expert in system testing, enhancements, and implementation of batch program modifications using C and PowerBuilder programming languages.
- A solid background in testing, implementation, programming and user training in the state and local government environment.
- A Bachelor of Science degree in Information Systems Management or Computer Information Systems or equivalent experience.
- Programming experience in PowerBuilder.
- Programming experience in C.

**RFP OSI 2046
CURRENT SYSTEM**

- Experience in shell scripting.

System Administrator

The contractor provides System Administrator(s) with the following qualifications:

- Experience in Windows NT administration.
- Experience in UNIX administration.

Operations Technician

The contractor provides Operations Technician(s) with the following qualifications:

- A background in operations, hardware maintenance, and batch cycle processing and monitoring.
- Knowledge in computer networking, PC hardware components and software installation are also needed.
- One (1) year experience operating UNIX, Windows NT, and utility software such as HP OpenView.

Verification Technician

The contractor provides Verification Technician(s) with the following qualification:

- One (1) year experience in working as a Verification Technician on a project similar to SFIS.

Database Administrator

The contractor provides Database Administrator(s) with the following qualifications:

- Minimum of two (2) years experience as an Informix Database Administrator, including, but not limited to:
 - Experience in the administration of the HP UX open TCP/IP and FTP telecommunications environments.
 - Experience configuring, generating and implementing HP UX and Informix software upgrades and patches.
 - Experience as an Informix Database Administrator managing the multiple database environments.

RFP OSI 2046
CURRENT SYSTEM

- Experience in the administration of the HP UX automated system operations environment that manages and controls an HP9000 system with minimal operator interaction.
- Experience in managing relational administration.
- Experience designing and establishing standards for complex database environments, physical structure and specialized database applications.
- Experience in determining and designing data security strategy and processes at the application interface level.
- Experience in assisting application developers in determining complex database environments requirements.
- Experience includes experiences in fingerprint match verification, spreadsheet and statistical software, and database updates.
- Bachelor of Science degree in Information Systems Management, Computer Information Systems or equivalent work experience.
- Knowledge of and experience with SQL.

Technical Writer

The contractor provides Technical Writer(s) with the following qualifications:

- At least four (4) years of experience in writing technical documents.
- Experience authoring documents using Microsoft software.
- ROBO Help experience is desirable.

Testing Staff

The contractor provides Testing Staff with the following qualifications:

- Two (2) years testing an automated system similar in size and complexity to SFIS as described in Section III, Current System, including but not limited to:
 - Development of test plans.
 - Knowledge and experience with function testing.
 - Knowledge and experience with system testing.
 - Knowledge and experience with regression testing.
- Technical writing skills.

**RFP OSI 2046
CURRENT SYSTEM**

- SDLC knowledge and experience in implementation and use of SDLC standards.

A summary of the current staff positions and the percent of time that they devote to SFIS in order to fully support SFIS is provided in the following table. The table identifies the number of positions that are filled by the Prime Vendor personnel and as well as subcontracted personnel.

Position	% of time devoted to SFIS
Contract Project/Operations Manager	100%
Systems Engineer (EDS and NextLevel)	100%
Database Administrator (DBA)	100%
Systems Administrator	100%
Help Desk Coordinator	One hundred percent (100%)
Help Desk Agent (Level 1)	One hundred percent (100%)
Help Desk Agent (Level 2)	One hundred percent (100%)
Technical Writer	Fifty percent (50%)
Operations Technician	One hundred percent (100%)
Verification Technician	One hundred percent (100%)
Testing Staff	One hundred percent (100%)
Motorola/Printrak Management and Staff	Up to one hundred percent (100%) as needed (Ongoing)

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

N. HELP DESK

HELP DESK SUPPORT DESCRIPTION SUMMARY

A permanent user Help Desk function exists for SFIS. Help Desk support is available to county users during the time periods that SFIS is online, normally 7 a.m. to 7 p.m. Monday through Friday, except for State holidays.

The Help Desk is housed at the SFIS Central Site and consists of first level Help Desk Agents; second-level Agents, and a Contractor Help Desk Coordinator. All Help Desk Agents receive initial system training and ongoing training on any SFIS enhancements or changes. All Help Desk Agents and Coordinators have other responsibilities such as integration testing or verification in addition to Help Desk duties, and are therefore not dedicated to the Help Desk on a full time basis.

The Help Desk Agents provide assistance and additional training to SFIS end-users, answer questions on SFIS use and operational procedures, determine the communication status of devices in the network, centrally test on-site equipment, and restore service to malfunctioning hardware.

Help Desk Level of Effort

The current Help Desk provides a sufficient level of Help Desk equipment and personnel so that, when a State and/or county user places a call to the SFIS Help Desk, the user waits no longer than an average of two (2) minutes (computed weekly) before the user is put in direct contact with the Help Desk Agent and the Help Desk procedures are begun without further interruption. The Help Desk system records the following data: time that the call entered Help Desk queue; total time that the call has been in queue waiting for direct contact with the Help Desk Agent; average queue time for all callers; and the number of callers who abandon the queue while waiting for a response from the Help Desk. All Help Desk data listed above is reported on a monthly basis.

SFIS Help Desk Structure

The SFIS Help Desk is the single point of contact with the current Contractor for all SFIS users. The maximum number of users operating workstations at any one (1) time is approximately three hundred and seventy-five (375).

The following paragraphs describe the organization of the SFIS Help Desk. This section is presented to describe the environment in which the SFIS Help Desk operates and the personnel available for escalation paths.

**RFP OSI 2046
CURRENT SYSTEM**

SFIS Help Desk Support Team

The SFIS Help Desk Support Team is made up of personnel found throughout the SFIS project organization chart, as well as vendors that support SFIS hardware and software. The table in the Exhibit below summarizes the SFIS Help Desk Support Team levels.

