MANATEE COUNTY SHERIFF’S OFFICE
RFP-2012-15-002-MCSO AFIS

REQUEST FOR PROPOSALS
FOR IMPLEMENTATION, DELIVERY AND SUPPORT OF AN
AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AFIS)
FOR THE MANATEE COUNTY SHERIFF’S OFFICE

RFP Attachment 1

AFIS Requirements Specification

June 1, 2012
# Table of Contents

1 SYSTEM ARCHITECTURE AND SIZING ................................................................. 1

  1.1 AFIS Technology ...................................................................................... 1
  1.2 System Architecture .................................................................................. 1
    1.2.1 Central AFIS Components .................................................................. 1
    1.2.2 User Workstations, Software and Terminals ........................................ 2
  1.3 Data Storage and Workload Capacities ....................................................... 4
  1.4 System Performance .................................................................................. 5
    1.4.1 Response Time Performance .............................................................. 5
    1.4.2 Tenprint Identification Performance .................................................. 6
    1.4.3 Latent Identification Performance ...................................................... 7
    1.4.4 Interfaces with External Systems ......................................................... 7

2 SYSTEM FUNCTIONALITY .................................................................................. 10

  2.1 Image Acquisition and Processing ............................................................. 10
  2.2 Records Management ................................................................................ 10
  2.3 Tenprint and Palmprint Identification ....................................................... 13
    2.3.1 Tenprint and Palmprint Records ......................................................... 13
    2.3.2 Tenprint and Palmprint Record Origination ........................................ 13
    2.3.3 Tenprint and Palmprint Transaction Processing ................................. 14
    2.3.4 Tenprint Identification .......................................................... .......... 15
    2.3.5 Search of Unsolved Latents (TP:ULF and PP:ULF) ............................. 17
  2.4 Latent Identification ................................................................................ 17
    2.4.1 Latent Records ............................................................................... 17
    2.4.2 User Workstations ........................................................................... 19
    2.4.3 Latent Identification Processing ....................................................... 22
  2.5 Mugshot and SMT Identification ............................................................... 23
    2.5.1 MCSO Mugshot and SMT Records .................................................... 23
    2.5.2 Photo Capture ................................................................................. 24
    2.5.3 Photo Identification ....................................................................... 25
    2.5.4 Photo Investigation Capabilities ...................................................... 26

3 SYSTEM OPERATIONS AND ADMINISTRATION ............................................ 28

  3.1 System Operations .................................................................................. 28
  3.2 Status Monitoring and Diagnostics ........................................................... 28
  3.3 System Configuration Management ......................................................... 30
  3.4 User Administration .............................................................................. 31
  3.5 Management Reporting .......................................................................... 31

4 TECHNICAL REQUIREMENTS .......................................................................... 33

  4.1 Technology Standards Compliance .......................................................... 33
  4.2 National Standards Compliance ............................................................... 35
  4.3 Security .................................................................................................. 35
  4.4 Network Communications ....................................................................... 36
  4.5 Electrical and Environmental Standards ................................................ 37

5 SYSTEM IMPLEMENTATION REQUIREMENTS ............................................ 39

  5.1 Contractor Responsibility .......................................................................... 39
  5.2 Implementation Project Management ....................................................... 39
    5.2.1 Project Plan .................................................................................... 40
    5.2.2 Automated Project Management Tool ........................................... 41
    5.2.3 Project Status and Progress Reporting ............................................ 41
5.3 PROJECT STAFFING ..........................................................................................................................42
  5.3.1 Key Personnel .............................................................................................................................42
  5.3.2 Personnel Assignments and Access .............................................................................................45
5.4 SYSTEM DESIGN ...............................................................................................................................45
5.5 SYSTEM INSTALLATION ....................................................................................................................46
  5.5.1 Installation Planning and Management .........................................................................................46
  5.5.2 Site Surveys .................................................................................................................................47
  5.5.3 System Delivery and Installation .................................................................................................48
5.6 SYSTEM ACCEPTANCE .....................................................................................................................48
  5.6.1 System Acceptance Testing .........................................................................................................48
  5.6.2 Acceptance Testing Plan and Procedures .....................................................................................50
6 CONVERSION AND LOADING OF EXISTING RECORDS ....................................................................51
  6.1 SCOPE ................................................................................................................................................51
  6.2 RECORD CONVERSION PERFORMANCE .......................................................................................52
7 TRAINING ...............................................................................................................................................53
  7.1 SCOPE ................................................................................................................................................53
  7.2 TRAINING PLAN ................................................................................................................................54
  7.3 TRAINING DELIVERY .......................................................................................................................54
    7.3.1 Training Management ..................................................................................................................54
    7.3.2 Training Courseware ...................................................................................................................54
    7.3.3 Scheduling and Conducting Training ........................................................................................55
8 MAINTENANCE AND SUPPORT ...........................................................................................................57
  8.1 SCOPE OF MAINTENANCE AND SUPPORT ....................................................................................57
  8.2 SYSTEM WARRANTY .........................................................................................................................58
  8.3 SYSTEM MAINTENANCE ...................................................................................................................59
    8.3.1 Local Technician ..........................................................................................................................59
    8.3.2 Operations Support .....................................................................................................................59
    8.3.3 System Backups ...........................................................................................................................59
    8.3.4 Preventive Maintenance .............................................................................................................60
    8.3.5 Remedial Maintenance ...............................................................................................................60
    8.3.6 Repair / Replacement of Defective Components .......................................................................61
    8.3.7 Software Maintenance ..............................................................................................................61
    8.3.8 Functionality and Reliability Improvements ..............................................................................62
    8.3.9 Maintenance Scheduling, Problem Tracking and Reporting .....................................................62
    8.3.10 Annual User Group Meeting ..................................................................................................63
  8.4 SYSTEM MAINTENANCE PLAN ..........................................................................................................63
  8.5 TECHNICAL SUPPORT FOR ONGOING OPERATIONS AND SYSTEM EXPANSION ...................64
    8.5.1 Configuration Management ......................................................................................................64
    8.5.2 Test and Training Support .........................................................................................................64
    8.5.3 System Expansion ......................................................................................................................65
APPENDIX 1. GLOSSARY OF TERMS AND ABBREVIATIONS ..................................................................66
APPENDIX 2. NIST TYPE-1 RECORD TRANSACTION TYPES .................................................................72
  2.1 TENPRINT IDENTIFICATION TRANSACTIONS ..............................................................................72
  2.2 LATENT IDENTIFICATION TRANSACTIONS ..................................................................................72
  2.3 REMOTE LATENT SEARCH TRANSACTIONS ...............................................................................73
  2.4 UNSOLVED LATENT MAINTENANCE TRANSACTIONS .................................................................73
  2.5 REMOTE FINGERPRINT IMAGE REQUEST TRANSACTIONS ....................................................73
  2.6 FINGERPRINT IMAGE SUBMISSION TRANSACTIONS ...............................................................74
  2.7 LATENT ADMINISTRATIVE QUERY TRANSACTIONS .................................................................74
1 System Architecture and Sizing

1.1 AFIS Technology

a) The AFIS proposed in response to this solicitation shall utilize proven, current-production AFIS system COTS (Commercial Off-the-Shelf) hardware and software components. Any proposed component or functional capability that is not in current production must be identified as a ‘developmental’ capability, and the plan and timeline for implementation; testing and full availability of any developmental capability proposed for the system must be fully disclosed.

b) The proposed hardware and software configuration shall be updated at no additional cost at the time of system delivery to replace any discontinued or superseded component(s) listed in the proposal with equivalent or better current-production model(s) and Contractor-qualified software.

c) During the life of the system while the system remains under a current maintenance agreement, any system version updates and enhancements developed and offered by the system vendor to agencies in the State of Florida shall be provided and implemented at no additional cost.

1.2 System Architecture

1.2.1 Central AFIS Components

a) The replacement AFIS core system shall be installed at the new Manatee County Public Safety Center and shall consist of the following major components:

1) A vendor-provided central AFIS system providing fingerprint, palmprint and latent identification processing and matching.

2) A vendor-provided EMC Clarion or VNX Storage Area Network (SAN) system providing on-line fingerprint and palm print record storage.

3) A vendor-provided CommVault Simpana 9.0 Enterprise Backup system including a disc-based backup unit, tape backup unit and appropriate enterprise backup/restore software providing on-line fingerprint and palmprint record storage.

4) Vendor-provided communications switches and network appliances necessary to interconnect the central AFIS system components and to connect the central AFIS to the LAN/WAN networks.

b) MCSO will provide the following components as County Furnished Equipment (CFE) and the system implementation shall incorporate and utilize these components in the AFIS architecture:

1) One (1) equipment rack in the Manatee County Public Safety Center. The central AFIS system components must be installed in the provided equipment rack.

2) MS Forefront Enterprise Anti-Virus capabilities managed by Manatee County.
1.2.2 User Workstations, Software and Terminals

a) The selected Contractor shall provide and install AFIS workstations, software and terminals in locations to be designated by MCSO. Tables 1.2-1 provide a summary of the workstation and terminal requirements.

Table 1.2-1 AFIS Workstations, Software and Terminals Summary

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>LiveScan Workstation, cabinet model, with signature pad</td>
<td>§2.3.2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>LiveScan Workstation, portable model with signature pad</td>
<td>§2.3.2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Latent Input/Analysis Workstation</td>
<td>§2.4.2</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Tenprint Input/Analysis Workstation</td>
<td>§2.4.2.1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Enterprise Software License - Multifunction Analysis Workstation Application</td>
<td>§2.4.2.1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>System Operations and Administration Workstation</td>
<td>§3.2.b</td>
</tr>
</tbody>
</table>

b) The selected Contractor shall provide AFIS workstations, software and terminals, as follows:

1) Three (3) FBI-certified, cabinet-model LiveScan workstations. The LiveScan workstations must provide the following capabilities:
   - Capture and digitize standard tenprint fingerprint and palmprint records associated with arrest/booking, ex-felon registration, and MCSO employment applicant background checks.
   - Perform image quality checks to detect poor quality fingerprint and palmprint images and image capture sequence errors and provide immediate feedback to the operator to correct the problem(s).
   - Connect to the MCSO network, transmit NIST-formatted fingerprint and palmprint records to the central AFIS for identification processing, and receive notifications and software/configuration updates from the central AFIS.
   - Interface with the existing MCSO Jail Management System (Intergraph ILEADS RMS/JMS) to import demographic information associated with an arrest booking and pre-populate the associated demographic fields for tenprint and palmprint record capture.
   - Capture and digitize the handwritten signature of each subject using an attached signature pad, provide NIST record formatting, and transmit the signature record to the central AFIS for storage.
   - Print to both vendor provided printers and agency network printers.

2) One (1) FBI-certified, portable LiveScan workstation. The portable LiveScan workstation must provide capabilities for identification record creation, capture,
processing and forwarding that are equivalent to the MCSO stationary cabinet-model LiveScan Workstations and shall include:

- A rugged transportable case to hold all LiveScan components and protect the workstation components from damage during transport.
- A power conditioner to protect the LiveScan equipment from power spikes and surges.
- Communications capabilities to support two modes of network communications:
  1. Direct connection to the MCSO communications network, where available.
  2. Wireless connectivity from a field location using commercial cellular telephone communications to transmit records as email attachments over a secure (e.g. VPN or SSL) internet connection.
- An attached signature pad to capture and digitize the handwritten signature of each subject.
- Print to agency network printers

3) Two (2) Multifunction Analysis Workstations configured for Latent Input and Analysis. These workstations shall each include:

- 24-inch diagonal or larger flat panel display monitors with display resolution capabilities in conformance with the FBI Image Quality Specifications for latent fingerprint image display.
- An FBI-certified desktop scanner capable of scanning hardcopy tenprint and palmprint records, latent lifts and latent photos. The scanner shall be capable of using the full active scan area for latent imaging, with a variable size capture box.
- A boom-mounted camera for direct imaging of latent prints, latent lifts, and photos.
- A variable-intensity, variable position lighting system consisting of at least two flexible light sources, capable of being easily adjusted to optimize the image capture of a latent image.
- Latent capture, processing, AFIS submission, and search results analysis software (Reference Requirements Section 2.4.2).
- Status Monitoring, User Administration and Management Reporting software components (Reference Requirements Section 3.2.b).
- Print to both vendor provided printers and agency network printers.

4) One (1) Multifunction Analysis workstation for tenprint operations. This workstation shall include:

- 24-inch diagonal or larger flat panel display monitor with display resolution capabilities in conformance with the FBI Image Quality Specifications for latent fingerprint image display.
- An FBI-certified desktop scanner capable of scanning hardcopy tenprint and palmprint records.
- Tenprint/palmprint capture, processing, AFIS submission, and search results analysis software (Reference Requirements Section 2.4.2.1).
- Status Monitoring, User Administration and Management Reporting software components (Reference Requirements Section 3.2.b).
- Print to both vendor provided printers and agency network printers.

5) Multifunction Analysis Workstation enterprise software license (Reference Requirements Section 2.4.2.1), including Status Monitoring, User Administration and Management Reporting software components (Reference Requirements Section 3.2.b) for installation on four (4) to six (6) MCSO-furnished desktop workstation PCs. These workstations should also be able to print to the vendor provided printers and agency network printers.

6) One (1) System Operations and Administration workstation. This workstation shall include:
   - 24-inch diagonal or larger flat panel display monitor.
   - AFIS Administrative Applications Software Suite (Reference Requirements Section 3.2.b).
   - Print to both vendor provided printers and agency network printers.

### 1.3 Data Storage and Workload Capacities

a) The AFIS shall include a high-reliability on-line data storage subsystem to store and maintain the system’s tenprint, palmprint and unsolved latent databases in support of automated and interactive identification operations. The on-line storage solution shall support the required long-term storage capacity requirements, and shall be expandable as needed over the life of the system to support the actual growth of the system.

b) The system’s storage capacity must be sized to store the projected number of records that will be accumulated by Year-10 of AFIS operations, as shown in Table 1.3-1. Proposers shall specify the proposed on-line identification database storage sizing in gigabytes and show the average size and number of each type of record used in the capacity computation.

<table>
<thead>
<tr>
<th>Identification Record Projections</th>
<th>2011 Totals</th>
<th>Required (Year-10) AFIS Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Tenprint Records</td>
<td>766,000</td>
<td>1,094,000</td>
</tr>
<tr>
<td>Criminal Palmprint Records</td>
<td>416,000</td>
<td>745,000</td>
</tr>
<tr>
<td>Unsolved Latent Fingerprint Image Records</td>
<td>40,000</td>
<td>150,000</td>
</tr>
<tr>
<td>Unsolved Latent Palmprint Image Records</td>
<td>40,000</td>
<td>150,000</td>
</tr>
</tbody>
</table>
c) The delivered baseline system shall be sized to handle the projected Year-10 Workload Volume of each type of identification transaction as specified in Table 1.3-2, and shall be capable of handling peak workload volumes for up to 4 consecutive hours in any 24-hour period without degradation of performance (‘Peak’ hourly workload is defined as three times the average workload).

Table 1.3-2 System Workload Projections

<table>
<thead>
<tr>
<th>Identification Transaction Rate Projections</th>
<th>Daily Transactions Year-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP:TP &amp; TP:ULF</td>
<td>125</td>
</tr>
<tr>
<td>PP:ULF</td>
<td>125</td>
</tr>
<tr>
<td>Latent Inquiries (L:TP or L:PP + L:ULF)</td>
<td>400</td>
</tr>
</tbody>
</table>

d) The system design shall permit incremental expansions in workload and database capacity through addition of system components without software redesign.

e) The system shall support the connection of additional quantities of standard terminals and workstations to the system and shall provide full operational capabilities and workflow support without requiring software redesign or engineering modifications to the system, and without restriction, as long as the aggregate workload from each type of workstation or terminal does not exceed the associated system workload specifications. Connectivity and support of any of the following types of workstations and terminals at regional Law Enforcement Agencies (LEAs), as authorized by MCSO, shall be supported:

- Permanent LiveScan Workstation installations and temporary Portable LiveScan Workstation installations.
- Universal Latent Workstation (ULW) installations.

1.4 System Performance

1.4.1 Response Time Performance

a) The AFIS shall be designed to provide the following levels of response time performance at the full simultaneous daily average and peak input processing workload for tenprint, palmprint, and latent transaction submissions identified in Table 1.3-2.

Table 1.4-1 AFIS Response Time Performance

<table>
<thead>
<tr>
<th>Search Type</th>
<th>Daily Average Response Time</th>
<th>Maximum for Any Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenprint to Tenprint 1:N open search (TP:TP)</td>
<td>30 seconds</td>
<td>45 seconds</td>
</tr>
<tr>
<td>Tenprint to Tenprint 1:1 Verification (TP:TPV)</td>
<td>10 seconds</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Tenprint to Unsolved Fingerprint Latent Search (TP:ULF)</td>
<td>30 seconds</td>
<td>60 seconds</td>
</tr>
<tr>
<td>Transaction Type</td>
<td>Guaranteed Performance Levels</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------------------------</td>
<td></td>
</tr>
<tr>
<td>Palmprint to Unsolved Palm Latent Search (PP:ULF)</td>
<td>45 seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>60 seconds</td>
<td></td>
</tr>
<tr>
<td>Finger Latent to Tenprint Records Search (LF:TP)</td>
<td>90 seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>120 seconds</td>
<td></td>
</tr>
<tr>
<td>Finger Latent to Unsolved Latent Search</td>
<td>90 seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>120 seconds</td>
<td></td>
</tr>
<tr>
<td>Palm Latent to Palmprint Records Search (LP:PP)</td>
<td>150 seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>180 seconds</td>
<td></td>
</tr>
<tr>
<td>Palm Latent to Unsolved Latent Search</td>
<td>150 seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>120 seconds</td>
<td></td>
</tr>
</tbody>
</table>

Proposers shall state their guaranteed response time performance levels for each of the transaction types listed in Table 1.4-1.

b) Guaranteed AFIS response time performance at the full simultaneous daily average and peak input processing workload for tenprint, palmprint, latent and transaction submissions must be maintained in any expansion scenario, as described in Section 1.3, identified in Table 1.3-2.

