STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **11**
to
Contract Number **MA071B7700122C**

CONTRACTOR	
	Idemia Identity & Security USA LLC
	5515 East La Palma Avenue Suite 100
	Anaheim CA 92807
	Majid Assemi
	714-238-2011
	Majid.Assemi@idemia.com
	CV0000922

STATE			
	Program Manager	Various	Various
	Contract Administrator	Nichole Harrell	DTMB
		517-449-9245	
		harrelln@michigan.gov	

CONTRACT SUMMARY			
Automated Biometric Identification System (ABIS)			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
June 14, 2017	June 13, 2022	2 - 60 Months	June 13, 2027
PAYMENT TERMS		DELIVERY TIMEFRAME	
ALTERNATE PAYMENT OPTIONS		EXTENDED PURCHASING	
☐ P-Card ☐ Direct Voucher (PRC) ☐ Other		☐ Yes ☒ No	
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐	60 Months	☐		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
$15,669,846.00	$155,165.00	$15,825,011.00		

DESCRIPTION
Effective June 6, 2024, the following changes are hereby incorporated into this Contract: 1. This Contract is hereby increased by $155,165.00 for Michigan State Police (MSP) to provide (4) additional years of hardware and software maintenance on the Jacket Scan BatchScan stations used for the Jacket Scan Project. This funding will be allocated as follows: 2025: $36,000.00 2026: $37,800.00 2027: $39,690.00 2028: $41,675.00 2. The Contract Administrator is updated from Jarrod Barron to Nichole Harrell (Harrelln@michigan.gov, 517-449-9245). All other terms, conditions, specifications and pricing remain the same. Per Contractor, agency, and DTMB Central Procurement Services approval. Internal Note: Ad Board balance after this change notice: $94,834.99

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov
MSP	Michael Ransom	517-420-7156	RansomM@michigan.gov

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **10**

to

Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Majid Assemi
	714-238-2011
	majid.assemi@idemia.com
	CV0000922

STATE			
Program Manager	Various	MSP
Contract Administrator	Jarrod Barron	DTMB
	(517) 249-0406	
	barronj1@michigan.gov	

CONTRACT SUMMARY						
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)						
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE			
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2027			
PAYMENT TERMS		DELIVERY TIMEFRAME				
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING			
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No		
MINIMUM DELIVERY REQUIREMENTS						

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		June 13, 2027
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
$14,728,113.00	$941,733.00	$15,669,846.00		

DESCRIPTION

Effective 5/23/2023, the parties add $941,733.00 for the Jacket Scan Project services detailed in the attached statement of work. . All other terms, conditions, specifications and pricing remain the same. Per contractor, agency, DTMB Procurement and State Administrative Board approval on 5/23/2023.

Internal Note: Ad Board balance after this change notice: $249,999.99.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
MSP	Michael Ransom	517-420-7156	ransomm@michigan.gov
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov

MICHIGAN DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK

Project Title: Jacket Scan Project	Period of Coverage:
Requesting Department: Michigan State Police	Date: 4/28/2023
Agency Project Manager: Jaala McClain	Phone: 517-899-2099
DTMB Project Manager:	Phone:

This statement of work is subject to the existing terms and conditions of Contract 071B7700122.

BACKGROUND:
There are currently approximately two million fingerprint jacket files remaining at Michigan State Police (MSP) headquarters housed within the Criminal Justice Information Center (CJIC). This involves no backup capability as these are the only copies of the approximately four million valid arrests within the files. If the files are digitized and placed within the Michigan Automated Fingerprint Identification System (AFIS) Archive hosted within a cloud environment the security of the files becomes more reliable. The usability, accessibility, convenience, and efficiency of the files being stored within AFIS Archive all improve vastly. In moving toward with this digized solution it allows for further improvement of our data security which supports the goals of our agency.

PROJECT OBJECTIVE:
The objective for this project is to digitize all remaining fingerprint files to Michigan AFIS Archive.

SCOPE OF WORK:

- Create a shared folder for the BatchScan output to support one or more of the BatchScan Workstations.
  - Configure BatchScan card formats based on MSP requirements.
  - Configure the BatchScan application to read the barcode on the scanned card.
  - Configure the BatchScan application to read the front and back of each card.
  - Put the card images in the BatchScan Output folder using the TCN as the folder name.
- Create a script that will read the contents of the BatchScan output folder.
  - Create Jar, XML and Trigger files for the images in the output folder using the image folder name as the TCN.
  - Submit the files to the PtkOSM folder for DSM pickup and call the MBIS BatchScan workflow to process card scan images.
- Create a DES to format the NIST file putting the TCN in the Type-2 record.
  - Convert the front and back of the card images into 300 DPI format.
  - Create a PDF of the card images.
  - Store the images in the NIST Type 7 record.
- Create a BatchScan workflow to:
  - Insert the NIST file into the MAS.
  - Note that the BatchScan workflow will not send the card images to the FES for coding, nor to the MBSS for searching.