Level 1	Level 2	Level 3
Help Desk Agents	Advanced Help Desk Agents	Miscellaneous Support Personnel (HP, <u>Motorola/Printrak</u> , State, etc.)
	Fujitsu Maintenance Technicians	

Deleted: Printrak

Exhibit: SFIS Help Desk Support Team Levels

The first level of the SFIS Help Desk Support Team consists of the Help Desk Agents, who are employed and managed by the current Contractor Project Manager. The second level includes Advanced Help Desk Agents, also employed and managed by the current Contractor, and Fujitsu Maintenance Technicians. Finally, the third level consists of other support personnel, such as HP Maintenance Representatives, Motorola/Printrak Support Personnel, Informix Support Personnel, State Personnel, and other personnel, as needed.

Deleted: Printrak

The following paragraphs describe the various areas and roles that make up the SFIS Help Desk Support Team:

Help Desk

- Help Desk Agents.
- Advanced Help Desk Agents.
- Current Contractor Project Manager.
- Current Contractor Help Desk Coordinator.

Network/Hardware Support

- System Administrator.
- Operations Technicians.
- Database Administrator.

**RFP OSI 2046
CURRENT SYSTEM**

Application Hardware Support

- Systems Engineers.

Fujitsu Maintenance Technicians

- Repair/replace defective hardware at remote sites.

HP Maintenance Representatives

- Repair/replace defective HP hardware at Central Site.
- Support for hardware/operating system at Central Site staff via telephone.

Motorola/Printrak Support Personnel

- Resolve Motorola/Printrak related software issues.
- Maintain Motorola/Printrak hardware at Central Site.
- Provide support for finger image related topics including expert fingerprint testimony.

Deleted: Printrak

Deleted: Printrak

Deleted: Printrak

State Staff

- Manage and resolve State Telecommunications issues.
- Manage training requests from SFIS users.
- Perform Move/Add/Changes (MACs).
- Provide in person oversight at the Central Site of new release deployment and major operational changes.
- Investigate network issues.
- Handle State System Administrator responsibilities, such as:
 - Image removal requests.
 - Addition of E level IDs.
 - Clarification of county and *State procedural issues*.

**RFP OSI 2046
CURRENT SYSTEM**

SFIS Help Desk Approach

The current Contractor uses a two-tiered approach for the SFIS Help Desk. Help Desk Agents interact with callers during overlapping shifts to provide complete coverage from 7 a.m. to 7 p.m., Monday through Friday (except State holidays). Help Desk Agents also work with other contractors and/or vendor staff at higher levels as required when handling SFIS Help Desk calls. The levels of interaction function as follows:

SFIS Help Desk Agents

Help Desk Agents receive SFIS Help Desk calls, determine whether the problem relates to policy and procedure, or the SFIS system itself, and gather information pertaining to the issue. In the case of an SFIS system call, the Help Desk Agent will attempt to resolve the issue. If the Help Desk Agent cannot resolve the issue, they will escalate the call to Network/Hardware Support, Application Support, or a member of the State staff.

Network/Hardware Support

Network/Hardware Support (including Advanced Help Desk Agents and Fujitsu Maintenance Technicians) resolve system related calls that cannot be resolved by the Help Desk Agents. The Fujitsu Maintenance Technicians may also be dispatched to sites for hardware related problems.

Application Support

Application Support personnel are experts who deal with problems beyond the knowledge of Network/Hardware Support team members. They include the Database Administrator, Systems Engineers, State personnel, and other vendor hardware/software support maintenance (including HP Maintenance Representatives and Motorola/Printrak Support Personnel).

Deleted: Printrak

SFIS HELP DESK IMPLEMENTATION

The major components of the SFIS Help Desk include facilities, a toll-free telephone number, automated tools, reports, and training.

SFIS Help Desk Location

The SFIS Help Desk is located in Sacramento, California and is structured as described in Section III of this document. Help Desk Agents are available to

RFP OSI 2046 CURRENT SYSTEM

answer calls and provide service from 7 a.m. to 7 p.m., Monday through Friday (except State holidays).

Toll-Free Telephone Number

The toll-free telephone number has a roll over capacity to allow the phone line dialed to roll to the next available phone if the initial line is busy. This process helps to ensure the phone lines are available and accessible during operational hours. Callers are also given the option to leave a voice mail message. The Automatic Call Distribution (ACD) Coral CallMaster (CCM) system records the following data:

- Number of calls received.
- Number of calls answered.
- Number of calls not answered (abandoned).
- Average ACD ring time.
- Average talk time.
- Average wait time on queue.
- Maximum wait time on queue.
- Abandoned calls log.

Additionally, in the event of a large-scale event, such as the Central Site server is down, an automated message, known as a “front end prompt” can be provided, indicating an estimated time to attempt to log on to the system or call back. This message can be updated as necessary and is removed once the system returns to normal operation.

Automated Tools

The paragraphs below describe the following automated tools used by the SFIS Help Desk Support Team:

- Peregrine Systems ServiceCenter (formerly Renaissance Enterprise Management (REM)/Vantive).
- Global Request Management (GRM) Knowledgebase.
- CA-Unicenter The Next Generation (TNG) WorldView.
- ControllT.
- Automatic Call Distribution (ACD) ACD.

**RFP OSI 2046
CURRENT SYSTEM**

SERVICECENTER

The ServiceCenter Help Desk module is used by the Help Desk Agents to manage data, solve end user problems, and track solutions. Tracking resolution of end user problems is the core activity performed with ServiceCenter. Typically, an agent receives a call and begins to verify caller information. After a caller is established as a valid SFIS user, the request for service is reviewed and recorded in the system as a ServiceCenter case. Every action for a ServiceCenter case is recorded as an event. Recording events makes it possible to track cases and their solutions.