1.4.2 Tenprint Identification Performance

a) The system shall provide a capability to achieve at least a 98% “lights-out” capability in automated processing of tenprint search results, as follows. Proposers shall state their guaranteed performance levels.

1) Automated search results processing shall either eliminate all respondents or identify a single high-confidence match candidate in not less than 98% of all tenprint-to-tenprint 1:N searches, regardless of the quality of search and file records prior to quality control.

2) Fewer than 2% of all tenprint-to-tenprint 1:N searches shall require manual analysis for resolution of multiple possible-match candidates (not counting actual duplicate records that are detected in the database).

b) The system shall achieve the following false negative error rates. A false negative error occurs when a matching record is in the AFIS database but the system’s tenprint search processing fails to return the matching record as one of the search respondents, or when post-processing incorrectly eliminates the matching record from the respondent list. Proposers shall state their guaranteed performance levels.

1) Less than 3.0 % false negative error rate for all tenprint search transactions regardless of the quality of search and file records prior to quality control.

2) Less than 1.0 % false negative error rate for all tenprint search transactions where both the search prints and matching record in the system meet minimum AFIS quality thresholds for lights-out searching.

3) Less than 0.5 % false negative error if a matching record is correctly returned as a tenprint search respondent.

c) The system’s automated processing of tenprint search results shall achieve a false positive error rate of less than 0.1 % of all tenprint search transactions that return a single match candidate “hit.” A false positive error occurs when a non-matching record is identified as a high-confidence “hit.” Proposers shall state their guaranteed performance levels.
d) In greater than 99.5% of all tenprint closed search identification transactions for which the search fingerprint record and designated file fingerprint record represent the same individual, the system shall correctly identify the records as a match. *Proposers shall state their guaranteed performance levels.*

e) In greater than 99.5% of all tenprint closed search identification transactions for which the search fingerprint record and designated file fingerprint record do not represent the same individual, the system shall correctly identify the records as not being a match. *Proposers shall state their guaranteed performance levels.*

### 1.4.3 Latent Identification Performance

a) In not less than 95% of all latent-to-tenprint and latent-to-palmprint searches, if a matching tenprint or palmprint record is in the database, and if the latent has at least 10 identifiable minutia points, the matching tenprint or palmprint record shall be among the top 5 candidates based on match score. *Proposers shall state their guaranteed performance levels.*

b) In not less than 95% of all latent-to-tenprint and latent-to-palmprint searches, if the unknown latent and the matching tenprint or palmprint record have at least 20 minutia points in common, the matching record shall be identified in the first position of the candidate list based on match score. *Proposers shall state their guaranteed performance levels.*

c) The system shall provide high accuracy in identifying unsolved latents through reverse searches of incoming tenprint and palmprint records against the Unsolved Latent File (ULF) and high reliability in discriminating actual matches from non-matching respondents in the candidate list.

1) If an incoming fingerprint record is a true match to an existing Unsolved Latent print, the system must provide high accuracy in detecting the match and identifying the unsolved latent to an analyst for confirmation. *Proposers shall state their guaranteed performance levels.*

2) If an incoming palmprint record is a true match to an existing Unsolved Latent print, the system must provide high accuracy in detecting the match and identifying the unsolved latent to an analyst for confirmation. *Proposers shall state their guaranteed performance levels.*

3) If an incoming fingerprint record or palmprint record does not match any of the latents in the Unsolved Latent File (ULF), the system shall provide high-reliability in discriminating the search respondents to reduce manual review workload to the maximum extent possible. *Proposers shall state their guaranteed performance levels.*

### 1.4.4 Interfaces with External Systems

a) The system shall provide flexible and configurable capabilities to interface with external State and national AFIS and with County and municipal AFIS systems in the State of Florida.
1) **FDLE BIS Search and Registration**: Transmission of NIST-formatted identification search requests to FDLE BIS for tenprint, palmprint and latent identification search and registration transactions and receipt and processing of search results responses.

2) **FBI IAFIS Search and Registration**: Transmission of NIST-formatted tenprint, palmprint and latent identification search and registration requests to the FBI IAFIS in accordance with State and FBI procedures, and handling of IAFIS search results responses.

3) **Searches of External Municipal and County AFIS**: Transmission of NIST-formatted tenprint, palmprint and latent identification search requests to County and municipal law enforcement AFIS systems in accordance with established cooperative services agreements, and receipt and handling of search results messages.

4) **Search Requests from Municipal and County AFIS Systems**: Receipt of NIST-formatted tenprint and palmprint identification search requests and ULW latent search requests from an external County or municipal law enforcement AFIS system, in accordance with a cooperative services agreement, and automated lights-out processing and return of search results messages to the requester.

b) The proposed AFIS shall provide capabilities to interface and interoperate with the existing MCSO jail management system. The jail management system interface shall support:

1) Interaction with the JMS at booking to import booking information from the JMS into a LiveScan workstation in preparation for a fingerprint and palmprint capture and Pass-1/Pass-2 submissions to FDLE in accordance with FDLE identification protocols:
   - Pre-populate Type-2 demographic record data in the LiveScan (Pass-1).
   - Update Type-2 booking data, e.g. charges in the LiveScan workstation (Pass-2)

2) Transmission of record update information to the JMS including, as applicable, the OBTS number, Booking number, State ID number and FBI number.

3) Email message communications between the local AFIS and a designated jail management system terminal or workstation to provide timely feedback to the JMS regarding record capture error conditions and identification search results.

c) During the design and implementation phase of the project, the selected Contractor shall work pro-actively and cooperatively with MCSO technical staff and with the JMS vendors to develop interface specifications and to implement and test interfaces with FDLE and the MCSO jail management system. The AFIS must support import of photo records and NIST files that are sent by JMS as FTP transfers.

d) The AFIS system implementation shall provide the capability to import and export identification record information (NIST Type 2 data) in accordance with the XML version of the ANSI/NIST standard (ANSI/NIST-ITL 2-2008) and the National
Information Interchange Model (NIEM 2.1) standard to interchange information with MCSO jail management and criminal records system.
2 System Functionality

2.1 Image Acquisition and Processing

a) All new fingerprint imaging components provided with the AFIS, including LiveScan workstations and desktop scanners and latent camera capture stations shall capture and digitize distortion-free fingerprint, palmprint and latent images at a spatial resolution of 1,000 pixels per inch (ppi) in both the horizontal and vertical dimensions, and with a minimum of 8-bits per pixel gray-scale quantization.

b) Image quality produced by the imaging components shall be consistent with the FBI Image Quality Specifications (IQS) established in most recent version of the FBI Electronic Biometric Transmission Specification (EBTS) Appendix F.

1) The image acquisition devices provided with the system, including live-scan scanners and flatbed scanners, shall be capable of maintaining image quality performance throughout the life of the component.

2) A capability is required that enables a qualified technician to periodically conduct, log and report on-site tests of installed flatbed scanners and LiveScan scanners and demonstrate IQS compliance of each component with IQS ¶2.1 Geometric Image Accuracy and IQS ¶2.4 Gray Scale Range of Data (dynamic range).

c) All new latent fingerprint imaging components including cameras, scanners and associated workstations and AFIS applications provided with the AFIS shall be capable of capturing and digitizing distortion-free latent images in color and gray-scale at a spatial resolution of 1,000 dpi in both the horizontal and vertical dimensions, and with at least 8-bit gray-scale / 24-bit color depth. A 3-channel color imaging capability with 16-bits per channel color depth is preferred.

d) The AFIS system shall be able to handle both 500 ppi and 1,000 ppi NIST-formatted tenprint fingerprint image records and palmprint image records and to use all image records in automated and interactive identification operations without limitation.

e) The AFIS system shall provide for efficient transcoding from 1,000 ppi images to 500 ppi images as necessary to support interaction with external devices and systems that are not capable of handling 1,000 ppi images.

2.2 Records Management

a) The AFIS databases shall provide direct user access to the fingerprint records, palmprint records, and latent records maintained by the system, and shall support automated fingerprint, palmprint and latent identification processing.

- The system shall enable an authorized administrator to query and analyze any system database and to develop reports and statistical analyses of database contents.
- The system shall provide operating system utilities for individual record and batch file manipulation, including copy, delete, dumping and merging.
- The on-line data storage subsystem shall provide capabilities for bulk data loading and extraction of identification records via direct SQL access to the database.

b) The design of the database management system shall ensure that database transaction data is secured such that a temporary loss of communications or processing capability will not result in the loss of any data.

c) The system shall be designed as a “multi-incident” system in which every record from all booking, registration and applicant background check transactions shall be registered in the system and used in AFIS identification processing, including:
   - 500 ppi WSQ-compressed Tenprint and Palmprint Records (legacy records converted from the previous AFIS)
   - 1,000 ppi JPEG-2000 compressed Tenprint and Palmprint Records
   - 1,000 ppi uncompressed Latent Fingerprint Image Records and associated Latent Minutia Record.

d) All records maintained in the system, including tenprint, palmprint, unsolved latent, and signature records must include all demographic and descriptor data contained in the original records, including agency-assigned tracking numbers and other record information, whether or not the information is of use in the AFIS identification process.
   - The demographic and descriptor information must be stored in individual data fields. A card image may be retained in the system, but primary storage of the record demographic information in the form of card images is not acceptable.
   - NIST formatting is preferred for internal storage and management of identification records in the system. If an alternative format is proposed for internal storage and records management, the format must be fully described.
   - A data dictionary must be provided as user-accessible on-line documentation that defines the format and content of each data field in each type of identification record stored in the system.

e) All image records, including tenprint, palmprint, latent images which are maintained in the system shall be original compressed or uncompressed images, as applicable, and shall not be cropped or otherwise reduced such that a complete exact copy of the original record could not be generated from the images and information stored in the system database.

f) The AFIS shall use two primary index numbers for managing tenprint and palmprint identification records in the AFIS:
   - The AFIS ID # (aka ‘PIN’ or ‘Personal ID Number’) will be assigned and used internally by AFIS to provide a unique reference to all of the records in the database for a given individual.
   - The Transaction Control Number (“TCN”) will be assigned and used by AFIS to provide a reference to each specific record capture transaction (adult or juvenile arrest, criminal registration, and employee enrollment/update).
g) The AFIS shall maintain a master cross-reference table that provides the associations of the AFIS primary index numbers with each of the agency-specific index numbers (e.g., booking #) used in MCSO operations.

h) A NIST export capability shall be provided that enables an authorized user to selectively export any record, specified group of records, or the entire database as complete NIST records conforming to the formatting standards established in the most recent version of the *American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information – Part 1.*

- This requirement shall apply equally to tenprint, palmprint, unsolved latent, and signature records.
- The system must enable an authorized user to select one or more records, up to and including the entire on-line identification records database for export. Any limitation of this capability or dependence on the vendor to extract and export NIST records from the AFIS is unacceptable.
- The system shall provide automated NIST formatting and export of user-selected records to a portable media device (e.g., USB drive).
- The system shall enable the user to include record documentation in the export data set that provides a complete field-level definition for each field in each type of exported record.

i) The system shall enable an authorized operator to mark a specific record set (fingerprints and palmprints associated with a specific booking transaction) as “sealed” in response to a sealing order received from a court, and the system shall:

- Limit access to sealed records to specifically authorized system administrators.
- Exclude sealed records from general identification searches.
- Enable an authorized system administrator to remove a “sealed” attribute from any record and restore the record to full use in the identification database.
- Enable an authorized system administrator to create hardcopy and/or electronic copies of a record for off-line storage, and delete a record from the system databases in response to an expungement order.
- The system shall maintain a log of all sealing and purging transactions and shall automatically record each transaction, including the date, time, record number and user ID of the administrator that performs or authorizes removal of the record from the system.

j) The vendor provided CommVault Simpana 9.0 enterprise backup capability shall:

- Support full and partial backups of system databases and logs with minimal or no impact to production AFIS operations.
- Provide interactive restoration/recovery capabilities, including the capability to restore individual identification records, a database segment, or a complete on-line AFIS database from system backups.
- Provide for backing up data to both disk and tape.
MCSO intends in the future to move from tape based backups to cloud based backups, the enterprise backup solution shall provide for that feature when MCSO is ready to make that change.

2.3 Tenprint and Palmprint Identification

2.3.1 Tenprint and Palmprint Records

a) Tenprint records maintained by the system shall include 20 fingerprint images and their corresponding minutia sets, including a rolled fingerprint image and minutiae and a flat (plain impression) fingerprint image and minutiae for each of an individual’s ten fingers.

b) Palmprint records maintained by the system shall be complete whole-palm records including images and minutia records of the left hand and right hand finger segments, upper and lower palm segments, and the writers palm segment.

2.3.2 Tenprint and Palmprint Record Origination

a) Stationary (cabinet model) and portable LiveScan workstations shall be configured to create FDLE-standard and FBI-standard criminal and applicant fingerprint cards. The workstations must:
   ▪ Support pre-configuration of individual workstations to create one particular type of record as a default standard;
   ▪ Enable an operator to override the default selection and easily select another type of fingerprint record to be created from a workstation control screen display, as necessary.
   ▪ Display a data entry form on the screen with data entry fields, code tables and field validation appropriate for the type of record to be created.

b) The LiveScan workstations must enable a user to create an identification record and enter and edit tenprint identification text records via form-oriented text data entry.

c) The LiveScan workstations shall support an electronic interface with the MCSO jail management system and shall be able to import booking information from the local jail management system to preload biographic and demographic information in a fingerprint record.

d) For every LiveScan record creation transaction, the LiveScan workstation must automatically assign a Transaction Control Number (TCN). The same TCN shall be used as a positive linkage between the tenprint and palm print records produced for an individual subject.
   ▪ The LiveScan workstations shall automatically generate a standard OBTS number for use as the TCN.

e) Each LiveScan workstation shall capture fingerprint and palmprint images at a spatial resolution of 1,000 pixels per inch (ppi), with 8-bit (256 level) gray scale quantization.

f) Each LiveScan workstation shall be capable of capturing the palm print images as standard palm print segments for each hand:
A full palm image plus a “writer’s palm” image, or
An image of the finger segments, an upper palm image, a lower palm image, and a writer’s palm image.

g) Each LiveScan workstation shall be capable of applying AFIS-compatible quality algorithms to detect poor quality fingerprints and palmprints, with immediate rescan of any substandard images before data is forwarded to AFIS. The effect of the LiveScan quality check process must ensure that LiveScan records meet minimum image quality standards for automatic input processing by AFIS.

h) Each LiveScan workstation shall be capable of accomplishing a fully automatic comparison of each rolled image against the corresponding plain impression image, to detect sequence errors, with feedback controls for recapture of images as required to correct the errors before data is forwarded to AFIS or output to a printed card.

i) Each LiveScan workstation shall be equipped with a signature pad for capture of each subject’s signature for inclusion with the identification record, and must provide NIST record formatting and transmission of the signature record to the central AFIS for storage.

j) It is desirable that the LiveScan workstations have the capability to include codes in the tenprint or palmprint record indicating that an operator override has been used to bypass the suspension of record completion and transmission when either a low quality condition or a sequence error has been detected, and that the AFIS has the capability to log and report incidences of operator overrides.

2.3.3 Tenprint and Palmprint Transaction Processing

a) The AFIS shall be able to automatically input and process tenprint records and palmprint records:
   - Received from the LiveScan network.
   - Received from a multifunction workstation through a card scan transaction.
   - Received from an external agency as a NIST attachment to an email message.

b) The system shall provide automated workflow controls that enable workflows to be configured in accordance with MCSO business rules for conditional handling, routing and processing of individual identification transactions.
   - MCSO will specify preferences for lights-out and manual review, and the selected Contractor work pro-actively and cooperatively with MCSO to implement workflows for tenprint identification processing that reflect these preferences.
   - Finalized system workflows shall be documented in the System Design Specification.

c) The system shall support both “lights-out” unattended tenprint input operations and manual tenprint operations where input Quality Control is performed interactively by an operator.
In lights-out operations, incoming tenprint fingerprint records will be automatically checked to verify that minimum quality standards are met and then forwarded for automated identification searching.

The system shall automatically queue incoming tenprint records for manual QC analysis that do not meet the “lights out” processing standards.

d) Automated input quality checks performed by the AFIS shall automatically check to verify that each tenprint record contains all mandatory data and that fingerprint images are not missing or out of sequence.

The selected Contractor shall work pro-actively and cooperatively with MCSO staff to specify fingerprint identification quality standards and business rules, and shall configure automated workflows for transaction handling for “lights-out” input processing, manual input QC analysis, and conditional rejection of submitted records.

The selected Contractor shall recommend and pre-set the initial image quality thresholds for both LiveScan and AFIS acceptance / rejection of a LiveScan fingerprint image.