TASKS:
Technical support is required to assist with the following tasks:

Task 1 – Project Planning
Each Task to be performed by both the contractor and the MSP staff during project implementation and until final acceptance must be specifically addressed in the project plan. The project plan must include the general order in which the tasks and subtasks will be performed (some tasks may be conducted in parallel) and the order in which the deliverables will be produced.

Task 2 – Procurement
Upon delivery of the purchase order to other contractual commitment number from the state, the contractor shall start the procurement and installation of all configurations to the AFIS system.

Task 3 – Configuration
The contractor will setup and configure the Jacket project solution. This includes installation of software, network setup, updating all configurations, and fully implementing the workflow and batchscanners within the AFIS system. The contractor will assist in answering questions about the jacket project configuration and security controls, provide evidence (diagrams/screenshots) to show how security controls are implemented, approve the Plan of Action and Milestones (POAM), execute the POAM(s), and provide evidence that security vulnerabilities have been remediated.

Task 4 – Idemia application integration
Upon completion of Task 3 the Michigan AFIS will be reconfigured to utilize the batch scanners and workflow changes to scan fingerprint files directly to AFIS Archive. This process will be completed during a scheduled outage as the process interrupts normal operation of the system.

Task 5 – Testing
The contractor will conduct:
- Functional testing to ensure that the AFIS jacket scanning solution works satisfactorily.
- Volume/stress testing to ensure that the new solution works satisfactorily during high volumes of livescan transaction uploading, searching, and storing.
- Testing will ensure all functionality is to standard and all data is accessible by the MSP, Automated Print Identification Section.

DELIVERABLES:
Deliverables will not be considered complete until the Agency Project Manager has formally accepted them. Deliverables for this project include:
- Installation and configuration of the jacket scan project solution.
- Completed Functional testing.
- Completed Volume/stress testing.
- Completed interface testing.

ACCEPTANCE CRITERIA:
Acceptance criteria for the deliverables include:
- Demonstration of fingerpint file insertion and operation, including operation under high volumes/stress.
- Ensure all AFIS interface capabilities are functioning while inserting fingerprint files into AFIS Archive.

PROJECT CONTROL AND REPORTS:
A bi-weekly progress report must be submitted to the Agency and DTMB Project Managers throughout the life of this project. This report may be submitted with the billing invoice. Each bi-weekly progress report must contain the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates.
- Accomplishments during the reporting period, what was worked on and what was completed during the current reporting period.
- Tasks planned for the next reporting period.
- Identify any existing issues which are impacting the project and the steps being taken to address those issues.
- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified.

SPECIFIC DEPARTMENT STANDARDS:
Agency standards, if any, in addition to DTMB standards.

PAYMENT SCHEDULE:
Contractor may invoice the State $235,433.25 upon receiving the purchase order, $470,866.50 after delivering batch scanner devices, and $235,433.25 after the State formally accepts all deliverables detailed herein. Total statement of work costs are detailed below:

Qty.	Description	Price
4	MBIS BatchScan Workstation including: • PC • 24” Monitor • Fujitsu fi-7600 card scanner • MBIS BatchScan Software Application	$239,980
1	Additional MAS storage to support up to 4 million fingerprint card images in the MBIS Archive system and workflow changes	$509,963
	IDEMIA I&S Professional Services, including: • Program Management • Installation and Test • User Documentation • Logistical Services (Shipping, Delivery)	$155,790
4	1 Year Maintenance Price (per year)	$36,000
	Total Price:	**$941,733**

EXPENSES:
The State will NOT pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:
The designated Agency Program Manager is:

Jaala McClain
Michigan State Police
Biometrics and Identification Division
MSPHQ – Third Floor, A-Wing
7150 Harris Drive
Dimondale, Michigan 48821
571-899-2099
Mcclainj5@michigan.gov

The designated DTMB Program Manager is:

TBD

AGENCY RESPONSIBILITIES:
Provide the physical and logical assets as needed to a working environment.

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:

Contractor staff will work at Idemia, Anaheim, CA and onsite at MSP Headquarters, Dimondale, MI.

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:
Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing. No overtime will be permitted.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
320 S. WALNUT ST., LANSING, MICHIGAN 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **9**
to
Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Majid Assemi
	714-238-2011
	majid.assemi@idemia.com
	CV0000922

STATE			
Program Manager	Various	MSP
Contract Administrator	Jarrod Barron	DTMB
	(517) 249-0406	
	barronj1@michigan.gov	

CONTRACT SUMMARY			
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2027
PAYMENT TERMS		DELIVERY TIMEFRAME	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
☐ P-Card ☐ PRC ☐ Other			☐ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		June 13, 2027
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
$14,585,513.00	$142,600.00	$14,728,113.00		

DESCRIPTION

Effective 6/21/2022, the parties add $142,600.00 for the Web Services updates detailed in the attached statement of work. The MSP Program Manager is also changed from Scott Blanchard to Michael Ransom. All other terms, conditions, specifications and pricing remain the same. Per contractor, agency, and DTMB Central Procurement approval.