After opening a ServiceCenter case, the SFIS Help Desk will prioritize the call using the table shown in the Exhibit below as a guideline.

Priority	Severity	Response Time	Impact
1	1	Notify Network/Hardware/Application Support within ten (10) minutes. Network/Hardware Support to provide a status report to the user(s) within one (1) hour.	Severe problem resulting in complete work stoppage for all or a large number of users. An example is a Central Site system crash. Any user impacted with a client waiting. Any hardware failure at a site with only one (1) workstation.
1	2	Notify Network/Hardware/Application Support within one (1) hour. Status reports to user(s) within two (2) hours.	Four (4) or more users impacted without a client waiting. An example is one (1) or more workstations are malfunctioning or losing access to critical applications and there is no alternative work around.
2	2	Notify Network/Hardware/Application Support within four (4) hours. Status reports to user(s) within twenty-four (24) hours.	One (1) or more users are impacted, a work around exists and users are able to function. Examples are routine application setup, installation, or enhancement request. Requests to State Administrator regarding CIN removal.

**RFP OSI 2046
CURRENT SYSTEM**

Priority	Severity	Response Time	Impact
3	3	Notify Network/Hardware/Application Support within eight (8) hours. Status reports to user(s) as scheduled.	Non-urgent/non-critical and can be scheduled; delaying resolution for an agreed upon time will not adversely affect users. An example is installation of a new version of software. Requests for consumables, brochures, manuals, etc. Requests for training, reports, or system changes.
3	4	State to update ServiceCenter case by 9 a.m. each business day.	Network failure affecting one (1) or more county where sites can still process clients using stored transactions. This case will be originated by the SFIS Help Desk as a Priority 1 Severity 1; Current Contractor Network/Hardware Support will contact the appropriate SFIS State contact person to make them aware of the case; State Telecom will change the Priority/Severity after initial evaluation. The resolution may take longer than twenty-four 24 hours.

Exhibit: Call Prioritization Guidelines

Priority/Severity Handling Process

Priority/Severity of 1,1

A case issued to Network/Hardware Support and a phone call is made to Network/Hardware Support.

- If ten minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made.
- If ten more minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support and call is made to the current Contractor Project

RFP OSI 2046
CURRENT SYSTEM

Manager. The current Contractor Project Manager will notify the State contact.

- If twenty (20) more minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support and call is escalated to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.

Priority/Severity of 1,2

A case issued to Network/Hardware Support and a phone call is made to Network/Hardware Support.

- If ten minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support.
- If thirty (30) more minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support and call is made to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.
- If thirty (30) more minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to SFIS Help Desk; follow up call made to Network/Hardware Support and call is escalated to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.

Priority/Severity of 2,2

A case issued to Network/Hardware Support.

- If four (4) hours elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support.
- If thirty (30) more minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support and a call is made to the current

RFP OSI 2046
CURRENT SYSTEM

Contractor Project Manager. The current Contractor Project Manager will notify the State contact.

- If thirty (30) more minutes elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support and call is escalated to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.

Priority/Severity of 3,3

A case issued to Network/Hardware Support.

- If eight (8) hours elapse and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support.
- If one (1) more hour elapses and Network/Hardware Support has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; a follow up call made to Network/Hardware Support and a call is made to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.
- If one (1) more hour elapses and Network/Hardware Support has not acknowledged the case a trigger message is sent to the SFIS Help Desk; follow up call is made and call is escalated to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.

Priority/Severity of 3,4

A case assigned to State as a result of a phone called received from the State Telecom Team. Note: This type of case is originated by the Help Desk as a Priority 1, Severity 1; current Contractor Network/Hardware Support will contact the appropriate SFIS State contact person to make them aware of the case and the State Telecom team will change the Priority/Severity after initial evaluation.

- If ten minutes elapse and State has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support. Network/Hardware Support will follow up with the State team.

RFP OSI 2046 CURRENT SYSTEM

- If ten more minutes elapse and State has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support and call is made to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.
- If twenty (20) more minutes elapse and State has not acknowledged the case, a trigger message is sent to the SFIS Help Desk; follow up call made to Network/Hardware Support and call is escalated to the current Contractor Project Manager. The current Contractor Project Manager will notify the State contact.

Tracking trouble tickets and cases (ticket that contains multiple tickets/calls) is a function of ServiceCenter. Through the use of the Action History and Events pages, reports, cases, trouble tickets, and their solutions may be tracked. Examples include who created the case, who resolved the case, what had to occur in order to resolve the case, when the case was resolved, how the case was resolved, and case resolution time. Managing information, resolving end-user problems, and tracking resolutions are some of the functions of ServiceCenter that enable the Help Desk Agents to provide service to the SFIS and its end users.

Knowledgebase

The Global Request Management (GRM) Knowledgebase is a database used by the Help Desk Agents to quickly access SFIS policies and procedures to assist users when they call the SFIS Help Desk. The Knowledgebase is updated with new or updated policies, procedures, and general SFIS information as it is developed or obtained. The current Contractor Help Desk Coordinator maintains the Knowledgebase using MS Front Page. A copy of all data found in the SFIS Knowledgebase is maintained by the State. The current Contractor Help Desk Coordinator forwards any Knowledgebase additions or updates to the State as they occur.

WorldView

WorldView is a component of the CA-Unicenter The Next Generation (TNG) used to monitor the SFIS network. It provides a top-down view of mission-critical hardware and software. It can also be used to view specific details pertaining to a single resource.