If the LiveScan override notation capability described in 2.3.2.i is not implemented, at a minimum, the AFIS shall identify and log records and originator information for incoming tenprint records containing image sequence errors which shall be interpreted as having resulting from an operator override of LiveScan sequence errors.

e) The AFIS shall be able to automatically detect duplicate booking record submissions, when an incoming tenprint record has the same TCN # as a previously submitted record, and shall queue duplicate booking records for manual analysis.

f) The system shall provide interactive capabilities that enable an authorized tenprint fingerprint analyst to select a transaction from a manual input processing queue, review and correct automatically-detected errors, and either submit the transaction for identification processing or reject the transaction and transmit a rejection notification to the originator.

g) The AFIS shall automatically log incoming tenprint transactions at each stage of processing such that transactions can be auto-recovered without loss of any transaction in the event of a system outage or processing disruption.

h) All tenprint and palmprint identification transactions shall be automatically transmitted to FDLE for search and registration in accordance with FDLE workflow specifications and interface standards. Search results returned as a result of FDLE and FBI IAFIS searches shall be recorded in the AFIS database.

2.3.4 Tenprint Identification

a) The AFIS shall automatically perform searching and matching of tenprint records.

The system shall automatically select and utilize at least the four (4) highest quality fingerprints available in the input tenprint record for searching.
The system shall match against all original tenprint records in the database. Use of composite records for tenprint searches is not desired.

The system shall perform full open (un-delimited) tenprint 1:N searches for all automated input searches.

b) The AFIS shall perform automated post-processing of tenprint search results to automatically eliminate all non-matching candidates from a tenprint respondent list. If matching tenprint records exist in the database, the system shall eliminate all other non-matching records in the candidate list and return only the AFIS ID # of the matching record(s) for verification.

c) In the initial configuration, the system shall queue all TP:TP search results for manual analysis by an examiner.

d) As MCSO gains familiarity and confidence with the system, the Contractor shall provide support upon request to establish an automated workflow and configure the AFIS for automated search results analysis and processing. For fully automated search results processing, the AFIS shall be able to be configured to utilize match thresholds and automated multi-incident identification logic to eliminate the need for manual analysis of search results when a high-probability identification determination can be made automatically.

e) For all tenprint identification search transactions that are completed automatically or confirmed by manual analysis, the system shall:

- Automatically assign the identified AFIS ID # to the search record for a positive match result; or
- Automatically generate and assign a new AFIS ID # to the tenprint record if no matching record exists in AFIS; and
- Automatically assign the AFIS ID # to the associated palmprint, signature and digital photo records; and
- Transmit an SRE message to the record originator.

f) The system shall provide the capability to maintain an arrest notification list and to automatically notify a detective or other individual when the listed individual is arrested. The system shall:

- Enable an authorized system user or administrator to establish a notification record in the arrest notification list associated with a specific AFIS ID #, and enter associated requestor information and a validity period or expiration date.
- Automatically query the LDAP directory to retrieve current contact information and transmit an email notification to the listed contact if an individual on the arrest notification list is identified by the AFIS in association with a booking transaction.
- Automatically purge list entries after the entry expiration date or period, and notify the listed contact that the arrest notification list entry has expired and been removed.
g) The AFIS shall log each transaction and shall record information in the log for each transaction, including originator identification, record type information and search results.

h) The AFIS shall provide a capability to perform statistical analyses of the transaction logs and develop reports of AFIS identification submissions, identification processing performance, identification (hit) rates and multi-candidate result rates.

i) A fingerprint examiner shall be provided with the capability to request printing of a hardcopy 3”x5” Booking Index Card for filing and use by the Identification Unit, and the AFIS report generation function shall provide a capability to:

- Extract identification information from the database for a designated individual, including the individual’s Name, Race, Sex, DOB, FDLE#, Booking#, PIN #, and index fingerprint image;
- Format the text information and fingerprint image in a Booking Index Card format, consistent with the card layout used in current operations;
- Transmit a print request to an agency-designated network printer to generate a hardcopy of the Booking Index Card.

2.3.5 Search of Unsolved Latents (TP:ULF and PP:ULF)

a) The AFIS shall automatically perform TP:ULF searching and matching of ALL incoming tenprint records against the latent fingerprints in the Unsolved Latent File (ULF).

b) The AFIS shall automatically perform PP:ULF searching and matching of ALL incoming palmprint records against the latent palmprints in the Unsolved Latent File (ULF).

c) If the TP:ULF or PP:ULF search produces candidates, the system shall queue search results in a pending Latent work queue for analysis by a latent examiner.

d) The AFIS shall provide logging, analysis and reporting for all TP:ULF and PP:ULF transactions that logs the record originator information and search results and provides a capability to perform statistical analyses and develop transaction activity reports.

2.4 Latent Identification

2.4.1 Latent Records

a) The system shall enable authorized users to:

- create and maintain latent fingerprint case records
- input latent fingerprint and palm print images, associate each image with a case record, and process images in preparation for identification searching by the AFIS.
- conduct searches of latent prints against the local AFIS tenprint and palmprint record databases, and against the Unsolved Latent File (ULF), and refer candidate lists for manual analysis
- forward latent prints for identification searching and registration in the Unsolved Latent File (ULF) at FDLE and FBI IAFIS.
b) Latent case records shall support the optional entry and management of case information, for use by agency examiners in accordance with MCSO policies and standard practices. The system shall provide a capability to store and maintain data elements as part of each ULF record, and the selected Contractor shall work cooperatively with MCSO during the system design phase to develop a complete definition of standard latent case record data fields, including:

- Contributor ORI# - agency identifier; nine (9) alpha/numeric characters.
- Class of Crime - FBI uniform offense classification code; four (4) numeric characters.
- Date of Crime – YYYYMMDD; eight (8) numeric characters.
- Latent Image – 1,000 ppi uncompressed digital gray-scale or color image of the latent print with 8-bit gray-scale or 24-bit color depth; color depth capability of 16-bits per channel is preferred.
- MCSO Case Number or Outside Agency number.
- Item # (Lift #) - Five (5) alpha/numeric characters identifying a specific latent image associated with the case.
- Edit # - One numeric digit to identify one of potentially multiple alternate feature sets for the latent image.
- Barcode # - the evidence index number assigned by the originating agency.
- Operator ID# - AFIS operator identification number.
- Latent type (finger or palm latent, if known).
- Finger position or left/right palmprint hand (if known).
- Linkages to other latent images in a multi-finger lift.

c) The Contributor ORI# + Agency Case # + Item # + Edit # shall define a particular latent within the Unsolved Latent File (ULF). These numbers, displayed in the above order, shall be displayed and printed on candidate lists and individual candidate displays.

d) The system shall provide the capability to store and manage image feature sets (minutia sets) for each latent in the ULF database, with the capability to store and manage multiple feature sets (“Edits”) for each latent. The capability shall enable an authorized latent examiner to create and store a feature set, retrieve and edit a stored feature set, and selectively delete or replace an existing feature set or add a new feature set for the latent with a new Edit# prefix.

e) The system shall enable an authorized analyst to establish linkages between Items (Lifts) in a case, for example to identify sequential prints in a multi-print evidence sample, and the system shall use the linkage information in identification matching to highlight individuals appearing in multiple linked searches.

f) The system shall enable an authorized administrator to selectively delete individual ULF records or all ULF records associated with a selected Case. This capability shall be limited to only latent prints for which the administrator’s agency is the contributing ORI of the latent case.

g) The system shall provide a restricted interactive capability to purge latent prints from the database based on Crime Class and Date of Crime.
h) The system shall provide the capability to maintain a change log for the ULF database recording latent record additions, deletions and updates. The change log shall include at least the ULF record identifiers, operator ID, date/time, and type/description of the change.

i) The system shall provide a capability that enables latent examiners to create and maintain discrete datasets of tenprint and palmprint records associated with a specific latent case, e.g. an elimination print dataset.

- The AFIS shall ensure that the Latent Case Datasets are maintained separately from the production fingerprint and palmprint records and that Latent Case Dataset records are not comingled with the production fingerprint and palmprint records.
- Authorized users must be able to interactively select a dataset and search latent prints against the records in the selected dataset.

2.4.2 User Workstations

2.4.2.1 General Multifunction Analysis Workstation Capabilities

a) Each Multifunction Analysis Workstation shall be capable of being configured and used for tenprint/palmprint functions or latent functions or both.

b) The Multifunction Workstations shall enable an operator to import fingerprint, palmprint, and latent images from an external server or storage system, e-mail attachment, an attached imaging device (desktop scanner or digital camera) or a storage device (e.g., CD-ROM or usb drive), in standard formats including standard bitmap (.BMP), TIFF (.TIF), and JPEG (.JPG).

c) Each Multifunction Analysis Workstation shall be equipped with an FBI-certified high-resolution flatbed scanner for scanning and digitization of tenprint cards, palmprint cards, and latent images for importing into the AFIS. Required capabilities of the flatbed scanner are:

- Digitizing tenprint and palmprint records at a spatial resolution of 1,000 pixels per inch, with 8-bit (256 levels) gray-scale quantization.
- Digitizing color latent images at a spatial resolution of 1,000 pixels per inch, with at least 24-bits (8-bits per channel) color depth; capability for 16-bits per channel color depth is preferred.

d) The workstations shall have split screen display capabilities with sufficient resolution and contrast for side-by-side display of two panels of information, including record information, 500ppi and 1000ppi fingerprint images, palmprint images, and latent images.

e) Multifunction Analysis Workstations shall provide automated and interactive capabilities that result in high user efficiency in making comparisons, and confirming and documenting identifications, with capabilities for:

1) Display and editing of fingerprint, and palmprint images and the associated record information.
2) Selective display of any individual scanned or database image from a fingerprint, palmprint or signature record for on-screen side-by-side comparison with any other corresponding image, with the capability to generate a high resolution 1:1 screen print at actual size.

3) Automatically encoding any selected fingerprint or palmprint and enabling a user to edit the automatically encoded minutiae.

4) Preparation and submission of identification transactions, with interactive selection of search control parameters including search filters and search priority.

5) Accessing search results queues for search results analysis and reporting, with the capability for any analyst to selectively display and access only the status and results for their own search transactions, or to access the complete transaction status display or system search results queue.

6) Maintenance of database records, including capabilities for record annotation, consolidation, sealing and purging.

f) Each displayed image, whether displayed alone on the full screen or on a split screen with another image, shall be clearly annotated to indicate the source record number and image designation (e.g., right index).

g) Multifunction Analysis Workstations shall provide basic and advanced image processing and analysis capabilities for processing and analysis of an individual image or corresponding images in a split screen display, including:

1) Coupled and independent image rotation, pan, zoom and area selection.

2) Coupled and independent brightness and contrast adjustments with the ability to adjust the gray-scale dynamic range of any image.

3) Display of extracted features as an image overlay.

4) Positive/negative reversal of displayed images.

5) Separation of overlaid images.

6) User prompt to the user to save image enhancements under the same or a different Edit #.

7) User capability to add additional edits to a saved image or to revert to the original image.

8) The system shall enable an analyst to apply these image analysis tools at any point during the analysis process, before or during feature extraction/editing.

Proposers shall describe the standard and advanced image processing and analysis capabilities provided by their COTS analyst workstation applications software.

h) The Multifunction Analysis Workstations shall be able to selectively route print requests to any appropriate network printer in the local workgroup or to a designated remote printer.

i) Multifunction Analysis Workstations shall provide interactive capabilities that enable any authorized analyst to create and maintain latent case datasets in association with a
specific latent case, with the capability to construct a dataset of tenprint and/or palmprint
records by retrieving records from the AFIS databases, importing records from an
external server or storage system, or scanning and digitizing hardcopy records

j) Each Multifunction Analysis Workstation shall be capable of being configured with an e-
mail capability incorporating MCSO e-mail clients without resulting in conflicts with or
negative impacts to the AFIS applications.

2.4.2.2 Latent Input and Processing Capabilities

a) To support Latent Input, designated Multifunction Analysis Workstations shall be
configured with a high-resolution Latent Input Camera Subsystem to enable the capture
of latent print images directly from evidence samples and from lifts and photographs.
The Latent Input Camera Subsystem shall include a high-resolution video or digital
camera and lens system, and an accessory lighting system. Required characteristics of
the Latent Input Camera Subsystem components are:

- The camera and lens must be capable of digitizing images at a spatial resolution
  of 1000 pixels per inch, with at least 24-bits (8-bits per channel) color depth;
capability for 16-bits per channel color depth is preferred.
- The camera and lens must be demonstrably in conformance with the FBI Image
  Quality Specifications published in Appendix F of the FBI Electronic Biometric
  Transmission Specification (EBTS).
- The camera must be boom-mounted and provide for easy positioning of the
camera and the evidence sample.
- The accessory lighting shall be a variable-intensity, variable position lighting
  system consisting of at least two flexible light sources, capable of being easily
  adjusted to optimize the image capture of a latent print.

b) For advanced Latent Image processing, designated Multifunction Latent Analysis
Workstations shall be configured with the following image processing software packages.
Integration of operation of the Multifunction Latent Analysis Workstation applications
software and these image processing software applications is highly desirable.

- Adobe Photoshop CS5, or latest version.
- Foray Technologies Image Calibration Utility plug-in for Photoshop.
- Foray Technologies Chromatic Fast Fourier Transform (FFT) filter plug-in for
  Photoshop.
- Foray Technologies Gray-scale Pattern Removal Filter plug-in for Photoshop.

c) Each Multifunction Analysis Workstation designated for latent processing shall be
configured with an integrated Universal Latent Workstation (ULW) capability or
equivalent to support the submission of latent search requests to an external AFIS system
(e.g., FBI IAFIS). The integrated ULW or equivalent capability shall support an easy-to-
use interface to select a target AFIS for transmission of the search request, and shall
automatically perform any reformatting of the image or re-coding of the features as might
be required to submit and perform the external AFIS search.
d) The Latent Interoperability Transmission Specification and the Extended Feature Sets shall be supported by this system at install or as a no-cost upgrade once those specifications are adopted by the FBI.

2.4.3 Latent Identification Processing

a) The AFIS shall process and search latent fingerprints that are:
   - Input and submitted from AFIS latent workstations.
   - Input and submitted via network interconnection from other AFIS latent workstations installed at authorized agencies.
   - Submitted as an LFFS or LFIS transaction by an authorized external agency using ULW software.

b) The system shall provide configurable user preference settings at each workstation that automatically extract features for display/editing or that enable the examiner to interactively mark features prior to searching. The system shall automatically assign an Edit# and save the associated feature set when the examiner initiates a search transaction.

c) The system shall enable an authorized user to automatically perform searching of tenprint fingerprint records or palmprint records in the on-line Fingerprint and Palmprint Record Database.
   1) The finger latent search process shall enable a user to designate ('lasso') an area of the latent image for searching, perform a manual edit of latent features in the designated area of the latent, and automatically match the encoded features of the finger latent against each rolled fingerprint image and plain impression fingerprint image in every fingerprint record in the on-line fingerprint record database.
   2) The palm latent search process shall be to perform an auto-extraction of latent features from a designated ('lassoed') area of the palm latent, enable optional interactive editing of displayed features, and automatically match the encoded palm latent features against the left and right hand palm segment images in every palmprint record in the on-line palmprint record database.
   3) Under control of an authorized examiner, the system shall enable the examiner to perform directed searches, including:
      - Limiting a latent search by finger position or palm segment.
      - Interactively editing, adding and deleting automatically extracted features in the latent image.
      - Specifying either a full 360 degree rotation or standard rotation of the latent image for the search.

d) An automated capability to extract, characterize and match third-level detail features in a latent print as part of the matching process is desirable.

e) The system shall provide a seamless capability to submit latent searches to the local AFIS and FDLE and receive and distribute latent search results.
f) The system shall return match results in a candidate list, with candidates ordered from highest to lowest match score.

g) Each analyst shall be able to specify the candidate list length for any particular search transaction (e.g., top 50 candidates).

h) Authorized users shall have the interactive capability to select a particular search transaction from a work queue and view the search results.
   - For general users, the system shall display only the contents of work queues for the transactions originated by the logged-in workstation user.
   - An authorized system administrator shall be capable of viewing all transactions in any work queue for any user:

2.5 Mugshot and SMT Identification

An integrated capability shall be provided with the system to: (a) provide for the capture and storage of digital images of facial photographs (mugshots) and scars, marks and tattoos (SMT); (b) provide automated and interactive capabilities including parametric searching of the digital image databases; (c) provide investigative capabilities including preparation of line-ups, mugshots and image-based reports (e.g. wanted posters); and (d) provide interfaces to enable automated importing booking information from the MCSO jail management systems and accessing/automated importing digital images by the MCSO jail management system. The following paragraphs provide requirements for these capabilities.

2.5.1 MCSO Mugshot and SMT Records

a) The AFIS shall provide the capability to store and manage digital photo image records including facial photos (mugshots) and photo images of scars, marks and tattoos (SMT). The photo storage and management capability shall be configured to optimize the performance of photo identification processes including parametric searching of the mugshot and SMT records, and candidate data set compilation and display.
   - The system shall be capable of maintaining the original compressed digital photo images in the database for use in automated identification and search processes and in interactive presentation for comparisons.
   - Each record in the digital photo image database shall contain a set of record indices and descriptor information to support record access, retrieval and automated identification functions. Master record indices for each record shall include at least Last Name, First Name, Gender, DOB, AFIS ID #, TCN#, agency record indices, and other appropriate indices determined during the system design discussions.

b) Each facial and SMT record maintained by the system shall include descriptor information to enable parametric searching and retrieval/display of candidate photo records. The descriptor information shall include physical descriptors including:
   - All of the physical descriptor information (gender, height, weight, eye color, hair color, gender, etc.) contained in the associated NIST Type 2 record.
Supplementary physical descriptor information such as hair length, skin tone, physical build, etc., as defined in a cooperative effort between MCSO and the selected Contractor.

c) Each SMT image maintained by the system shall also include:

- A record index number providing a unique reference to a specific SMT image in the identification record for an individual,
- The standard FBI code for the scar, mark or tattoo indicating the type and location of SMT,
- A single word primary descriptor,
- A primary color, and
- A free text description.

d) The selected Contractor shall work cooperatively with MCSO staff to define the record data content and parametric descriptors for the digital photo image records maintained by the system. The photo image database data model and the specific record descriptors and codes for the digital photo records shall be documented in the formal system design documentation.

e) The system’s storage capacity shall be sized to store the projected number of records that will be accumulated by Year-10 of AFIS operations, as shown in the following extension of Table 2.5-1:

<table>
<thead>
<tr>
<th>Identification Record Projections</th>
<th>Current (May 2011) Totals</th>
<th>Required (Year-10) Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCSO Mugshot Records (2 images / record)</td>
<td>325,694</td>
<td>700,000</td>
</tr>
<tr>
<td>MCSO SMT Records (3 images / record)</td>
<td>0</td>
<td>350,000</td>
</tr>
</tbody>
</table>

Notes:

1) Mugshot records include a front and a profile facial photo (2 images/record)

2) MCSO currently captures SMT records with an average of 3 SMT images for each booking record.