RFP OSI 2046 CURRENT SYSTEM

WorldView provides a graphical visualization of the SFIS domain network. WorldView can be used to:

- Discover all the devices in the SFIS network using the Discovery process.
- See the entire SFIS network graphically represented on 2-D and 3-D maps, grouped into networks, sub-networks, and segments based on their logical relationships.
- Trace all events reported by network devices, isolate faults, and display them within the WorldView interface.

In order to monitor devices managed by CA Unicenter, the devices need to be “discovered” on the network. The Discovery process automatically detects or “discovers” devices on the SFIS network and populates the Unicenter TNG Common Object Repository with objects that represent the SFIS network devices and their relationships. Once created, these objects can be displayed by the WorldView graphical user interface in a 2-D map and monitored on the console. As the 2-D map is launched, the objects display automatically in folders and are arranged according to the SFIS network topology.

The severity status of any object experiencing difficulty is updated in real-time. Status is converted into severity by an alarm set, which is a table that maps the many possible status values into the few severity values. SFIS severity values will be set to responding or not responding initially with refinement made during ongoing operations as necessary.

The severity of objects propagates up to their parent in the display, allowing the current Contractor System Administrator and/or Network/Hardware Support to track down a problem by tracking the red icons (in 2-D). Currently, WorldView is running on a workstation known by the name Jade, located at the Central Site, and monitored by the current Contractor System Administrator and Network/Hardware Support. The current Contractor is expected to produce one (1) TNG severity report, per day, for the State. If necessary, action will be taken by the user to correct any problems upon discovery.

RFP OSI 2046 CURRENT SYSTEM

WorldView is used to monitor devices that are IP driven. These devices include database servers, workstations, and network printers. The devices will be grouped together by site. Peripherals that are not IP driven such as the fingerprint scanner, digital camera, slave printers, etc. will not be seen by WorldView but will be placed on CA Advanced Help Desk (AHD) for inventory tracking. The discovered objects, or any SFIS device previously discovered by CA Discovery, will be located on the ServiceCenter database for inventory tracking, as well. These objects, upon discovery, will be labeled using the assigned host name. For SFIS workstations, the hostname will be the SFIS workstation name.

WorldView monitors and displays the status of the Central Site database server, coordinators, and the Matching subsystem. Should the SFIS Help Desk be the first party to receive indication that a Central Site server is not responding, the SFIS Help Desk will notify the Central Site personnel of the need to correct the problem. Correction of the problem is not an SFIS Help Desk staff activity.

Control/IT

Control/IT allows Help Desk Agents to view and take control of the caller's workstation screen (assuming that network connectivity exists).

Once the Help Desk Agent initiates Control/IT, whatever is on the target workstation's screen is also viewable to the Help Desk Agent. This function allows the agent to see the actual error message, or steps that caused an error message, from the Central Site. Additionally, the agent may manipulate the screen remotely, progressing through the SFIS application or the login process. This allows the agent to obtain information or effect any needed change on the workstation that might resolve the problem. During the time when the agent is "in control" of the workstation, the SFIS user may watch on the workstation monitor. This function enables the Help Desk Agent to demonstrate system functionality.

Automatic Call Distribution (ACD)

The SFIS Help Desk uses the ACD system Coral CallMaster (CCM) to manage incoming SFIS Help Desk calls. CCM includes open, industry-standard software that performs call processing of both inbound and outbound calls, and has the capacity to process up to one hundred thousand (100K) calls per hour. It also generates reports

RFP OSI 2046 CURRENT SYSTEM

showing statistical information on SFIS Help Desk Calls. The reports that are generated by CCM are:

- Group Performance Report by Interval.
- Group ACD Calls Distribution Report by Interval.
- Group Abandoned Calls Analysis/Report by Interval.
- Abandoned Calls Log.

Reporting

To accomplish tracking of SFIS Help Desk problem/resolution events, the ServiceCenter Reporting function is used to generate information for the following reports:

- SFIS Weekly Maintenance Report.
- Closed Cases by Product (by Site).
- Summary of Calls.
- Monthly Closed Activity Report.
- Profile Change Report.
- Configuration Problem Report.
- "Z Other" Product Report.
- Performance Metrics Report.
- The current Contractor Help Desk Coordinator uses the reports to review SFIS Help Desk performance and to identify recurring problems and refer them to the appropriate staff. The reports serve as management tools to track the responsiveness of the Fujitsu Maintenance Technicians and the SFIS Help Desk call/answer response time.

Training

In addition to learning about the SFIS hardware, software, and network during orientation, the SFIS Help Desk Support Team also receives formal training on the SFIS application and SFIS Help Desk procedures.

New Help Desk Agents will be trained by the current Contractor Help Desk Coordinator and current Help Desk Agents. The current Help Desk Agents are considered SFIS Subject Matter Experts (SMEs) and are utilized for training depending on their knowledge level, experience, and expertise. Help

**RFP OSI 2046
CURRENT SYSTEM**

Desk Agents are provided training on the SFIS application and the various processes involved in the Help Desk function including escalation procedures. After completion of training, Help Desk Agents are issued a G-level ID and allowed to answer SFIS Help Desk calls independently, upon approval by the State.

Network/Hardware Support and Application Support personnel are all chosen for acquired skills in their areas of expertise with additional training in their subject area as required.

The Exhibit below lists the training provided by the Contractor to the SFIS Help Desk Support Team.

Subject	Informal training	Formal training	Self-Paced Studies
Crystal Reports	Required: <ul style="list-style-type: none"> • Network/Hardware Support • Application Support Suggested: <ul style="list-style-type: none"> • Help Desk 	Required: <ul style="list-style-type: none"> • Network/Hardware Support Suggested: <ul style="list-style-type: none"> • Application Support 	Required: <ul style="list-style-type: none"> • Network/Hardware Support Suggested: <ul style="list-style-type: none"> • Help Desk
SFIS Application	Required: <ul style="list-style-type: none"> • Help Desk Suggested: <ul style="list-style-type: none"> • Network/Hardware Support 	Required: <ul style="list-style-type: none"> • Help Desk • Network/Hardware Support • Application Support 	
ServiceCenter	Required: <ul style="list-style-type: none"> • Help Desk • Network/Hardware Support 	Required: <ul style="list-style-type: none"> • Help Desk • Network/Hardware Support 	
KnowledgeBase	Suggested: <ul style="list-style-type: none"> • Application Support 	Required: <ul style="list-style-type: none"> • Help Desk • Network/Hardware Support 	
ACD	Required: <ul style="list-style-type: none"> • Help Desk • Network/Hardware Support Suggested: <ul style="list-style-type: none"> • Application Support 		
Hardware – Printer	Required: <ul style="list-style-type: none"> • Help Desk 	Required: <ul style="list-style-type: none"> • Network/Hardware Support 	Required: <ul style="list-style-type: none"> • Help Desk

**RFP OSI 2046
CURRENT SYSTEM**

Subject	Informal training	Formal training	Self-Paced Studies
Hardware – Scanner	Required: • Help Desk	Required: • Network/Hardware Support	
Hardware – Camera	Required: • Help Desk	Required: • Network/Hardware Support	
Hardware – Workstation	Required: • Help Desk	Required: • Network/Hardware Support	
Telecommunications	Required: • Network/Hardware Support Suggested: • Application Support		
Networking	Required: • Network/Hardware Support	Required: • Application Support Suggested: • Network/Hardware Support	Suggested: • Network/Hardware Support • Application Support
Client/Server systems	Required: • Application Support	Required: • Application Support	Suggested: • Application Support
Customer Service	Required: • Help Desk • Network/Hardware Support	Required: • Help Desk • Network/Hardware Support Suggested: • Application Support	

Exhibit: SFIS Help Desk Support Team Training

**RFP OSI 2046
CURRENT SYSTEM**

SFIS Help Desk Process

This section describes the incoming call handling process.

Overview

Calls received into the SFIS Help Desk call queue are answered on average within two (2) minutes of entry into the queue. The Help Desk Agent receiving the call immediately begins entering pertinent data into the automated SFIS Help Desk tool, ServiceCenter. This action triggers the ServiceCenter system to generate a case and assign a case number to be used in tracking the call through resolution. The Exhibit below illustrates the process flow for SFIS Help Desk call management.

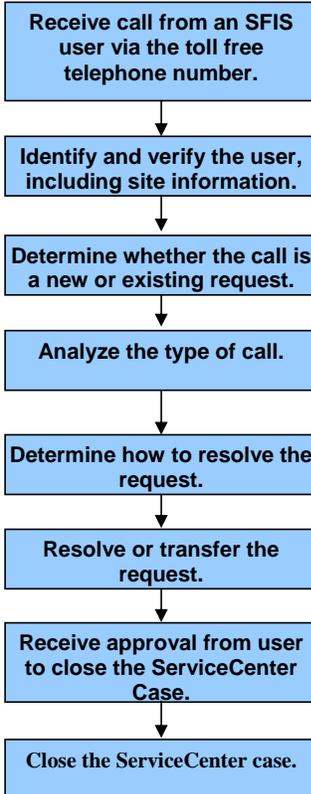


Exhibit: Process Flow of Help Desk Management

**RFP OSI 2046
CURRENT SYSTEM**

Once the caller's issue is resolved, the caller is notified and, if the caller agrees that the issue has been resolved, the case is closed and logged in the system. Routine calls generally result in the problem or question being resolved over the telephone during the initial call. In the event a problem is not resolved over the phone, the ServiceCenter case number will be given to the caller for reference and the caller will be advised of the required steps that will be taken to resolve the problem. The ServiceCenter case will be updated with the steps taken to resolve the problem and the case will be closed.

The Exhibit below describes the call flow for the SFIS Help Desk.

Help Desk (Routine Calls) 1 st Point of Contact	Network/Hardware Support (Non-Routine Calls)	Dispatch Network/Hardware Support (As Required)	Application Support (DBA, SE, Motorola/Printrak, Hewlett Packard)
<p>Track and Prioritize:</p> <ul style="list-style-type: none"> • Entry into ServiceCenter • Determine Type of Problem • Similar Problem • Resolve problem OR • Search KnowledgeBase for additional information <ul style="list-style-type: none"> • Resolve problem • Complete ServiceCenter case • Information not available <ul style="list-style-type: none"> • Obtain assistance from Network/Hardware Support 	<p>Calls:</p> <ul style="list-style-type: none"> • Gather additional information • Conduct research • Implement action in conjunction with user • Complete ServiceCenter case <p>Hardware:</p> <ul style="list-style-type: none"> • Test • Repair • Exchange • Inventory 	<p>Hardware (Remote Sites):</p> <ul style="list-style-type: none"> • Repair • Exchange • Inventory • Software Upgrades • Preventive Maintenance (PM) 	<p>Calls:</p> <ul style="list-style-type: none"> • Gather additional information • Conduct research • Implement fix or required user action • Report to Network/Hardware Support for ServiceCenter case closure <p>Hardware (Central Site):</p> <ul style="list-style-type: none"> • Implementation Control • Coordinate Upgrades • Coordinate Central Site PM