3) MCSO is unable at this time to separate the mugshot record and SMT record totals from each other, they are a combined total above in Table 2.5.1.

**2.5.2 Photo Capture**

a) The Photo Image Capture capability shall be provided to collect photo identification records and shall be implemented as an integrated component of each MCSO LiveScan workstation installation, with control of the photo capture operation from the LiveScan workstation.

1) The photo capture system must include an auto-aperture color camera capable of capturing 24-bit color photo images, an accessory lighting system and an 18%
gray backdrop screen. The camera will be either ceiling or wall mounted if it is not feasible to have the camera mounted on the LiveScan workstation.

2) The Workstation operator must be able to control the camera using automated pan, tilt, zoom and focus controls provided via the workstation keyboard and controls.

3) The camera systems must provide a live display of the subject on the workstation display screen to enable the operator to adjust the camera for correct image position, scale and focus, and the operator must be able to reject and recapture any photo image as necessary to attain acceptable quality.

4) Photo Image Capture Workstations shall be able to print out on 4x6 photo paper the following information: First Name, Last Name, Booking Number, Race, Gender, DOB and the Mugshot. This paper is punched out on a die and attached to a wristband for the inmate.

b) The photo camera system, controls and operations must be substantially compliant with the NIST Best Practice Recommendations (NIST BPR) for mugshot capture, and the image capture application must provide on-screen tools (crosshairs, guidelines, etc.) to assist the operator in capturing images that conform to NIST BPR image orientation and scaling recommendations.

c) User training shall be provided for LiveScan operators in the use of the digital image capture capabilities and in the techniques required for compliance with the NIST BPR.

d) The system shall support electronic interfaces with systems including the Jail Management System (JMS), SQL Reporting System (SSRS), and a public website application, and shall support the interchange of information, including:

1) The Photo Image Capture Workstations shall be able to import booking information from JMS to preload biographic and demographic information in facial and SMT photo records

   - Photo Image Capture Workstations shall be equipped with a barcode reader that will be used to scan a subject’s wristband to activate the import and pre-loading of booking data for the subject into the workstation.

2) The preloaded record data shall be displayed on the Data Entry Form screen for review and verification by the workstation operator prior to initiating photo capture. Photo record images captured by AFIS at booking shall be able to be accessed and retrieved by the JMS, and the selected AFIS contractor shall work with the JMS vendor (Intergraph) to implement the JMS mugshot image access capability.

3) Photo record images stored in AFIS shall be able to be accessed and retrieved by the MS SSRS for use in various reports.

4) Photo record images stored in AFIS, along with associated record data, shall be able to be exported to or retrieved by a public website display application.

2.5.3 Photo Identification

a) The AFIS shall support the following types of digital photo identification transactions:
1) **Facial Photo Parametric Search:** An automatic search of the on-line Mugshot records to produce a mugbook or lineup of facial photo records based on:
- Similarity of appearance to an operator-selected record; or
- Demographic and physical descriptor attributes in common with a list of input search parameters (e.g., gender, age range, race, hair color, eye color, height, weight, SMT location/type/descriptions, etc.).

2) **SMT Photo Parametric Search:** An automatic search of the on-line SMT records to produce a mugbook or lineup of photo records that have attributes in common with a list of descriptive image search parameters (e.g., tattoo location, size, color, description, etc.), and optionally a set of demographic search parameters (e.g., gender, age range, race, hair color, eye color, height, weight).

b) The system shall provide the capability to provide automatic facial photo (mugshot) retrieval and display in support of intake/booking processing of arrested individuals at the MCSO County Jail. An Applications Program Interface (API) shall be provided for integration of the photo retrieval and display capability into the jail management system booking application, and the selected Contractor shall provide technical support as required to successfully implement the photo retrieval and display capability.

### 2.5.4 Photo Investigation Capabilities

a) The digital photo management and identification capabilities shall include web-based interactive investigative tools for accessing, retrieving and searching mugshot and SMT records in the AFIS database.

b) The system shall be able to organize the photo image search respondents in a mugbook format or sequential line-up format.
- The mugbook display shall contain 25-50 images per page, with a user-selectable capability to display or hide image annotations. The full size image shall display as a 5”x7” image.
- The line-up display shall include eight (8) photo images in the following user-selectable modes, and the selected Contractor shall work with MCSO to define the viewing session setup.
  - displayed in sequence in an interactive viewing session, with a user-selectable capability to display or hide image annotations.
  - displayed in sequence in a printed lineup with the images numbered one through eight.
- Image annotations that may be displayed with a mugbook or lineup include the AFIS ID #, Agency index number(s), and name. The selected Contractor shall work with MCSO to define the information that shall be displayed in a photo annotation.
- The system shall provide interactive capabilities that enable a user to format and display photo identification information:
  - Assign a name to a mugbook or lineup and to associate the mugbook or lineup with an investigative case file for storage and retrieval.
o Print a mugbook or lineup with or without annotations.

o Store a mugbook or lineup for later use

o Edit and save as a new mugbook or lineup from an existing mugbook or lineup.

o Find existing mugbooks or lineups based on master name of suspect. Compile, store and print a warrant sheet or wanted poster containing a color facial photo image of the subject and formatted text entered by the user.

c) Email a mugshot, lineup (with or without annotations), or a warrant sheet, as an email attachment. The Contractor shall work with MCSO to have integration with the Jail Management and Records Management system to provide additional information such as charges on viewing a full mugshot.

d) Detailed training shall be provided for system users in accessing digital photo records and in using the digital photo investigative tools (mugshot/SMT searching, line-ups, etc.).
3 System Operations and Administration

3.1 System Operations

a) Each AFIS system workstation shall be provided with complete on-line user documentation specific to the workstation type or application, which is either permanently loaded on each workstation’s hard drive, that is on a CD or DVD and can be accessed using the CD/DVD drive in the workstation, or that is maintained on a central server and is accessible via the network.

b) The workstation documentation provided for each AFIS workstation shall provide a comprehensive description of:

- Operational procedures for all of the workstation’s applications functions and diagnostic capabilities.
- System error messages, along with reference to the component or process from which the message originated, a description of the meaning of the message, and a list of recommended operator responses.
- User maintenance procedures for the workstation, all workstation components and peripheral devices.

c) Each equipment installation location shall be provided with one complete set of technical reference materials for each type of workstation installed at the location. The technical reference materials for a given workstation type shall include manufacturer’s manuals for the workstation and all peripheral components, to support training, operations and maintenance at the location.

3.2 Status Monitoring and Diagnostics

a) The system shall provide system monitoring and alerting capabilities using Simple Network Management Protocol (SNMP) monitoring, with capabilities including:

- Capability to automatically monitor the central system components, processes and infrastructure services, and to provide real-time detection of the occurrence of system problems including hardware component failures, software problems and service interruptions.
- Capability to automatically generate and send email messages for notification of the system administrator and/or the responsible maintenance entity regarding the detection of a system problem.
- System administrator dashboard display of system status and problems detected with drill-down descriptions of status/problem details and response requirements.
- Capability for authorized management personnel to access and monitor system usage and system status dashboard information from a networked workstation.

b) A comprehensive AFIS Administration Applications Software Suite shall be provided to enable the designated administrator(s) to perform all required system administration, user administration, security, database administration and reporting functions of the system.
1) The Administrative Applications Software Suite shall include four primary components with the following capabilities:

- Central system operations component:
  - Central system monitoring, operations control, diagnostics, error correction and process control;
  - System update implementation;
  - System, database, and security administration;
  - Monitoring and control of transaction processing activity;

- Operations Usage and Status component: enabling authorized management personnel to access and monitor system usage and system status dashboard information from a networked workstation.

- User Administration component

- Management Reporting components
  - Database and transaction log access, analysis and reporting;
  - Operations and performance analysis and statistical reporting.
  - Complete standard and ad-hoc management reporting.

- A dedicated System Operations and Administration Workstation, including the complete Administration shall be installed and integrated into the AFIS configuration, to provide authorized administrators and the Contractor’s field engineer with on-site system access, monitoring, control and administration capabilities.

- A copy of the Status Monitoring, User Administration and Management Reporting software components shall be installed on or accessible from each Multifunction Analysis workstation.

c) The system shall maintain system monitoring logs, which are defined as the date/time stamped record of system or component starts and restarts, system or component shutdowns and off-line conditions, hardware errors reported by the AFIS operating system, software errors reported by the system’s applications software programs and infrastructure electrical service and network communications interruptions.

- The system shall provide on-line retention of daily system monitoring logs for at least 90 days, followed by permanent archival storage.

- The system shall enable authorized system administration and system support personnel to access the system monitoring log, and to selectively print reports for a specific error or incident or for a specified time period, from any workstation. Reports shall be in an easy-to-read format that clearly states the nature and extent of the hardware and/or software problem reported.
The system shall be capable of providing error logs and system status information in response to system user requests. This information shall provide intelligible assistance in the diagnosis of problems.

d) The system shall provide built-in system diagnostics and error correction capabilities, including:

- Interactive diagnostic tools with comprehensive capabilities for status checking and problem isolation for every component of the central AFIS system segments.
- Comprehensive on-line system administration documentation, including descriptions of system error messages and their interpretation, system diagnostic capabilities and operational procedures, and response requirements for specific problems.
- Remote control troubleshooting and maintenance capability to allow a remotely-located system engineer to operate central server and networked workstation diagnostics, correct operational problems and download software modifications.

e) Each AFIS system workstation shall support remote access and administration via a secure communications network connection for:

- Installing updates, including table updates, software patches, and virus signature updates on the workstations.
- Performing maintenance on the workstations, including running system diagnostics, reloading the application, restoring system defaults and local site configurations, removing or resetting transactions in the queue, resetting passwords, etc.
- Accessing and retrieving information from workstation logs, including access control logs, transaction logs and anti-virus logs (updates, detection history, etc.).

f) The system shall be able to log accesses to each workstation, maintain a record of the updates and modifications, and support analyses and reporting of the access, update and modification information.

### 3.3 System Configuration Management

a) A comprehensive capability shall be provided for the management of the system configuration, including automated and interactive tools for maintaining hardware and software configuration information, and for tracking and reporting change history.

b) The AFIS design shall incorporate user-maintainable data structures (e.g., code tables, communications routing tables, user permissions) which define and control all standard codes, values, physical configurations and security, and are supported by comprehensive documentation and user training.

c) The system shall be able to be maintained by a trained system administrator and shall not require reprogramming or manufacturer intervention to maintain system tables.

d) The system shall include a capability to test changes in an operational system environment prior to introduction of the changes into the production configuration.
3.4 User Administration

a) The system shall provide comprehensive tools and capabilities for administration of user authorizations and system security.

- The system shall enable an authorized system administrator to add and remove users, to assign, modify and suspend access privileges for any user or group of users (e.g., latent examiners), and to reset passwords.
- All system workstations shall restrict each user’s access to the application, maintenance and operating system functions of the workstation and the system applications, according to each user’s specific access authorizations.

b) The primary mechanism for access control and user authentication shall be User-ID + Password. The AFIS system shall support “strong” password authentication consistent with FBI CJIS Security Policy guidelines, for accessing and communicating AFIS information via the MCSO network infrastructure.

- LiveScan workstations shall support standard User-ID + Password.
- All AFIS latent and tenprint input/analysis workstations shall support strong password authentication and enforce associated password policies in conformance with MCSO policies.
- Where required by MCSO, and/or FDLE security policy, the capability to implement a second authentication factor using fingerprint biometric authentication shall be provided.

c) The system shall provide scheduled and on-demand administrative reporting including:

- Periodic summaries of authorized users, including individual permissions, user status (active or suspended) and date of last log-in.
- Periodic password policy compliance audits.
- Periodic security assessment compliance audits, including unsuccessful log-in analysis.

3.5 Management Reporting

a) The AFIS system shall provide the capability to generate statistical analysis and system activity reports, including standard pre-defined management reports and special reports based on user-defined ad-hoc queries.

b) The initial delivery of the system shall include a comprehensive set of standard cataloged management reports that will be produced by the system on a regular recurring basis. Full reporting capabilities shall be provided with the initial operational capability delivery of the system, including the following types of reports.

1) Database Statistics Reports: Record counts and record activity.
2) System Transaction Activity Reports

- Transaction activity statistics for identification transactions.
- System throughput and response time analysis reports.

3) Identification Operations Reports
- Active Cases & Case Details.
- Case Closures.
- Recidivist statistics.

4) Ad-hoc Reports for log analysis and audits.

The selected Contractor shall work closely with MCSO to define all details of the standard management reports (report types, content, frequency, routing, etc.) to be implemented in and delivered with the initial system configuration.

c) The system shall enable MCSO to utilize their existing MS SSRS SQL Reporting System capabilities without restriction to query system databases and logs in order to generate management reports.

d) A capability shall be provided that enables a system administrator to establish regular reporting schedules for each type of report, and that produces the reports according to the pre-defined schedules.

e) The system shall enable an administrator to selectively generate any standard report on-demand under operator control and this shall not affect the established automatic production schedule for the report.

f) The standard report generation capability shall include interactive controls that enable an operator to selectively enter filtering parameters such as ORI, AFIS ID #, Agency index number (Agency ID #, OBTS, Booking #, etc.), and date range to generate specific reports.

g) Standard reports shall be able to be automatically routed according to a pre-set distribution list, or routed under operator control to designated network workstations and/or network printers.
4 Technical Requirements

4.1 Technology Standards Compliance

a) MCSO has established internal standards for equipment and software as indicated in the following Table, and strongly prefer that hardware and COTS software provided with the AFIS be in conformance with these standards. County-furnished (CFE) capabilities, equipment and software provided for the AFIS implementation (e.g., Anti-Virus clients) will be in conformance with these standards.

<table>
<thead>
<tr>
<th>Component</th>
<th>Technology</th>
<th>Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>MS Windows 2008</td>
<td>Dell Rack Mounted</td>
</tr>
<tr>
<td></td>
<td>Advanced Server</td>
<td></td>
</tr>
<tr>
<td>Web Server</td>
<td>Linux</td>
<td>Red Hat</td>
</tr>
<tr>
<td>Workstations</td>
<td>MS Windows 7</td>
<td>Dell</td>
</tr>
<tr>
<td>Networks</td>
<td>1 Gigabit Ethernet</td>
<td>Cisco</td>
</tr>
<tr>
<td>RDBMS</td>
<td>SQL-compliant</td>
<td>Oracle / MS SQL 2008 R2</td>
</tr>
<tr>
<td>Storage Area Network</td>
<td>VNX Fiber Channel / iSCSI SAN</td>
<td>EMC</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Internet Explorer 9</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>Enterprise Anti-Virus</td>
<td>MS Forefront</td>
</tr>
<tr>
<td>E-mail</td>
<td>Outlook/MS Exchange</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Wireless</td>
<td>Cellular Subscriber Services</td>
<td>Verizon/Sprint</td>
</tr>
<tr>
<td>WiFi</td>
<td>Wireless Access Points</td>
<td>Cisco with p12 certificates</td>
</tr>
<tr>
<td>Enterprise Backup</td>
<td>Simpana 9.0</td>
<td>CommVault</td>
</tr>
</tbody>
</table>

b) MCSO has contracted with Konica Minolta to provide our agency network printers. The AFIS and AFIS workstations shall be able to print to the following printer models: Bizhub C452, C220, 501, 223, C360.

c) MCSO has established internal standards for equipment and software as indicated in the following Table, and strongly prefers that hardware and COTS software provided with the AFIS be in conformance with these standards. County-furnished (CFE) capabilities,
equipment and software provided for the AFIS implementation (e.g., Anti-Virus clients) will be in conformance with these standards.

d) The system shall utilize high-reliability components for servers and data storage systems to provide a high-availability management of identification service request transactions, with the capability to handle simultaneous transactions without loss of data.

- The system shall operate twenty-four (24) hours/day, seven (7) days/week except for a maximum of 4 hours per month of regularly scheduled system maintenance.
- System availability measured on a monthly basis shall be equal to or greater than 99.9%, excluding regularly scheduled maintenance.