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

Help Desk (Routine Calls) 1 st Point of Contact	Network/Hardware Support (Non-Routine Calls)	Dispatch Network/Hardware Support (As Required)	Application Support (DBA, SE, Motorola/Printrak , Hewlett Packard)
Application: <ul style="list-style-type: none"> Use application knowledge AND Refer to User Guide OR State System Administrator 	Application: <ul style="list-style-type: none"> Use application knowledge AND Refer to User Guide 	Software: <ul style="list-style-type: none"> Verify current software release is loaded on PC 	Application: <ul style="list-style-type: none"> Research issue to identify potential programming fixes OR For fingerprint expertise contact Motorola/Printrak Software: <ul style="list-style-type: none"> Coordinate Upgrade (PC and Servers)
Procedures (Refer To): <ul style="list-style-type: none"> County Coordinator OR CDSS Fraud Bureau AND State Procedures Manual 	Network: <ul style="list-style-type: none"> No data circuit communications Test data circuit Open State request Resolve 	Network (Remote Site): <ul style="list-style-type: none"> Check connections Test with Central Site Network/Hardware Support or Application Support and State 	Network: <ul style="list-style-type: none"> Testing by System Administrator Testing by current Contractor Network Group Coordinate with State Resolve
User Error: <ul style="list-style-type: none"> Correct AND/OR Training issue – Refer to Training Specialist 	Setup Dispatches: <ul style="list-style-type: none"> Open request (SMA/HMR) Dispatch Network/Hardware Support OR Dispatch Vendor Maintenance Technician 		
Resolve Issue or Escalate: Close ServiceCenter case OR Determine Escalation: <ul style="list-style-type: none"> Central Network/Hardware Support Dispatch Network/Hardware Support 	Resolve Issue or Escalate: Close ServiceCenter case, Notify Caller as Appropriate OR Escalate to Application Support	Resolve Issue: Close ServiceCenter case with Network/Hardware Support	Resolve Issue: Close ServiceCenter case

Deleted: Printrak

Deleted: Printrak

**RFP OSI 2046
CURRENT SYSTEM**

Help Desk (Routine Calls) 1 st Point of Contact	Network/Hardware Support (Non-Routine Calls)	Dispatch Network/Hardware Support (As Required)	Application Support (DBA, SE, Motorola/Printrak, Hewlett Packard)
Receive Call Back on ServiceCenter Case: <ul style="list-style-type: none"> Connect to Network/Hardware Support or Application Support 			

Deleted: Printrak

Exhibit: SFIS Help Desk Call Flow

The following paragraphs describe the other personnel shown in the Exhibit including the County Coordinator, State System Administrator, and the California Department of Social Services (CDSS) Fraud Bureau.

County Coordinator

The County Coordinator is responsible for security level E functions at the county level, including all level A, B, and C responsibilities, registering new county users, inactivating county user IDs, enabling county password logon, resetting county passwords, viewing county queues and performing inquires, printing county Match Responses and reports, requesting county floater user IDs, customizing security level and county preferences, and updating county Bulletin Board messages.

Any caller request falling into these areas is referred to the County Coordinator. One (1) example involving the County Coordinator is the process of clearing a password lockout for a security level of D or below. A call to the SFIS Help Desk will result in instructions to contact the County Coordinator. The ServiceCenter case is closed upon referral to the County Coordinator.

State System Administrator

The State System Administrator is responsible for security level G functions at the state level, including all functionality available to level E at the State level, creating Crystal Reports, registering and inactivating users, resetting State passwords, viewing queues and performing SFIS inquiries for the State, printing State Match Responses and reports, receiving floater user IDs from the Help Desk, changing State parameters, removing images, and updating State Bulletin Board messages.

RFP OSI 2046 CURRENT SYSTEM

Any caller request falling into these areas is referred first to the County Coordinator (unless it is a security level E caller), who then contacts the State System Administrator. The security level E caller is referred to the State System Administrator and provided the telephone number, if necessary. The ServiceCenter case is closed upon providing the phone number.

Certain procedural questions are also referred to the State System Administrator. These include county procedures related to the use of the system in the broader welfare environment, such as who to fingerprint, time frames for conversion, and other non-system usage questions.

Any ServiceCenter case falling into the above areas will be assigned to the 12957-State inbox and specifically assigned to the State System Administrator.

Request Workflow

The Exhibit below depicts the workflow of a typical request received at the SFIS Help Desk using ServiceCenter.

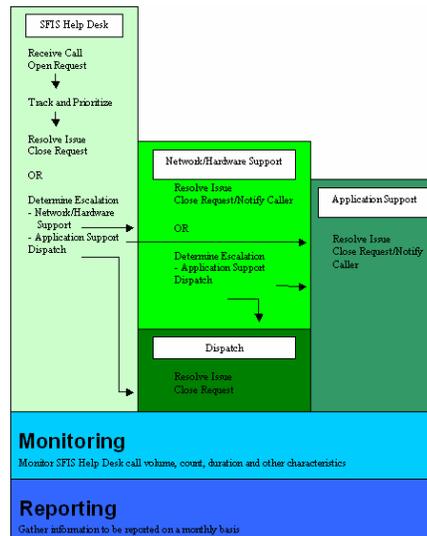


Exhibit: Request Workflow

RFP OSI 2046 CURRENT SYSTEM

Information Sources and Reports

The following paragraphs presents sources of information that may be accessed by the Help Desk Agents to assist in problem resolution, along with the reports that are available to monitor SFIS Help Desk performance.

Information Sources

In addition to KnowledgeBase, a number of manuals, guides, and procedural documentation are available to assist Help Desk Agents respond and resolve SFIS Help Desk calls and issues. Listed below, these reference tools provide information on SFIS hardware, software, and procedures.

- Help Desk Document.
- ServiceCenter User Guide.
- Telecommunication Hardware Manual.
- Printer Hardware Manual.
- Frame Grabber Hardware Manual.
- Fingerprint scanner hardware information.
- Photographic camera information.
- Site installation documentation.
- SFIS User Guides.
- Maintenance Representative Handbook.