*Proposers shall specify the guaranteed system availability that will be achieved by the proposed system.*

e) All workstations and applications provided with the AFIS system shall be based on standard commercially-available desktop PC computers running a Microsoft Windows operating environment. These PCs shall not be customized or otherwise modified such that MCSO would be unable to replace a defective or obsolete PC with a compatible, commercially-available replacement unit.

f) Each standard workstation shall be configured with:

1) A 24-inch or larger color flat-panel display screen with resolution adequate to support on-screen side-by-side viewing of fingerprint images and the capability to display images in at least 8-bit gray-scale or 24-bit color depth (8 bits/channel); 16-bit per channel color depth is preferred.
2) A QWERTY keyboard with a separate ten (10) key numeric pad.
3) USB mouse or pointing device.
4) An internal hard disk drive sized to support the applications software and operational data storage of the workstation in its AFIS application.
5) A CD/DVD drive with read/write capability.
6) At least two (2) USB 2.0 ports
7) A fingerprint scanner (either built-in or attached peripheral) enabling biometric authentication of users at login.

g) Anti-virus software shall be provided as CFE and administered by MCSO. All workstations and servers shall utilize MCSO’s centralized anti-virus capability.

h) All system workstations shall include a capability to synchronize the workstation clock with a universal time source.

i) Any workstation shall be able to be configured to utilize any existing network printer.

j) Each workstation type shall be configured and delivered with the appropriate applications software, peripheral devices, and system configuration settings to adapt the workstations for the intended purpose and use within the system.
4.2 National Standards Compliance

a) AFIS workstation fingerprint image acquisition, display and printing shall be in accordance with applicable FBI IAFIS Image Quality Specifications (IQS), as specified in Appendix F of the most recent version of the FBI Electronic Biometric Transmission Specification (EBTS).

b) The system shall utilize an FBI-certified compression technology for compression of fingerprint and palmprint images and shall be capable of handling images compressed with the following technologies, without restriction:

1) Wavelet Scalar Quantization (WSQ) compression method for the compression of 500 ppi tenprint and palmprint images, in accordance with the most recent version of IAFIS-IC-0110.

2) FBI-certified JPEG-2000 compression method for the compression of 1,000 ppi tenprint and palmprint images, in accordance with the most recent version of IS 15444-1, 2001, the JPEC-2000 standard approved by the FBI for 1,000 ppi fingerprint images.

3) The average (mean) compression of tenprint fingerprint images and palmprint images that are compressed by the AFIS or any AFIS workstation shall not exceed a compression ratio of 15:1.

4) Latent images (latent fingerprints and latent palmprints) shall not be compressed, and the system shall be capable of receiving, transmitting, processing, storing and maintaining latent images in uncompressed form. The system shall be capable of handling and processing compressed latent images obtained from an external agency or legacy system.

c) The AFIS system implementation shall provide full capabilities for formatting and communicating (transmitting and receiving) AFIS fingerprint and palmprint records, and latent image and minutia records in accordance with the latest version of the following national standards:


4.3 Security

a) The system and all workstation components shall provide and/or support the following security provisions:

1) All AFIS workstations shall have a standard password-protected screensaver. Users shall not be able to install other screensavers or wallpaper.
2) Standard Windows “remember your password” functions shall be disabled on all
workstations.

3) Automatically log-off a current operator when a new operator logs on, to ensure
that only a single operator can be the operator of record at any given time.

4) Automatically disable the workstation and require the operator to log in again
after a pre-determined time interval during which the workstation is inactive. The
system shall ensure that no in-process data or work is lost if a workstation is
automatically logged-off.

5) Automatically disable the workstation when a preset limit of unsuccessful login
attempts is reached and require intervention of an authorized supervisor or
administrator to re-enable the user’s access rights.

6) The system shall log all successful logons/logoffs and all unsuccessful logon
attempts.

b) Anti-virus software clients (reference §4.1) shall be installed, configured and maintained
on all Windows workstations and servers.

c) The system shall enable implementation, logging and reporting of regular security
updates (e.g. virus signatures, system software patches, network security updates) to
ensure that the security protections are current for all components of the system.

4.4 Network Communications

a) The AFIS system shall connect to and utilize the MCSO communications networks for all
communications with all AFIS workstations, terminals and peripheral devices.

b) Network communications, including network appliances (switches, routers, firewalls,
etc.) required for interconnecting the racked servers and associated components within
the central AFIS system segment or required for connecting the central AFIS segment to
the MCSO networks, shall be provided by the selected Contractor.

- Each central AFIS segment equipment rack shall be equipped with redundant
  switches for interfacing with the MCSO network.
- Each AFIS rack switch must have a 1 Gb uplink capability.
- The 1Gbps top-of-rack Ethernet switches shall be one of the following models:
  a. Cisco WS-3750X-24T-S (24 port)
  b. Cisco WS-3750X-48T-S (48 port)
- The Contractor-supplied Cisco switches shall be configured with the following:
  a. C3KX-PWR-350WAC redundant power supply
  b. C3KX-SM-10G uplink module
  c. GLC-SX-MM transceiver

c) The selected Contractor shall work pro-actively and cooperatively with MCSO technical
staff to specify network bandwidth and connectivity requirements, and to coordinate and
accomplish the planning, installation, and testing of the network connectivity for the
central AFIS system components and remote AFIS workstations and peripherals.
Proposers shall identify the recommended bandwidth requirements for communications between the core AFIS segment and the installed AFIS workstations, terminals and peripherals.

d) Designated system workstations shall be capable of being configured with an e-mail capability and the selected Contractor must work proactively with MCSO and Manatee County’s technical staff to identify and resolve any network connectivity and security issues associated with implementation of email capabilities on AFIS workstations.

e) All communications shall be compliant with FBI CJIS network security requirements for accessing and communicating criminal justice information, as applicable, and the selected AFIS Contractor shall be responsible for ensuring that all AFIS installations and operations obtain or support a full compliance certification.

1) The AFIS system shall support data encryption for communication of sensitive criminal justice information with external sources and recipients over public and private networks.

2) The AFIS system shall provide support for Virtual Private Network (VPN) and Secure Socket Layer (SSL) communications for establishing network connections with external sources and recipients over public or private networks. Any SSL encrypted application shall be required to provide 2-factor authentication including primary user-ID/password and secondary authentication, such as HW token, smart card, or biometric verification. For the AFIS system and workstations, the preferred method for secondary authentication is fingerprint biometric identification.

3) All communications with FDLE BIS and FALCON must comply with FDLE standards, message and data formats, and interface protocols.

4.5 Electrical and Environmental Standards

a) All AFIS equipment and workstations installed in or delivered to MCSO or Manatee County facilities shall be certified to be in compliance with applicable Underwriter's Laboratory (UL) standards for product and user safety.

b) All AFIS servers and workstations installed in or delivered to MCSO or Manatee County facilities shall operate on standard U.S. electrical power:

   ▪ Servers and workstations shall be configured to utilize 110 VAC, 60 Hz electrical power.

   ▪ The AFIS installation location at the MCSO data center is protected by a Manatee County-furnished UPS and generators with A and B power.

Proposers must provide the expected power consumption for their proposed central site equipment, including the AFIS, SAN, Enterprise Backup system, and associated network equipment.

c) AFIS equipment and workstations installed in or delivered to MCSO or Manatee County facilities shall be in compliance with Federal Communications Commission (FCC) Electromagnetic Interference (EMI) standards, FCC Part 15 or FCC Part 18, as applicable.
d) AFIS equipment and workstations installed in or delivered to MCSO or Manatee County facilities shall be designed for use in a normal office or jail environment as applicable, and manufacturer’s recommended conditions for operations shall cover the following environmental ranges:

- Ambient Temperature: 60°F – 90°F
- Relative Humidity: 20% – 80% Non-condensing
5  SYSTEM IMPLEMENTATION REQUIREMENTS

The goal of the AFIS Replacement Project is to complete the design, implementation and installation of the system and achieve full production operations as soon as technically feasible. The Master Implementation Schedule included in the proposed system implementation plan shall reflect the guaranteed schedule under which the system will be implemented and delivered and complete transition to production operations will be achieved. Selection preference will be provided for the vendor proposing the most expedited implementation schedule that can be realistically achieved. Proposers must acknowledge that significant penalties in the form of liquidated damages will be assessed for failure to meet guaranteed implementation schedules and are strongly advised to propose a realistic success-oriented schedule.

5.1 Contractor Responsibility

a) The selected Contractor shall be responsible for all aspects of system implementation, as required to accomplish the successful delivery of the AFIS and associated implementation services in accordance with the specified system requirements and established delivery timeline objectives. Contractor responsibilities shall include:
   - Project planning and management;
   - System requirements analysis and system design;
   - Network and infrastructure requirements specification;
   - System configuration and integration;
   - Data conversion and loading;
   - Installation planning and preparation;
   - System delivery and installation;
   - User training;
   - System testing and transition to production identification operations.

b) The selected Contractor shall maintain effective communications with the MCSO project team through the duration of the implementation process to ensure the effective exchange of information, responsiveness to customer inquiries and directives, and timely identification and resolution of questions and problems.

c) The selected Contractor shall provide leadership for implementation planning and system implementation, with pro-active support to assist MCSO in updating AFIS business rules and workflows, external system interface requirements and interoperability, network communications and security requirements and change planning/implementation, and other technical issues that require updates to realize the full potential of the new system.

5.2 Implementation Project Management

a) The selected Contractor shall be responsible for all aspects of project management, including planning, staffing, performance monitoring and oversight, subcontractor management, project coordination, quality assurance and reporting. The following specific Implementation Project Management activities shall be performed.
5.2.1 Project Plan

a) The selected Contractor shall develop a comprehensive Project Plan for the AFIS implementation project, and shall maintain the project plan through the active implementation phases of the project. The Project Plan shall include the following:

1) Project Staffing Chart – An organization chart and contact list for all individuals in the Contractor’s organization and any subcontractors who are assigned to the MCSO project or have a management or support role for any aspect of the project.

2) Master Implementation Schedule – A detailed Gantt chart, showing the time-phased schedule for accomplishing all design, development, integration, delivery and testing activities, with milestone schedules for accomplishing the primary project milestones.

3) Deliverable Schedule – A detailed Gantt chart showing the delivery, review and approval schedules for all deliverable reviews, plans, reports and documentation.

b) The Master Implementation Schedule shall include guaranteed dates for the key implementation and delivery milestones listed in Table 5.2.1-1.

c) The Deliverable Schedule shall include a detailed description and delivery schedule for reports, plans and technical documentation items that will be prepared and delivered in association with system implementation. At a minimum, the following Deliverable Data Items shall be prepared and provided in association with the AFIS implementation.

- Project Plan (final)
- Monthly Project Status Reports
- Site Preparation and Installation Plan
- Training Curricula, Courseware and Training Delivery Plan
• System operations, administration and maintenance documentation; workstation user guides for each type of workstation.

• System Acceptance Test Plan and Procedures

• System Maintenance Plan

d) The Deliverable Schedule shall reflect the understanding that all deliverables are subject to customer review and approval, and shall allow for rework to correct deficiencies prior to final review and approval.

Proposers shall submit a preliminary Project Plan as part of their response. The preliminary project plan shall provide specific details of the proposed master implementation milestone and deliverable schedules. The list of Deliverables in the Deliverable Schedule shall specifically identify each user guide and system manual that will be provided with the system.

5.2.2 Automated Project Management Tool

a) Microsoft Project shall be used for developing and maintaining the master implementation schedule and subordinate work plans.

b) The automated project management software (MS Project Professional 2010) shall be used to plan, implement, and monitor project work plans. The primary work plan and all subordinate detailed work plans (e.g., the System Implementation, Testing and Quality Control plan, Deliverable plan, etc.) shall be implemented and maintained using the automated project management software. The detailed plans shall be defined and maintained at a level that will enable an ongoing assessment of the adequacy of the plan and the progress of planned implementation activities.

c) The master implementation schedule shall be updated as necessary throughout the implementation cycle to reflect changes in scheduled activities. The baseline schedule shall be separately maintained to enable assessment of progress against the original schedule.

d) The monthly project schedule update shall be delivered not less than two full working days prior to the monthly project status review meeting.

e) One copy of MS Project Professional 2010 shall be delivered to the MCSO Project Manager for use in project tracking within ten (10) days after contract award.

5.2.3 Project Status and Progress Reporting

a) Informal weekly reviews and formal monthly reviews of project status, progress and current issues shall be provided throughout the duration of the AFIS implementation project.

1) The selected Contractor shall prepare for and participate in informal weekly project status meetings with the MCSO Project Team to discuss project status and to resolve issues. Directives, resolutions and action assignments shall be documented in writing by the Contractor’s Project Manager and the document shall be delivered to the Project Team no later than 4:30 p.m. of the next business day after the meeting.
2) The selected Contractor shall prepare for and participate in formal monthly project review meetings with the MCSO Project Team. At the formal monthly project review, the Contractor shall present the status of all project tasks, identify problems and potential risk areas, coordinate the development of action plans to resolve issues, and discuss the detailed activities planned for the next reporting period. Each review shall include a detailed discussion of the project schedule and any actual or projected variances between the baseline schedule and the current activities. Directives, resolutions and action assignments shall be documented in writing by the Contractor’s Project Manager and the document shall be delivered to the Project Team no later than 4:30 p.m. of the next business day after the meeting.

5.3 **Project Staffing**

a) Contractor shall be responsible for providing adequate qualified staffing for the project to accomplish the system implementation and provide the associated services in accordance with the contractually-established schedule.

b) The project staffing plan shall include the identity and qualifications of key staff that will be assigned to the project, including key individuals for the following positions. **Proposers shall provide a staffing plan in their proposal response that identifies all key personnel, describes their roles and responsibilities, provides an experience summary for each key person that supports his/her project role, and defines the reporting structure of the project within the Offeror’s organization.**

5.3.1 **Key Personnel**

5.3.1.1 **Project Manager**

a) The selected Contractor shall provide a dedicated Project Manager whose project management responsibilities shall include:

- Planning and monitoring project activities.
- Working with the MCSO Project Manager and representatives of the agencies to ensure timely and effective response to information requirements and to resolve actual and/or potential problems.
- Reporting on project status.
- Providing analytical and technical expertise as required by the project.
- Obtaining and scheduling the use of required Contractor resources.
- Management and quality assurance of all required implementation and support services.
- Quality assurance of all documentation deliverables

b) The proposed Project Manager shall have directly applicable qualifications, including:

- AFIS implementation project management experience.
- Experience with Contractor's AFIS technologies.
5.3.1.2 System Engineer

a) The selected Contractor shall provide a dedicated senior System Engineer whose project responsibilities shall include:

- Oversight and coordination of the detailed system design and implementation activities, with ongoing monitoring to ensure conformance with all specified System Requirements.
- Primary technical liaison with the MCSO project team with responsibility for defining and obtaining concurrence for implementation and operational details including workflows, component configurations, default settings, etc.
- Oversight and coordination of system integration and testing activities to ensure conformance of the system with system requirements and implementation agreements.
- Direct involvement in the preparation of formal test plans for pre-delivery, installation, and formal acceptance testing, and leadership of all formal testing activities.
- Quality assurance of system deliverables and associated technical documentation.

b) The proposed System Engineer shall have directly applicable qualifications, including:

- Professional systems engineering experience.
- Experience with Contractor's AFIS technologies.
- Implementation experience with equivalent Law Enforcement AFIS systems.
- System acceptance testing and delivery experience.

5.3.1.3 Conversion Manager

a) The selected Contractor shall provide a Conversion Manager whose project responsibilities shall include:

- Development of the Conversion Plan, with ongoing coordination to maintain and update the detailed plans and procedures as necessary to accomplish the successful conversion and loading of the system data.
- Primary conversion liaison with the MCSO project team with responsibility for developing detailed procedures for record handling and tracking during conversion and providing regular status reporting on conversion activities.
- Oversight and coordination of conversion facility preparation and conversion activities.
- Preparation of analysis and test plans to verify and validate the converted and loaded databases, and leadership of the verification and validation activities.
- Direct management and technical oversight of the conversion, database loading, conversion verification/validation, and delivery of the converted data.

b) The proposed Conversion Manager shall have directly applicable qualifications, including:
   - Experience with Contractor's AFIS technologies.
   - Conversion planning and formal Conversion Plan preparation and coordination.
   - Electronic tenprint and palmprint conversion experience.
   - Electronic latent conversion experience.
   - Direct management responsibility for an equivalent conversion project.
   - Direct experience in quality evaluation, error correction enhancement, and delivery and acceptance of the converted data.

5.3.1.4 Training Manager

a) The selected Contractor shall provide a Training Manager whose project responsibilities shall include:
   - Development of the Training Plan, with ongoing coordination to maintain and update the detailed plans and procedures as necessary to accomplish the delivery of all required Training.
   - Primary training liaison with the MCSO project team with responsibility for developing detailed delivery plans and content requirements for each training course, and for providing regular status reporting on conversion activities.
   - Coordination of training schedules and preparation activities.
   - Oversight and direction of training delivery and leadership of the training assessment activities.

b) The proposed Training Manager shall have directly applicable qualifications, including:
   - Professional training management experience.
   - Professional AFIS Training experience for an equivalent installation.
   - Experience with Contractor’s AFIS technologies.

5.3.1.5 Operations and Maintenance Support Manager

a) The selected Contractor shall provide an Operations and Maintenance Support Manager whose project responsibilities shall include:
   - Primary responsibility for planning, coordinating and accomplishing system delivery preparations, system delivery and installation.
   - Development of the Operations and Maintenance Support Plan, with ongoing coordination to maintain and update the detailed plans and procedures as necessary to accomplish the effective delivery of operations and maintenance support.
• Primary technical liaison with the MCSO project team with responsibility for planning, coordinating, and implementing the operations and maintenance support capabilities.

• Participation in training preparation and delivery for providing operations and maintenance support training for system administrators and support staff.

• Oversight and direction of the operations and maintenance support activities during the initial warranty period and through the full production period.

b) The proposed Operations and Maintenance Support Manager shall have directly applicable qualifications, including:

• Technical experience with computer systems and software.

• Professional maintenance and technical support management experience.

• Experience with installation, operation and support of the Contractor’s AFIS technologies.

• Experience in providing technical support in a law enforcement environment.

5.3.2 Personnel Assignments and Access

a) All Contractor, subcontractor, and other personnel assigned by the Contractor to the MCSO AFIS project shall be apprised of and shall acknowledge their responsibilities with respect to the confidentiality of MCSO and Manatee County installations, capabilities, work processes and data.

b) MCSO reserve the right to approve all personnel assigned to the project, including all proposed staffing changes, and to explicitly authorize participation and facilities access for each assigned individual. MCSO reserve the right to unilaterally request the replacement of any individual assigned to the project, and the Contractor shall accomplish the replacement with a person of appropriate qualifications for the assigned position in a timely manner.

c) All personnel who perform services at any MCSO facility, or have access to data, shall be required to pass a background check, including a fingerprint-based criminal history check. Individuals who do not pass a background check will not be allowed to access facilities or data.

d) With respect 5.3.2.b and 5.3.2.c, above, the decision of the Sheriff is final.

5.4 System Design

a) The selected Contractor shall design the AFIS to provide comprehensive capabilities as defined in the AFIS Requirements Specification, and shall apply internal quality control processes to verify that the system design is in conformance with each and every detailed functional and performance requirement of the system.

b) In support of development of the system design, the selected Contractor shall organize and conduct a System Requirements Review to develop details of all system internal and external interfaces, each system workflow, and the definitions of all data to be used, created and managed by the system.
c) A detailed System Design Document (SDD) shall be prepared and delivered for review and approval in accordance with the deliverable schedule established in the Implementation Project Plan. The SDD shall include:

- A requirements traceability matrix, providing a reference index to the system/subsystem element and/or workflow that satisfies each technical requirement in the AFIS Requirements Specification.
- A data model for each of the system databases.
- A comprehensive set of system workflows for accomplishing all required elements of transaction processing.
- A detailed technical description of all modifications and upgrades to their standard COTS AFIS components that are proposed to satisfy the requirements of the MCSO installation.
- A system configuration specification, including Interface Control Document (ICD) sections describing the physical and logical configurations of each system external interface, and including full details of the network configuration that will be implemented to interface with the MCSO networks for communications among the AFIS components.

5.5 System Installation

5.5.1 Installation Planning and Management

a) The Contractor shall be responsible for planning and accomplishing installation of the AFIS, its components and its workstations, and for providing effective coordination with MCSO to ensure minimal impacts to operations at each installation site.

b) The core segment of the central AFIS system shall be installed in the Manatee County PSC data center.

c) Rack enclosures, distribution, and inter-rack cabling are provided in the PSC data center to ensure consistency, efficiency and interoperability. Racks in the PSC data center are standard 19" width with a maximum working depth of 29" (APC rack model AR3100). Racks are supplied with two power distribution units (A + B) in either 110v or 220v. All equipment within a rack must run at one of those voltages.

d) The PSC data center facility provides power protection (power conditioning and backup power), HVAC environmental conditioning, and direct access to the MCSO Core Network.

1) The central AFIS servers and associated equipment shall be configured and installed in a County-furnished standard 19-inch equipment rack in the Manatee County PSC Data Center. In their response, Proposers shall include:

   a) A rack diagram illustrating the components and installation layout proposed for the central AFIS segment to support Year-10 projected workloads and storage capacities.
b) An estimate of the power consumption requirements for the central AFIS components that will be installed in the MCSO Data Center, including start-up and steady-state requirements for each itemized component and for the complete central AFIS.

c) An estimate of the thermal load produced by the central AFIS components for each itemized component and for the complete central AFIS.

2) The Contractor shall work cooperatively with MCSO and Manatee County technical staff to plan, prepare for and manage the installation of the systems in the designated data centers. The Contractor shall be responsible for accomplishing AFIS installation, configuration and testing while minimizing any disruption or impact to on-going production operations in the MCSO and Manatee County’s Data Center.

e) The Contractor shall work cooperatively with each agency to identify the specific installation locations for each deliverable component and to coordinate the installation and testing of all AFIS workstations and peripheral components.

f) The AFIS and workstation installations shall utilize existing MCSO LAN and WAN communications networks for communicating between the central AFIS and remote workstations. The selected Contractor shall be responsible for implementing the system communications in accordance with MCSO policies and standards, shall work cooperatively with MCSO to plan, implement and test the system’s network communications, and shall be solely responsible for resolving any conflicts between the AFIS system and existing applications using the core network. Proposers shall provide a positive response to this requirement.

g) Contractor shall be responsible for implementing all network security provisions on all AFIS components, as necessary to comply with FBI CJIS, FDLE and MCSO communications security policies.

h) Contractor shall provide assistance to MCSO for coordinating and accomplishing the removal of the existing MorphoTrak AFIS equipment, workstations and associated peripherals for disposition by MCSO.

5.5.2 Site Surveys

a) Contractor shall conduct site surveys of each designated installation location and work with facility managers at each location to identify specific installation locations and associated requirements to support preparation of a detailed installation plan. Contractor shall:

1) Provide a detailed floor plan showing equipment sizes, clearances, and suggested arrangement for installation site.

2) Document the thermal loads associated with AFIS equipment in each installation area, assess the environmental conditioning capability at each installation site, and identify locations where the thermal loads may result in environmental issues.

3) Assess the adequacy of power supplies in each installation area and identify any potential power issues associated with the AFIS equipment installations.
4) Identify communications network connectivity requirements at each installation area and provide site-specific requirements for network drops.

5) Identify any other special facility preparation requirements and installation support equipment at installation location that are necessary for installation of the applicable system components or to support training and testing.

b) Contractor shall develop a detailed Site Preparation and Installation Plan and provide timely coordination with MCSO to effect installation location preparation requirements such that facility preparation requirements do not delay installation of the system. MCSO shall be responsible for providing all such facility preparations and supplying installation support equipment.

### 5.5.3 System Delivery and Installation

a) Contractor shall be responsible for coordination and accomplishing the delivery and installation of all system components, including:

- Coordination of shipping, delivery and receiving of all system components;
- Installing all system components in their designated installation locations;
- Loading software and databases as necessary and configuring all components to operate in the MCSO environments;
- Connecting the installed components to the communications networks at each installation location and verifying interfaces with external systems, including the MCSO jail management system and the FDLE BIS and FALCON systems;
- Inspecting and testing all installed components to verify complete functionality of the system and the operability of all system interfaces.

b) Installation of all AFIS components, workstations and peripherals shall be in accordance with applicable laws, codes, ordinances and industry standards.

c) In the event that any installation is found to violate specific law, code or ordinance, the Contractor shall be responsible working proactively with the host agency management to accomplish timely modifications to bring the installation into conformance.

d) At the completion of system installation and successful accomplishment of the installation test, Contractor shall certify the availability of the full operational capabilities of the installed system and obtain MCSO approval to proceed with formal acceptance testing.

### 5.6 SYSTEM ACCEPTANCE

#### 5.6.1 System Acceptance Testing

a) The system shall be subjected to a sequence of formal tests associated with major implementation milestones, and each formal test shall be performed and successfully completed before the Contractor will be authorized to proceed to the next implementation stage. The following formal and informal acceptance tests will be performed at the designated implementation stages:
<table>
<thead>
<tr>
<th>Test</th>
<th>Implementation Pre-requisite</th>
<th>Result of Successful Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Installation Verification and Operational Readiness Test (informal)</td>
<td>Completion of system development, database loading, site installations, network connectivity, and final configurations.</td>
<td>Approval to commence final Formal Acceptance Test Test (SAT)</td>
</tr>
<tr>
<td>System Acceptance Test (SAT)</td>
<td>Completion of system delivery, user training, and establishment of the support infrastructure.</td>
<td>Completion and sign-off of formal acceptance testing.</td>
</tr>
</tbody>
</table>

b) The Site Installation Verification and Operational Readiness Test shall include:
   - Inspection and acceptance of record conversion and database loading;
   - Inspection of all equipment installations;
   - Operability verification of all component-level functional capabilities;
   - Operability verification of system interfaces and system workflows.
   - Inspection of system administration documentation and user guides.

c) The System Acceptance Test (SAT) shall include:
   - A comprehensive functional test demonstration of all system capabilities;
   - A throughput and accuracy performance benchmark test;
   - Verification of completion and certification of all user training.
   - A final verification of complete requirements satisfaction using a comprehensive requirements matrix.

d) The Operational Acceptance Test (OAT) shall include:
   - Successful completion of 60 days of full production operations.
   - Analysis of production data and activity reports, and confirmation of required operational availability and performance levels.
   - Resolution of all outstanding deficiencies and retesting as necessary.
   - Final acceptance certification.
5.6.2 Acceptance Testing Plan and Procedures

a) Contractor shall prepare and deliver a formal System Acceptance Testing Plan and Procedures (SAT Plan/Procedures) document, which shall be used to coordinate each stage of system acceptance testing. The SAT Plan/Procedures shall include a detailed definition of all tests, including:

- Operational, functional and performance test scenarios and procedures.
- Makeup and content of test data sets.
- Operational and technical oversight and support during testing, and the roles of participants.
- Development, management and reporting of resolution plans for correcting any system deficiencies and discrepancies that are found during acceptance testing.

b) A detailed requirements traceability matrix shall be included in the SAT Plan/Procedures which shall facilitate the assessment of the test plan, test results and compliance of the system with all requirements.

c) The SAT Plan/Procedures shall be prepared and delivered not less than two (2) weeks prior to commencement of the final SAT.

Proposers shall include the proposed testing and delivery schedules in their proposed Master Implementation Schedule, and shall include the initial delivery and each test-specific update of the Acceptance Test Plan and Procedures as deliverable milestones in their Implementation Schedule.
6 CONVERSION AND LOADING OF EXISTING RECORDS

6.1 Scope

a) The selected Contractor shall be responsible for converting and loading existing identification records into the new AFIS system. The long-term goal for conversion is to establish high-quality identification record databases with 1,000 ppi fingerprint images for the highest possible identification accuracy. Selection preference will be given to the VENDOR that commits to pursue and implement the most cost effective approach to meet this goal within the MCSO’s budgetary constraints.

b) A comprehensive analysis of the converted records shall be performed to provide an initial characterization of the AFIS databases, to identify errors, and to provide automated correction of correctable errors.

1) A report shall be prepared and provided that documents:
   - The total numbers of records of each record type;
   - Record quality distributions of each record type;
   - Error statistics in the converted data, for types of errors specified by MCSO.

2) A master list report of all person records shall be prepared which identifies and provides statistics of all complete and incomplete person records. For incomplete records, the report will indicate which record elements are missing in each person record.

3) Automated checking of each converted tenprint record shall be performed to detect and, where possible, correct tenprint sequence errors. A report shall be prepared and provided that documents the records in which sequence errors were detected, the corrected on-line records, and the records that could not be corrected during the conversion processing.

4) Automated AFIS matching of all fingerprint records shall be performed to detect duplicate records in the converted databases. A comprehensive duplicate record report shall be prepared and provided showing all records automatically consolidated under a given AFIS ID #.

c) The 2011 year-end totals for records maintained in the existing system were approximately:
   - 766,000 tenprint records
   - 416,000 palmprint records

There were approximately 366,000 MCSO mugshot records on at the beginning of 2012. MCSO mugshot records are maintained in an SQL database under MCSO control.

The following Table provides estimates of the number of each type of record that will be required to be converted and loaded in the new AFIS system, based on 2011 year-end projections.
Table 6.1-1: Record Conversion Requirements

<table>
<thead>
<tr>
<th>Files</th>
<th># of Records (estimate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST Tenprint Fingerprint Records</td>
<td>785,000</td>
</tr>
<tr>
<td>NIST Palmprint Records</td>
<td>435,000</td>
</tr>
<tr>
<td>Unsolved Latent Finger Images</td>
<td>50,000</td>
</tr>
<tr>
<td>Unsolved Latent Palm Images</td>
<td>50,000</td>
</tr>
<tr>
<td>MCSO Mugshot Records (2 images/record)</td>
<td>385,000</td>
</tr>
</tbody>
</table>

d) The selected Contractor shall convert all available records of each type.

Cost proposals shall provide a cost for conversion of all available records (Table 6.1-1), and provide a per-record cost for conversion of additional records of each type above the quantities shown in Table 6.1-1. For hardcopy tenprint and palmprint conversion, cost estimates shall identify costs for each increment of 100,000 records, as well as a per-record cost for conversion.

6.2 Record Conversion Performance

a) The selected Contractor shall be responsible for all aspects of accomplishing record conversion and initial loading of the AFIS databases, including planning, process management, quality control, progress reporting and agency coordination. The selected Contractor shall also be provided access to all electronic NIST records for conversion. A Conversion Manager shall be assigned to lead and coordinate conversion planning and accomplishment.

b) During the planning and accomplishment of record conversion, the Conversion Manager shall participate in weekly and monthly program reviews, provide status reporting, and coordinate the resolution of issues.
7 TRAINING

7.1 Scope

a) The selected Contractor shall provide comprehensive training in the operations and management of the AFIS system and its workstation components, as applicable to system users, supervisors, managers and operations support personnel.

b) The system shall be capable of supporting training of new users without impacting production operations or the integrity of the system’s identification records databases.

c) The following types of operations and administration training shall be developed and provided for MCSO managers, administrators, and operations staff:

1) **MCSO Management Training:** A one-hour (approximate) management-level orientation presentation covering the system architecture and installation, system operations and administration, system monitoring and performance assessment, management reporting, and the roles, responsibilities and procedures for operations and support.

2) **System Administrators:** Detailed system and application-specific training for the assigned system administrators in the use of the System and Database Administration Workstation applications, including procedures for AFIS, system administration, database administration, user administration, security administration, and system monitoring and reporting.

3) **System Users:** Detailed training for designated users of each specialized type of workstation or terminal, including the LiveScan Workstations, Multifunction Analysis Workstations, and Latent Input Workstations. The training shall include an overview of the system and a discussion of general operational concepts and support procedures, along with detailed classroom and hands-on training in the operation of all functions of the specific workstation. Individual training courses shall be designed for each operational unit and multiple training courses shall be provided as necessary to accommodate all designated trainees.

4) **Operations Managers & Supervisors:** Training for operations managers and supervisors shall include procedures for database and transaction log access, activity analysis, security management, and report generation. The training shall be designed as appropriate for each operational unit.

d) Technical orientation training shall be provided for the designated MCSO Information Technologies staff. This training shall include technical descriptions and operating procedure discussions covering the AFIS system architecture and operations, network operations, database administration, system monitoring, security management, backup and archival operations, business continuity operations, and system recovery operations.
7.2 Training Plan

a) The selected Contractor shall develop a detailed training plan identifying the task and milestone schedule for coordinating training requirements coordination, training courseware development, and training delivery.

b) The Contractor shall coordinate with all MCSO operational units to identify the training requirements for each group of AFIS users, supervisors and managers, including:
   - Number of users, supervisors and managers requiring training, and the maximum number that can be trained in each training class;
   - Specific training to be provided in each of the general types of training classes identified in §7.1.c, and the estimated duration of each class.
   - Training location(s) for each type of training for each operations unit.

7.3 Training Delivery

7.3.1 Training Management

a) The selected Contractor shall be responsible for all aspects of preparing and delivering training for AFIS users, supervisors and administrators at all of the equipment installation sites.

b) A Training Manager shall be assigned to lead the planning, preparation, coordination, and delivery of training for the system and its distributed workstation and application components.

c) The Training Manager shall work closely with the MCSO Project Manager to ensure that MCSO policies and procedures are correctly represented in each training session.

d) During the planning, preparation for, and delivery of training, the Training Manager shall participate in weekly and monthly program reviews, shall report status, and coordinate the resolution of problems and issues.

7.3.2 Training Courseware

a) Comprehensive training courseware and associated training materials shall be developed and submitted for review and approval. Any required modification or updates shall be incorporated and final courseware and materials shall be delivered prior to commencement of training.

b) All AFIS lesson plans, courseware and training materials shall be delivered in a form that can be reproduced and used by MCSO in on-going training and shall become the property of MCSO.

c) Under the system maintenance agreement, the selected Contractor shall provide updates and modifications to the courseware and training materials as required to maintain currency of the training materials as system upgrades and changes are implemented throughout the life of the system.
7.3.3 Scheduling and Conducting Training

a) On-site training shall be provided for MCSO units at each unit’s operations location(s).

b) The selected Contractor shall develop a training delivery schedule in close coordination with each operations unit.

- Each type of training identified in Section 7.1 shall be scheduled in coordination with MCSO, and the final coordinated schedule shall be incorporated in the final Training Plan.

- Multiple training sessions shall be provided as required to accommodate all designated trainees at each location, and day, evening, and night-shift training shall be scheduled to support shift workers as required.

c) Each of the Contractor’s training courses shall include a provision for MCSO Project Manager or designates to participate as co-trainers in all training classes to present MCSO policies and procedures related to AFIS operations.

d) Table 7.3-1 lists the projected number of personnel in each agency and unit that shall receive each type of training in association with the implementation of the AFIS.
Table 7.3-1. Training Headcount Projection

<table>
<thead>
<tr>
<th>Type of Training</th>
<th>Management Training</th>
<th>System Administration Training</th>
<th>Latent Workstation User Training</th>
<th>Tenprint ID Workstation Training</th>
<th>LiveScan Training</th>
<th>Mugshot Investigations Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Shift</td>
<td>1 1 1 1 1 2 3 4 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o MCSO Management</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>o MCSO Fingerprint Unit</td>
<td>1 3 4 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o MCSO IT</td>
<td>15 3 1 1 2</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o MCSO Jail LiveScan</td>
<td>6 6 6 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o MCSO Detectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>
8 MAINTENANCE AND SUPPORT

8.1 Scope of Maintenance and Support

a) The selected Contractor shall have the primary role in supporting and administering the AFIS system, and a comprehensive program of technical support, operations support and preventive and remedial maintenance support for AFIS system equipment and software shall be provided throughout the life of the system. The central AFIS installation and all AFIS workstations must be 100% Vendor supported and administered.

b) The required elements of this technical, operations, administrative and maintenance support that shall be provided by the Contractor are:

1) AFIS product and application support, including system configuration, system operations, database administration, reporting, system performance monitoring, backup and archival operations, and system recovery operations.