Reports

The following reports provide information on the SFIS Help Desk performance.

SFIS SERVICECENTER REPORTS

WEEKLY

- sfis_main_w.xls – Weekly Maintenance Report.

MONTHLY

- 12957_009.xls – Closed Cases by Product (by site).
- 12957_010.xls – Closed Cases by Product (all).

RFP OSI 2046
CURRENT SYSTEM

- 12957_011.xls – Summary of Calls.
- 12957_012.xls – Monthly Closed Activity Report.
- 12957_014.xls – Profile Change Report.
- 12957_016.xls – Configuration Problem Report.
- 12957_017.xls – “Z Other” Product Report.
- 12957_025.xls – Performance Metrics Report.

**RFP OSI 2046
CURRENT SYSTEM**

O. TRAINING AND TESTING

The current Contractor has built and maintains a Statewide Fingerprint Imaging System (SFIS) test and training environment, which the SFIS trainers (County and State) utilize when delivering SFIS training, and the Contractor uses for testing changes. The State is currently responsible for delivering SFIS training at two (2) training facilities, one (1) in Monrovia, on Contractor property, and one (1) in Sacramento, on State property. Currently SFIS has two (2) trainers, one (1) of whom is also designated as the Training Coordinator. Additionally, counties may designate their own county trainers and deliver training from a production workstation in their county using the training database via a method referred to as SFIS Direct Training (DT) (see Training DT Section below).

TRAINING CENTERS

SFIS provides comprehensive classroom training for all of its users: Client Input Operators, Portable Input Operators, Fraud Investigators, System Administrators, Supervisors, County SFIS Trainers, and Coordinators. The courses are conducted in interactive computer-based learning environments, utilizing multi-media presentations and system demonstrations in order to provide users with a comprehensive understanding of the entire SFIS process. The training centers are equipped with Multifunction Workstations, Portable Workstations, a switch box, and a projector used to project the trainer's presentations from a laptop.

By using various learning techniques, such as instructor facilitation, and independent and group activities, SFIS training teaches operators how to use the system tools that are necessary for them to perform their jobs. The following learning objectives, met by all curriculums, ensure that users:

- Understand their role in maintaining internal system security;
- Understand the "big picture" process of the SFIS;
- Understand all of the avenues of help that are provided by and for SFIS;
- Understand how to perform preventative maintenance on selected hardware components; and
- Understand the hardware configuration

**RFP OSI 2046
CURRENT SYSTEM**

CLASS DESCRIPTIONS

Client Input Workstation

Client Input Operators learn that SFIS is user friendly and valuable for reduction of fraud. In an interactive computer-based learning environment and through multi-media presentation and system demonstration, Client Input Operators learn SFIS' background and processes. Through instructor facilitation, independent and group activities, Client Input Operators learn to use the tools necessary for proper SFIS client intake including: File Clearance, Add/Update, File Inquire, and Print Functions. Operators also learn their role of proper photo and fingerprint imaging, learn the avenues of help that are available, understand the configuration of hardware components, and learn how to perform preventative maintenance on selected components. Understanding the importance of their role is also a learning objective of the Client Input Workstation class.

Fraud Investigation Workstation

Fraud Investigators learn that SFIS is user friendly and valuable for the reduction of fraud. In an interactive computer-based learning environment and through multi-media presentation and system demonstrations, Fraud Investigators learn most aspects of SFIS. Investigators learn how SFIS may prompt an investigation, provide tools for the investigation, and record investigative conclusions. Investigators learn that while SFIS is not a replacement for current county investigative practices and procedures, it is a supplemental investigative tool. Investigators learn the avenues of help that are available, understand the hardware components, and learn how to perform limited preventative maintenance on the equipment. Understanding the importance of and what their role is in maintaining internal system security is also a learning objective of the Fraud Investigation Workstation class.

**RFP OSI 2046
CURRENT SYSTEM**

Portable Input Workstation

Portable Input Workstation Operators learn that SFIS is user friendly and valuable for the reduction of fraud. In an interactive computer-based learning environment and through multi-media presentation and system demonstrations, Portable Input Operators learn the background and processes of SFIS. Through instructor facilitation, independent and group activities, Portable Input Operators learn to use the tools that are necessary for proper Portable SFIS client intake including: Add/Update Function and Copy to Zip Disk Function. Operators learn their role of proper photo and fingerprint imaging and learn the avenues of help that are available. Operators also learn the configuration of Portable Input Workstation hardware components and are provided with a hands-on opportunity to set-up and to dismantle the equipment. Understanding the importance of and what their role is in maintaining internal system security is also a learning objective of the Portable Input Workstation class.

System Administration Workstation

System Administrators learn that SFIS is user friendly and valuable for the reduction of fraud. In an interactive computer-based learning environment and through multi-media presentation and system demonstration, System Administrators learn the SFIS from start to finish and are able to utilize the SFIS Administration Tools including: Security Administration Function, Print Function, and Crystal Reporting. System Administrators will also learn about the avenues of help that are available, hardware components, and how to perform preventative maintenance on selected equipment. Understanding the importance of and what their role is in maintaining internal system security is also a learning goal of the System Administration Workstation class.

Special Issues Workshop

The SFIS Special Issues Workshop enables attendees to better understand and perform SFIS functions that are noted by the SFIS Help Desk as re-occurring issues. The workshop consists of facilitated group and independent activities in a computer-based learning environment. SFIS County Coordinators decide who should attend the workshop from their county (The topics covered are generally of interest to a supervisor, coordinator and/or system administrator). As a prerequisite to the workshop, the attendee must be trained on SFIS, and have a basic understanding of the topics to be discussed in order to benefit from a deeper knowledge of the topics covered, which are updated as needed. Special Issues Workshops are organized on an as needed basis.

RFP OSI 2046
CURRENT SYSTEM

Training Database

The State has created and administers an SFIS Microsoft Access training database. The database tracks information such as the class name, date, instructor, attendees, coordinator contact information and class evaluation results. The Training Database Administrator (the PMO) issues class confirmations and is able to generate comprehensive statistical reports used for assessing training needs and trends via the training database.

Enrollment Procedures

Procedures for enrollment in all Classes are as follows:

- SFIS Coordinators call the SFIS Training Scheduler (the PMO) or fill out an online Enrollment Form to enroll in an SFIS class. The following information is provided:
 - Attendee name(s);
 - Attendee contact information;
 - Course desired to attend; and
 - Date desired to attend.
- Training Scheduler places trainee(s) in appropriate Class (or Classes) and confirms enrollment with the County Coordinator via e-mail or phone within a twenty-four (24) hour period.
- Training Scheduler sends a confirmation letter to Coordinator via e-mail or fax approximately two (2) weeks prior to class. Confirmation includes:
 - Class attendee list;
 - Class title;
 - Class date;
 - Class description;
 - Class location;
 - Directions to site; and
 - Time class begins.
- Training Scheduler reviews schedule with Training Coordinator approximately two (2) weeks prior to class in order to determine if cancellation is necessary.
- Classes may be cancelled that have less than fifty percent (50%) enrollment:
 - SFIS Training Scheduler will call SFIS Coordinators to notify of cancellation; and

**RFP OSI 2046
CURRENT SYSTEM**

- Attendees have option to enroll in alternate class date.
- If an attendee needs to cancel - Call or e-mail Training Scheduler.

Training Schedule

The SFIS training schedule is posted on the SFIS website at www.sfis.ca.gov and allows on-line training registration. The schedule below is an example of the Sacramento training schedule in 2004.

Date	Course	Location	Status	Time	Register	Class ID
*	Portable Client Input Workstation	Arranged by Request	*	9AM - 3:30PM	**	*
1/07/04	Fraud Investigation Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	549
1/29/04	Client Input Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	526
1/30/04	System Administration Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	527
2/27/04	Fraud Investigation Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	554
3/10/04	System Administration Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	558
3/24/04	Client Input Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	528
3/25/04	Special Issues Workshop	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	529
4/22/04	System Administration Workstation	Monrovia	Class Completed	9AM - 3:30PM	Register for This Class	559
5/13/04	Fraud Investigation Workstation	Sacramento	Class Cancelled	9AM - 3:30PM	Register for This Class	530
6/24/04	Client Input Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	531
8/26/04	Client Input Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	532
10/20/04	Client Input Workstation	Sacramento	Class Completed	9AM - 3:30PM	Register for This Class	533
11/10/04	System	Sacramento	Space	9AM -	Register for	534

**RFP OSI 2046
CURRENT SYSTEM**

Date	Course	Location	Status	Time	Register	Class ID
	Administration Workstation		Available	3:30PM	This Class	
11/11/04	Special Issues Workshop	Sacramento	Space Available	9AM - 3:30PM	Register for This Class	535
11/12/04	Fraud Investigation Workstation	Sacramento	Space Available	9AM - 3:30PM	Register for This Class	536
11/13/04	System Administration Workstation	Sacramento	Space Available	9AM - 3:30PM	Register for This Class	537

Exhibit: 2004 Training Schedule

SFIS Direct Training (DT)

SFIS Direct Training (SFIS DT) is a training database, accessible by all counties, designed to enhance their on-site training. SFIS DT:

- Allows each county to train operators using the SFIS Project's training database.
- Provides training workbooks (scripted exercises), presentations and instructor notes that are used in the SFIS Training Centers, and that always reflect the current production environment because they are updated every time that changes are made to the system. County Checklists are also posted to the website and may be used as training/instructor "outlines."
- The training database always reflects the production environment because all changes to production are delivered simultaneously to the training database.
- SFIS DT is available during the hours of 7 a.m. to 5 p.m..
- The pre-approved SFIS County Coordinator is the only individual authorized to call the Help Desk and request to use SFIS DT. (The coordinator may approve others to activate SFIS DT by sending an e-mail message to the SFIS State Help Desk Coordinator stating that the listed individuals are approved to activate SFIS DT.)
- SFIS DT will be reset every night. For this reason:
- All photos and fingerprints taken during use of SFIS DT are erased every evening after 5 p.m..

RFP OSI 2046
CURRENT SYSTEM

- Scripted Opened Search demonstrations and exercises only function one (1) time per day per county.
- SFIS DT Open Search Match Responses must be manually printed from the Print Queue; they do not auto-print.
- SFIS DT Stored Transactions functions may not be used because production Stored Transactions may be stored on the workstation's hard drive and would appear while in SFIS DT training mode. If a production Stored Transaction is selected, an error message will appear and the system automatically logs the user off SFIS.

To Initiate Use of SFIS DT, the County Coordinator:

- Confirms who is approved in their county to request the activation of SFIS DT.
- Requests county datasheets from SFIS Training Coordinator or Help Desk.
- Prints training workbooks and instructor notes from the SFIS website.
- Locates host name and IP address on the SFIS monitor sticker.
- Calls the SFIS Help Desk: 1-866-860-7347.
- Requests workstation to be switched to SFIS DT.
- Logs on using county training datasheet Operator ID.
- Performs training.

To End Use of SFIS DT, the County Coordinator:

- Logs out.
- Calls the SFIS Help Desk: 1-866-860-7347.
- Notifies the SFIS Help Desk that training is completed.
- Requests the SFIS Help Desk switch workstation back to production.