2) Technical coordination with and support of MCSO/IT as necessary for network and security configuration and interoperability.

3) Regular preventive maintenance of the AFIS central identification system segments and the networked workstations.

4) On-site remedial response to hardware or software problems with the AFIS central identification system segments and the networked workstations.

5) Repair or replacement of defective components and components that can no longer maintain required levels of performance.

6) Provision and maintenance of spares kits containing critical spare parts for the AFIS central identification system segments and the networked workstations.

7) Software version management, with regular updates to apply approved patches and updates, maintain current versions of all software components and to achieve or maintain compliance with new and evolving federal and State standards.

8) Technical support for system expansion and extension of standard services to new users.

9) System configuration management.

10) System backups and restoration.

11) Monthly reporting of routine activities and problem detection and resolution status.

12) Support for annual User Group meeting attendance.

c) All service and support of the AFIS processing components, software, and workstations shall be provided under a comprehensive System Maintenance Agreement for the system. The System Maintenance Agreement shall provide for all of the maintenance support elements defined above, and the selected Contractor shall be solely responsible for delivery of maintenance services under the Agreement.
Proposers shall specify the services that will be provided under their proposed System Maintenance Agreement, and shall provide maintenance options for annual renewable maintenance and a 10-year Extended Warranty.

d) The System Maintenance Agreement shall establish contractual service level agreements and shall provide for performance penalties in the form of Liquidated Damages or another appropriate remedy in the event of failure to meet the established service levels.

### 8.2 System Warranty

a) The system shall be covered by a comprehensive two-year warranty, under which all elements of system maintenance and support as listed in §8.1 and described in §8.3 are provide at no additional cost for the two-year period beginning upon successful completion of the Operational Acceptance Test (reference §5.6.1) and final acceptance of the system.

b) The following options for extended warranty and maintenance support beyond the original 2-year warranty period shall be provided:

1) Annual renewable maintenance: (year-to-year system maintenance beginning after the base 2-year system warranty period), with a proposed not-to-exceed annual rate increase cap.

2) 10-year Extended Warranty support option: base 2-year system warranty plus 8 additional years of warranty maintenance support, with a complete technology refreshment during or at the end of year-5, as described in the following paragraph. The cost of the Extended Warranty support, including Technology Refreshment, shall be billable in equal annual amounts and shall not be subject to an annual rate increase over the term of the original agreement.

c) A Technology Refreshment option: A Technology Refreshment shall be performed during Year-5 of production operations. The Technology Refreshment shall be offered as a Priced Option, and the option prices shall be valid through month 60 of the contract. Under the 10-year Extended Warranty option, the Technology Refreshment cost shall be incorporated into the 10-Year Extended Warranty cost (i.e., the technology refreshment is not optional under the 10-year Extended Warranty plan). The technology refreshment shall include:

- Replacement of all hardware components (servers, workstations, storage systems, backup components, etc.) with current technology components.

- Expansion of system performance and capacity capabilities as necessary to maintain system performance at the projected year-10 workload and records storage projections.

- Update of all operating system software to the then-current versions.

- Update of all AFIS applications software to the then-current versions, including new features, functionality and support for federal and state standards.

- AFIS applications refresher and update training for all operators, administrators and managers.
8.3 **System Maintenance**

a) The Contractor shall provide system operations support, preventive maintenance, warranty maintenance and on-call remedial maintenance of the system in accordance with the following detailed requirements.

b) System maintenance shall be provided throughout the life of the system, so long as contractual maintenance coverage is maintained by MCSO.

   - System maintenance coverage shall not be terminated or discontinued by the Contractor during the operational life of the system.
   - The Contractor shall not refuse to renew the maintenance contract or unilaterally modify the terms of the maintenance contract.

8.3.1 **Local Technician**

a) The selected Contractor shall locate and assign a technician in the Manatee County area to provide all on-site maintenance services and coordinate remedial maintenance as required. The Contractor’s local technician shall be able to respond and be on-site within two hours of a call for service when on-site maintenance is determined to be necessary.

b) The technician shall be fully trained and qualified to provide all aspects of operations support, preventive maintenance, first-tier remedial maintenance, management of the spares inventory, performance of system backups and regular status reporting regarding routine operations and problem detection and resolution.

c) The assigned technician shall successfully pass an MCSO background check.

d) At their sole discretion, the MCSO may request, and the Contractor shall comply with the request to replace the assigned technician.

8.3.2 **Operations Support**

a) Contractor shall provide a 24x7 help desk capability that answers calls for service for incidents, problems and questions, and that coordinates problem resolution.

b) The help desk shall be staffed with technical system specialists, providing expertise in systems operations.

c) The help desk shall have remote diagnostic capabilities for remotely diagnosing problems and for either correcting problems remotely or providing detailed problem information to the local area technician.

d) The help desk shall maintain a detailed date/time-based log of all calls for service with updates documenting the response to the call and the resolution of the service issue (Reference §8.3.8). Contractor shall provide a weekly report of calls for service to the designated MCSO support office.

8.3.3 **System Backups**

a) The local area technician shall perform regular partial and full system backups, perform analyses of the backups to identify and correct problems, and maintain backup media indices.
Daily incremental backups (6 incremental backups / week), a weekly differential backup, and a full monthly backup shall be performed. The backup procedures shall ensure that a restore point is maintained within 24 hours of any potential outage.

b) Weekly reporting of backup status shall be provided.

c) The system backup process will utilize backup to disk with provision for offsite storage of Backup volumes at a designated MCSO facility.

8.3.4 Preventive Maintenance

a) Preventive maintenance of the central identification system and networked workstation components shall be scheduled performed on a regular monthly basis.

- System downtime associated with regular preventive maintenance and system updates shall be limited to a maximum of 4 hours per month.
- Central system maintenance shall be scheduled in conformance with MCSO maintenance schedules and policies.
- The regular workstation maintenance schedule for each facility shall be coordinated with facility or component managers to be at times selected to minimize impacts to operations.

b) The local area technician shall provide regular support to MCSO IT operations including but not limited to:

- Regular monitoring of anti-virus status. The technician shall monitor to ensure that virus signature updates are successfully distributed to all system workstations and shall provide periodic analysis and reporting of anti-virus status and issues.
- Providing regular system patches, maintaining the system at the current Microsoft patch level, and providing Operating System upgrades.

8.3.5 Remedial Maintenance

a) Contractor shall correct all system problems, whether caused by hardware or software or both in combination, when the problem reduces the functional or performance capabilities of the system or otherwise impacts operations.

b) Contractor shall utilize remote diagnostics to isolate, diagnose and correct system problems, and support the local area technician in correcting problems and restoring production operations. Connectivity and procedures for remote diagnostics shall be in accordance with MCSO security policies.

c) Remedial maintenance coverage shall be provided as follows on a 24 hours-per-day, 7 days-per-week basis.

1) The local area technician shall acknowledge a call for service within 10 minutes of the call and inform the call originator of the plan of action.

2) If applicable, remote diagnostics and remediation shall be initiated within 1 hour of the call for service to investigate or resolve the problem, and the call originator
or a unit supervisor shall be notified when remote access to the workstation or component is to be initiated.

3) If an on-site response is required, an estimate time of arrival shall be provided.
   - For central AFIS system problems, the on-site response time shall be not more than 2 hours.
   - For LiveScan problems at an MCSO Jail or Juvenile Center, the on-site response time shall be not more than 2 hours, and the problem shall be corrected and complete operational capabilities shall be restored within two (2) hours after the technician arrives at the workstation location.
   - For Latent or Tenprint workstation problems at MCSO, the on-site response time shall be not more than 2 hours during normal business hours (M-F, 7a-5p).

4) Throughout the resolution process, the call originator shall be kept informed of the progress of the resolution effort and shall be notified when the problem is resolved.

5) For central identification system problems, complete restoration of system capabilities shall expedited to maintain the required level of system availability established in this specification. The maximum allowable down-time for any single component is 24 hours, but that down-time shall not be allowable if it causes overall availability to fall below the required levels.

### 8.3.6 Repair / Replacement of Defective Components

a) Contractor shall be responsible for repair or replacement of defective components under the System Maintenance Agreement. A defective component is one that: (a) has completely failed; (b) has experienced intermittent problems requiring remedial maintenance attention more than three times in any 30-day period, or (c) cannot be corrected to provide required levels of performance or service. Contractor shall provide replacement components that are equivalent to new specifications.

b) Contractor shall have sole responsibility for securing warranty repairs and replacements under any applicable manufacturer’s warranty programs. However, failure to obtain any expected warranty service from a manufacturer shall not relieve Contractor of the responsibility for delivery of maintenance services in accordance with the response times defined in this section.

### 8.3.7 Software Maintenance

a) Contractor shall provide software and database maintenance support to maintain currency of the system software and to rapidly respond to and correct problems with system functional capabilities and databases.

b) Software maintenance shall include the replacement of software that becomes obsolete or for which the manufacturer discontinues support during the maintenance period. When the manufacturer (e.g. Microsoft) announces that support for a product will be
discontinued, the Contractor shall work proactively with the agencies to prepare for, plan, implement, test and transition the system to a current supported-technology system.

c) Contractor shall provide software updates, modifications and patches to maintain optimum operational capabilities, to maintain compliance with new agency, State and federal regulations, to maintain compliance with evolving imaging technology standards, and to maintain coherence and currency of operating environments.

d) The on-line user documentation shall be maintained and updated throughout the life of the workstation type to reflect hardware/software version updates and modifications.

e) The local area technician shall assist agency personnel in determining the necessity of applying critical and routine software updates (e.g., Microsoft service packs).

f) A formal change management process shall be implemented and used to provide scheduling and obtain approval for all software modifications.

8.3.8 Functionality and Reliability Improvements

a) All functionality and reliability improvements that are released by the selected Contractor for the same type of equipment as being maintained under the terms of the maintenance contract shall be implemented in the AFIS without additional charge during the period of the maintenance contract.

8.3.9 Maintenance Scheduling, Problem Tracking and Reporting

a) Comprehensive management of the maintenance program shall be provided during the life of the contract, including:
   1) Maintenance scheduling and management reporting.
   2) Problem tracking using a formal problem tracking, resolution and sign-off methodology.
   3) Standard problem escalation procedures for handling all types and levels of problem situations.
   4) Regular reporting of the status of all routine operations support, preventive maintenance, and problem response and resolution.

b) A problem log and service record shall be maintained for each system hardware and software component. Agency system administrators shall have interactive capabilities to access the log and obtain information to aid assessment of system availability and effectiveness.

c) An incident report shall be prepared and provided upon completion of each remedial maintenance call. The report shall include at least the following information:
   1. Type of incident
   2. Date and time notified
   3. Date and time of arrival
   4. Type and model number(s) of machine(s)
   5. Time spent for repair
6. Time repair completed  
7. Service provided  
8. Description of malfunction  
9. List of parts replaced  
10. Action taken to prevent recurrence  
11. Signature of site representative  

8.3.10 Annual User Group Meeting  

a) The maintenance contract shall include a provision for three (3) MCSO staff members to attend the annual User Group meetings through the life of the warranty period and maintenance agreement. The participation support shall include conference fees, airfare, and lodging for each agency participant. There should also be provisions for MCSO staff member shared rental ground transportation in areas without adequate mass transportation systems in place.  

8.4 System Maintenance Plan  

a) A comprehensive System Maintenance Plan shall be developed and maintained describing the plan and procedures for managing and providing system maintenance and operations support. The System Maintenance Plan shall include the following:  

1) Maintenance Organization – A description of the maintenance organization that will be directly responsible for performing the maintenance services for the central identification system and networked workstations. The description shall include qualifications of the local area technician and a description of the technical support organization capabilities and procedures.  

2) Warranty Period and Warranty Maintenance - A detailed discussion of the warranties provided for the system hardware and software components, the maintenance procedures that will be used during the warranty period, and the methods that will be used to secure the full benefits of the warranties.  

3) Operations Support - A detailed discussion of operations support, including a description of procedures for backup operations and backup QA, procedures for maintaining system virus protections, procedures for software update assessments, and other operations support activities that will be provided under the Maintenance Agreement. The section shall describe the planned frequency of each of the operations support activities, a description of how the services will be scheduled and coordinated, and proposed Service Level Agreement (SLA) performance levels.  

4) Preventive Maintenance - A detailed discussion of preventive maintenance, including a description of periodic service requirements (cleaning, calibration, etc.), the time required for each type of service, the planned frequency with which preventive maintenance services will be provided, a description of how the services will be scheduled and coordinated, and proposed Service Level Agreement (SLA) performance levels.
5) Remedial Maintenance - A detailed discussion of remedial maintenance procedures, including the problem response approach and sequence of activities, the methods used to ensure that response times are met and system availability requirements are maintained, a description of repair/replacement procedures and timeframes, a description of procedures for problem tracking, escalation and reporting, and proposed Service Level Agreement (SLA) performance levels.

*Proposers shall include the initial delivery and any subsequent updates of the System Maintenance Plan as deliverable milestones in their proposed Master Implementation Schedule.*

### 8.5 Technical Support for Ongoing Operations and System Expansion

a) The selected Contractor shall provide technical support through the life of the system, at the request of the system manager. This support shall include, but not be limited to, configuration management, periodic testing and training, and system expansion planning and implementation.

b) Not less than semi-annually, Contractor shall coordinate a meeting between Contractor’s Account Manager and MCSO system managers to review the status of the system and discuss operational issues, review the maintenance history and discuss any chronic problems, coordinate upcoming major activities, and discuss new reliability improvements and enhancements.

#### 8.5.1 Configuration Management

a) A procedure for formal configuration management and version control shall be provided to manage the system’s hardware and software configuration. The procedures shall include a notification and approval process whereby MCSO shall receive timely notification of the plans for an upgrade, have the opportunity to witness the regression testing and review test reports, and approve or disapprove the upgrade prior to its implementation in the operational system.

b) The configuration management procedure shall include source control and release management in order to insure that AFIS system downtime is minimized and that updates are applied efficiently and correctly.

c) The Contractor shall provide responsive support to the AFIS Project Management Office to ensure comprehensive Configuration Management is established and maintained through the life of the system.

#### 8.5.2 Test and Training Support

a) Contractor shall provide technical support for annual system testing and training exercises, as follows:

1) Annual performance benchmark test: Contractor shall configure and operate the system to repeat the Accuracy Performance Benchmark Test originally developed and performed as part of final system acceptance testing (ref: §4.6).

2) Annual Disaster Recovery / Business Continuity Training Exercise: Contractor shall support the planning, preparation and conduct of an annual training exercise
to ensure familiarity of all personnel with Disaster Recovery and Business Continuity procedures.

8.5.3 System Expansion

a) Contractor shall provide technical support for planning, implementing and testing customer-directed expansions and extensions of the AFIS, including but not limited to:

1) AFIS expansion and/or reconfiguration to provide increased capacity for tenprint, palmprint, and latent transaction workload handling.

2) AFIS expansion to provide increased record storage capacity.

3) Extension of AFIS Services to other MCSO operational activities and to other agencies in the region, as authorized by the AFIS operations manager.

4) Interconnection, workflow configuration, testing and transition to operations for additional LiveScan workstations, latent input workstations, and multifunction analysis workstations, as authorized by the AFIS operations manager. This requirement includes support for workstations and terminals supplied by the Contractor, and also to approved workstations and terminals provided by 3rd party suppliers and acquired directly by a regional agency.

5) Network expansion planning, specification support, reconfiguration and certification testing as necessary to maintain performance as system workloads increase, and to maintain compliance with FDLE and FBI CJIS Security policies.
APPENDIX 1. GLOSSARY OF TERMS AND ABBREVIATIONS

AES                   Advanced Encryption Standard.
AFIS                  Automated Fingerprint Identification System.
AFIS ID #             A unique Person Number assigned by the AFIS system to every record associated with a specific individual.
ANSI                  American National Standards Institute (a governing body for national Standards.
ANSI/NIST             Refers to national standards (in the context of this specification, fingerprint formatting and communications standards) developed by the National Institute of Standards & Technology and published by the American National Standards Institute.
ANSI/NIST-ITL 1-2000  Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo Information. This standard is equivalent to CJIS-RS-0010 v7.
Barcode Number        The inmate identification number assigned by JAMS; used by LiveScan to import a booking record from JAMS to avoid duplicate data entry into the LiveScan workstation.
FDLE                  Florida Department of Law Enforcement.
FDLE BIS              FDLE Biometric Identification System – the State Automated Fingerprint Identification System.
Candidate List        An ordered list of candidates (“respondents”) to an identification search ordered by match score.
Candidate Print        A file print selected during the matching function.
Candidate Ranking      The relative position of an identification match candidate on a candidate list ordered by match score.
CFE                   County Furnished Equipment and capabilities
Charting              The automated or interactive terminal function that enables corresponding minutia points on search and file images to be associated on a split screen display. The system or an operator draws lines between corresponding minutiae and/or assigns the same numbers to corresponding minutiae points on the search and file prints.
CHRI                  Criminal History Record Information.
Civil                 Synonymous with Applicant fingerprint submissions.
CJIS                  (1) Criminal Justice Information System – A computerized repository of criminal history records.
                        (2) FBI Criminal Justice Information Services Division.
CJIS Network          The State’s secure wide area network (WAN) for transmission of criminal justice information within the State of Florida.
Cold Search           A fingerprint search conducted against all records in the database, with or without search delimiters (aka “Open Search”)
Color Reversal  Reverse Video – The process of converting an image from negative to positive or from positive to negative on a workstation display. Used for clarifying print impressions for minutiae detection and verification.

Contractor  The term “Contractor” as used in this RFP means the organization that is awarded the contract to provide the AFIS and associated services as a result of submitting a proposal in response to this RFP.

COTS  Commercial-Off-The-Shelf. Equipment or software that is in current production manufacture.

DOJ  U. S. Department of Justice

Encoding  The process of detecting and recording minutia relationships and other characteristic features of a fingerprint image for use in automated identification searching.

FALCON  FDLE Criminal Justice Information System.

FBI  Federal Bureau of Investigation.

FDLE  Florida Department of Law Enforcement

FDLE BIS  FDLE Biometric Identification System – the State AFIS

FDLE/RID  FDLE Rapid-ID. A two-finger fingerprint identification search or identity verification match of the FDLE BIS identification database in support of State-mandated sex offender and DNA registration processes.

GJXML  Global Justice Extensible Markup Language Data Model (GJXDM) Version 3.0

GJXDM v3.0  Production version of the Global Justice XML Data Model - a data reference model for the exchange of information within the justice and public safety communities.

Gray Scale Image  A digital representation of a fingerprint image in which the fingerprint image is encoded with numeric quantities representing the relative level or degree of darkness of each pixel in the image. Standard 8-bit encoding will enable the distinction of 256 discrete gray scale levels of image density (darkness) of a fingerprint’s ridge structure.

IAFIS  Integrated Automated Fingerprint Identification System – The FBI’s system for integrating fingerprint comparisons with criminal history record processing located in Clarksburg, West Virginia. This system is utilized for the electronic submission of fingerprint cards to the FBI

Identification (Hit)  The automated computation of a positive identification resulting from a search and match of tenprint or latent prints with fingerprints stored in the AFIS.

III  Interstate Identification Index - An automated indexing system enabling access via the NCIC to state criminal history records for approximately 36 million individuals.

Image Enhancement  The modification of a digital image using automated methods with the objective of improving the quality of that image

Image Processing  In AFIS, a set of tasks that includes the scanning of an image to convert the image to digital (electronic) format, detecting and encoding image features which can be used for classification and identification, and compressing the...
image for the most efficient storage and/or transmission.

**Inquiry**
The process of searching a designated AFIS database with a specified fingerprint, palmprint or latent print.

**IQS**
FBI Image Quality Specifications as specified in Appendix F of the FBI Electronic Biometric Transmission Specification standard. The FBI’s specification of acceptable ranges of various technical parameters of scanning systems used to acquire digital fingerprint images.

**ISO**
International Standards Organization

**JPEG**
(1) Joint Photo Experts Group.
(2) An image data compression standard for continuous tone imagery.

**JPEG 2000**
JPEG 2000 is a wavelet-based image compression standard developed as the next generation of the JPEG standard. In 2000, the core JPEG 2000 algorithm was completed and is defined in the ISO 15444-1 JPEG 2000 standard.

The FBI has developed a new standard for the compression and formatting of 1,000 ppi fingerprint and palm images, called “Profile for 1,000 ppi Fingerprint Compression.” This profile requires the use of JPEG2000 for compression and formatting of 1,000 ppi images. WSQ will continue to be used for 500 ppi images.

**JXDD**

**LAN**
Local Area Network

**LDAP**

**Latent Case Record**
All fingerprints assigned a single Case Number. An electronic record derived from the images and alphanumeric data associated with a specific latent case.

**Latent print**
A fingerprint or palmprint obtained from a crime scene or evidence sample that may be used in an AFIS identification search.

**LEA**
Law Enforcement Agency.

**Item (Lift)**
Transfer tape or a photograph bearing a latent print impression developed from a crime scene.

**Lights Out**
Automatic encoding and match processing of tenprint fingerprints resulting in either a single positive match determination or a positive no-match determination, without manual intervention needed to initiate or perform any intermediate process associated with the identification search and the review of uncertain match results.

**Matching Process**
The automated comparison of a search print with file (database) prints resulting in a list of match candidates ordered by match score.

**MCSO**
Manatee County Sheriff’s Office.

**MDC**
Mobile Data Computer.

**MPLS**
Multi-Protocol Label Switching.

**NCIC**
National Crime Information Center - An automated database of criminal justice and justice-related records maintained by the FBI.

**NFF**
National Fingerprint File – a system and its procedures designed as a...
A component of the III system, which, when fully implemented, will establish a totally decentralized system for the interstate exchange of criminal history records.

**NIBRS**  National Incident-Based Reporting System - a system that permits the collection of multiple data elements per crime rather than just a count of the number of crimes.

**NIEM**  National Information Exchange Model.

**NIST**  National Institute of Standards and Technology (formerly “National Bureau of Standards”) - Founded in 1901, is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration.


**NIST Type 1 Record**  ANSI/NIST-ITL 1-2000 record format specification for transaction header information.

**NIST Type 2 Record**  ANSI/NIST-ITL 1-2000 record format specification for record index and demographic information for both the subject and the submitting agency.

**NIST Type 4 Record**  ANSI/NIST-ITL 1-2000 record format specification for high resolution gray scale images of fingerprints comprising a tenprint record, including up to 10 rolled fingerprint images, two plain-impression thumb print images and two plain-impression sequence print images of the right hand and left hand four fingers taken together ("slap prints").

**NIST Type 10 Record**  ANSI/NIST-ITL 1-2000 record format specification for digital facial image record

**NIST Type 14 Record**  ANSI/NIST-ITL 1-2000 record format specification for variable density fingerprint images, used for formatting and transmission of 1,000 ppi fingerprint images.

**NIST Type 15 Record**  ANSI/NIST-ITL 1-2000 record format specification for variable density palmprint images, used for formatting and transmission of 500 and 1,000 ppi palmprint images.

**NLETS**  National Law Enforcement Telecommunications System - a WAN provider for secure transmission of criminal history inquiries and criminal history records information.

**No-Hit Threshold**  A computed match score below which a candidate is considered not to match a submitted search print.

**Pattern Type**  Classification given to a fingerprint denoting the primary topological characteristics of its ridge structure (loop, whorl, arch, etc.).

**Offeror**  A qualified AFIS manufacturer who submits a formal proposal in response to the solicitation for an AFIS to replace the existing MCSO AFIS system.

**ORI**  Originating Agency Identifier

**OSE**  Open Systems Environment

**PDA**  Personal Digital Assistant (hand-held terminal, e.g., Palm Pilot or Blackberry)
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>POC</td>
<td>Point of Contact</td>
</tr>
<tr>
<td>PPI</td>
<td>Pixels per Inch</td>
</tr>
<tr>
<td>PP:ULF</td>
<td>Palmprint 1:N search of the Unsolved Latent File (ULF).</td>
</tr>
<tr>
<td>Procurement Process</td>
<td>The process of issuing an RFP, evaluating proposals submitted pursuant to the RFP, selection of a Contractor, and awarding a contract to the selected Contractor to supply the required products and services.</td>
</tr>
<tr>
<td>Proposal</td>
<td>A formal response to an RFP which offers to supply the specific products and services according to prescribed specifications, terms and conditions.</td>
</tr>
<tr>
<td>Purged (record or data)</td>
<td>Any record consisting of image, demographic or other personal identifying information that is deleted from the AFIS. Depending on statutory requirements, purged records may be saved for future reference in substantially the same or an altered state to ensure privacy.</td>
</tr>
<tr>
<td>Queue</td>
<td>Input and output items being stored temporarily in the system until processing can occur.</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Inexpensive Disks</td>
</tr>
<tr>
<td>Remote Terminal Location</td>
<td>An approved MCSO activity or external law enforcement agency that acquires its own fully- compatible AFIS equipment (e.g., LiveScan) that is directly interconnected to the central site AFIS computer.</td>
</tr>
<tr>
<td>Resulting Contract</td>
<td>The resulting contract is the contract awarded under this RFP that is signed with the Contractor.</td>
</tr>
<tr>
<td>RFP</td>
<td>Request For Proposal – A formal solicitation of proposals to satisfy requirements by supplying products and/or services according to specific specifications, terms and conditions.</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network – Equipment used to provide shared disk storage and services to agency applications.</td>
</tr>
<tr>
<td>SAT</td>
<td>System Acceptance Test</td>
</tr>
<tr>
<td>SDD</td>
<td>System Design Document</td>
</tr>
<tr>
<td>SMT</td>
<td>Scars, Marks, and Tattoos – NIST-standard descriptor codes and, optionally, digital images of unique features of an individual’s scars, marks and tattoos will be maintained in the AFIS for use in identification.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSN</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>SSRS</td>
<td>MCSO SQL Reporting System</td>
</tr>
<tr>
<td>System Restoration</td>
<td>The ability to completely restore the system hardware and software to operational status following a failure or damage.</td>
</tr>
<tr>
<td>System Warranty Period</td>
<td>That period during which the system provider will provide hardware &amp; software product support and/or maintenance at no additional charge. Any system warranty shall cover products of &quot;third party&quot; origin to the same extent as the warranty may apply to products manufactured by the primary system provider.</td>
</tr>
<tr>
<td>TCN</td>
<td>Transaction Control Number</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Terminal Control Protocol / Internet Protocol</td>
</tr>
<tr>
<td>Tenprint</td>
<td>A term that refers to an FBI-standard fingerprint card or the equivalent electronic record, with up to ten rolled fingerprints; also refers to a search of the database of tenprint data in AFIS.</td>
</tr>
<tr>
<td>TOT</td>
<td>Type of Transaction. The transaction type data element defined in the ANSI/NIST-ITL 1-2000 Type 1 record format specification.</td>
</tr>
<tr>
<td>TP:TP</td>
<td>Tenprint 1:N search of the on-line tenprint identification database.</td>
</tr>
<tr>
<td>TP:TPV</td>
<td>Tenprint 1:1 Identity Verification match of a search record with a corresponding record in the tenprint identification database.</td>
</tr>
<tr>
<td>TP:ULF</td>
<td>Tenprint 1:N search of the Unsolved Latent File (ULF).</td>
</tr>
<tr>
<td>Transcoding</td>
<td>Conversion of a 1,000ppi fingerprint image to a 500ppi image for submission to an external system that is incapable of accepting or processing 1,000ppi images.</td>
</tr>
<tr>
<td>UL</td>
<td>Underwriter’s Laboratory</td>
</tr>
<tr>
<td>ULW</td>
<td>Universal Latent Workstation - a software application program developed and distributed by the FBI.</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network - a way of connecting computer sites at distances greater than line-of-sight.</td>
</tr>
<tr>
<td>Workstation</td>
<td>A general-purpose computer system configured with special-purpose applications software and peripheral devices, which is used to perform a specific data input or analysis function associated with AFIS identification processing.</td>
</tr>
<tr>
<td>WSQ</td>
<td>Wavelet Scalar Quantization (WSQ) is the FBI-specified fingerprint compression standard used nationally and internationally. The WSQ standard, IAFIS-IC-0110 (v3) Wavelet Scalar Quantization, specifies how to represent biometric image data in a compressed image format. Additionally, ANSI/NIST ITL 1-2000 and CJIS-RS-0010(v7) (EFTS) specify or assume compliance with the WSQ. The WSQ compression algorithm is designed specifically for fingerprint images with a scanning resolution of 500 ppi.</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
APPENDIX 2.  NIST Type-1 Record Transaction Types

2.1  **Tenprint Identification Transactions**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOT</td>
<td>Tenprint Identification Request Transaction</td>
</tr>
<tr>
<td>CAR</td>
<td>Criminal Ten-Print Submission (Answer Required)</td>
</tr>
<tr>
<td>CAN</td>
<td>Criminal Ten-Print Submission (No Answer Necessary)</td>
</tr>
<tr>
<td>FANC</td>
<td>Federal Applicant (No Charge)</td>
</tr>
<tr>
<td>FAUF</td>
<td>Federal Applicant User Fee</td>
</tr>
<tr>
<td>NFUF</td>
<td>Non-Federal Applicant User Fee</td>
</tr>
<tr>
<td>MAP</td>
<td>Miscellaneous Applicant Civil</td>
</tr>
<tr>
<td>DEK</td>
<td>Known Deceased</td>
</tr>
<tr>
<td>DEU</td>
<td>Unknown Deceased</td>
</tr>
<tr>
<td>MPR</td>
<td>Missing Person</td>
</tr>
<tr>
<td>AMN</td>
<td>Amnesia Victim</td>
</tr>
<tr>
<td>TOT</td>
<td>Tenprint Identification Response Transaction</td>
</tr>
<tr>
<td>SRE</td>
<td>Submission Results – Electronic</td>
</tr>
<tr>
<td>ERRT</td>
<td>Ten-Print Transaction Error</td>
</tr>
</tbody>
</table>

2.2  **Latent Identification Transactions**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOT</td>
<td>Latent Identification Request Transaction</td>
</tr>
<tr>
<td>LFS</td>
<td>Latent Fingerprint Image(s) Submission</td>
</tr>
<tr>
<td>CFS</td>
<td>Comparison Fingerprint Image(s) Submission</td>
</tr>
<tr>
<td>MCS</td>
<td>Major Case Image(s) Submission</td>
</tr>
<tr>
<td>ELR</td>
<td>Evaluation Latent Fingerprint Submission Request</td>
</tr>
<tr>
<td>TOT</td>
<td>Latent Identification Response Transaction</td>
</tr>
<tr>
<td>LSR</td>
<td>Latent Submission Results</td>
</tr>
<tr>
<td>NAR</td>
<td>Notification of Action Response</td>
</tr>
<tr>
<td>ERRT</td>
<td>Latent Transaction Error</td>
</tr>
</tbody>
</table>
### 2.3 Remote Latent Search Transactions

<table>
<thead>
<tr>
<th>TOT</th>
<th>Remote Latent Search Request Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>LFIS</td>
<td>Latent Fingerprint Image(s) Searches</td>
</tr>
<tr>
<td>LFFS</td>
<td>Latent Fingerprint Features Searches</td>
</tr>
<tr>
<td>LPNQ</td>
<td>Latent Penetration Query</td>
</tr>
<tr>
<td>TOT</td>
<td>Remote Latent Search Response Transaction</td>
</tr>
<tr>
<td>SRL</td>
<td>Search Result – Latent</td>
</tr>
<tr>
<td>LPNR</td>
<td>Latent Penetration Response</td>
</tr>
<tr>
<td>ULM</td>
<td>Unsolved Latent Match Response</td>
</tr>
<tr>
<td>ERRL</td>
<td>Latent Transaction Error</td>
</tr>
</tbody>
</table>

### 2.4 Unsolved Latent Maintenance Transactions

<table>
<thead>
<tr>
<th>TOT</th>
<th>Unsolved Latent Maintenance Request Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>ULD</td>
<td>Unsolved Latent Record Delete Request</td>
</tr>
<tr>
<td>ULAC</td>
<td>Unsolved Latent Add Confirm Request</td>
</tr>
<tr>
<td>TOT</td>
<td>Unsolved Latent Maintenance Response Transaction</td>
</tr>
<tr>
<td>ULAR</td>
<td>Unsolved Latent Add Confirm Response</td>
</tr>
<tr>
<td>ULD</td>
<td>Unsolved Latent Delete Response</td>
</tr>
<tr>
<td>UULD</td>
<td>Unsolicited Unsolved Latent Delete</td>
</tr>
<tr>
<td>ERRL</td>
<td>Latent Transaction Error</td>
</tr>
</tbody>
</table>

### 2.5 Remote Fingerprint Image Request Transactions

<table>
<thead>
<tr>
<th>TOT</th>
<th>Remote Fingerprint Image Request Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRQ</td>
<td>Fingerprint Image Request</td>
</tr>
<tr>
<td>TOT</td>
<td>Remote Fingerprint Image Response Transaction</td>
</tr>
<tr>
<td>IRR</td>
<td>Fingerprint Image Request Response</td>
</tr>
<tr>
<td>ISR</td>
<td>Fingerprint Image Response Summary</td>
</tr>
<tr>
<td>ERRI</td>
<td>Image Transaction Error</td>
</tr>
</tbody>
</table>
## 2.6 Fingerprint Image Submission Transactions

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOT</td>
<td>Fingerprint Image Submission Transaction</td>
</tr>
<tr>
<td>FIS</td>
<td>Fingerprint Image Submission</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOT</td>
<td>Fingerprint Image Submission Response Transaction</td>
</tr>
<tr>
<td>FISR</td>
<td>Fingerprint Image Submission Response</td>
</tr>
<tr>
<td>ERRI</td>
<td>Image Transaction Error</td>
</tr>
</tbody>
</table>

## 2.7 Latent Administrative Query Transactions

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOT</td>
<td>Latent Administrative Query Transaction</td>
</tr>
<tr>
<td>LRSQ</td>
<td>Latent Repository Statistics Query</td>
</tr>
<tr>
<td>LSMQ</td>
<td>Latent Search Status and Modification Query</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOT</td>
<td>Latent Administrative Query Response Transaction</td>
</tr>
<tr>
<td>LRSR</td>
<td>Latent Repository Statistics Response</td>
</tr>
<tr>
<td>LSMR</td>
<td>Latent Search Status and Modification Response</td>
</tr>
<tr>
<td>ERRA</td>
<td>Administrative Error Response</td>
</tr>
</tbody>
</table>
THIS PAGE INTENTIONALLY LEFT BLANK