Internal Note: Ad Board balance after this change notice: $107,399.99.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
MSP	Michael Ransom	517-420-7156	ransomm@michigan.gov
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov

MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK

Project Title: Web Services	Period of Coverage:
Requesting Department: Michigan State Police	**Date:** 6/18/2022
Agency Project Manager: Michael Ransom	**Phone:** 517-420-7156
DTMB Project Manager:	**Phone:**

BACKGROUND:

Livescans currently transmit transactions from the field using an SFTP protocol. This has been determined very difficult to maintain updates to ensure proper securtiy protocols. It was determined the changing to a different protocol would not only ensure the latest security rules are followed, but switching to a web service protocol would line up better with what DTMB is doing with a lot of its other systems.

PROJECT OBJECTIVE:

The objective or goal for this project is to move from an SFTP protocol to a Web Services solution.

SCOPE OF WORK:

The Mobile ID move to the cloud will be in conjunction with the Digital Crime Scene move and will use the same scope of work. These tasks, subtasks, and deliverables in this Statement of Work (SOW) outline the scope of the contractor's work in completing the project objective. To achieve this, the contractor/vendor shall provide the following required Services:

- **Project Planning** – Develop a project plan. This includes but is not limited to the following:
  - Planning for project
  - Documentation (as requested)
  - Testing Cases
  - User Training (if necessary)
  - Validation (session and documentation)

- **Project Management** - Throughout the Terms of Agreement, under the direction of the MSP, the vendor shall apply requisite technical and management skills and techniques to assure satisfactory, timely completion of project tasks and deliverables. Progress regarding the status of the tasks and deliverables detailed in the project plan shall be reported to MSP. The MSP who will approve the deliverables prior to vendor receiving payment.

TASKS:

Unless specified otherwise, all tasks and subtasks described in this Statement of Work (SOW) shall be performed by the contractor. The contractor shall conduct all meetings, presentations, demonstrations remotely. The contractor/vendor shall prepare and deliver all deliverables described in this SOW, using the deliverable numbers and titles indicated. The process for receiving, reviewing, and accepting the deliverables is provided in the acceptance criteria section of this SOW. The timeline for this project varies vastly and will likely flow into the 2023 calendar year.

Task 1 – Procurement

Upon delivery of the purchase order to other contractual commitment number from the state, the contractor/vendor shall start the development

Task 2 – Development

The contractor shall develop software for the AFIS system to accept the new Web Services while also maintaining the ability to accept transactions in the SFTP format for a period of time so all livescan submitting vendors will be able to change their software to submit under the new protocol

Task 3 – Software integration

The contractor will integrate software to enable transactions to be passed to and from the AFIS from the livescan systems at the various fingerprinting locations. They will communicate the different interface and/or network configurations needed for the Michigan approved livescan vendors to be able to interface with them. Communication from Michigan AFIS to and from FBI will not need to be changed and will function as it currently does.

Task 4 – Testing

The contractor/vendor shall conduct:

A) Functional testing to ensure that the AWS cloud storage solution works satisfactorily.

B) Volume/stress testing to ensure that the new solution works satisfactorily during high volumes of search or image uploading.

C) Assist with testing of the Michigan approved livescan vendors when they are ready to cut over to the new protocol.

Task 5 – Acceptance

The contractor/vendor Project Manager shall work with MSP to determine completion of tasks, subtasks, and deliverables covered in the SOW and project plan for acceptance. Given the current work environment, an email will suffice for formal acceptance.

DELIVERABLES:

Deliverables will not be considered complete until the agency (MSP) project manager has formally accepted them. Deliverables for this project include:

- Installation and configuration of the new web services protocol
- Completed Functional testing.
- Completed Volume/stress testing.
- Completed of parallel testing or SFTP and Web Services.

ACCEPTANCE CRITERIA:

Acceptance criteria for the deliverables include:

- Demonstration of livescan transaction and messages submissions both to AFIS from livescan and to livescan from AFIS.

PROJECT CONTROL AND REPORTS:
A monthly progress report shall be submitted to the MSP project managers throughout the life of this project. This report may be submitted with the billing invoice. Each bi-weekly progress report must contain accomplishments and issues/risks which indicate what was worked on and what was completed during the current reporting period and any issues or risks identified.

SPECIFIC DEPARTMENT STANDARDS:
Vendor must adhere to all agency standards, if any, in addition to DTMB standards.

PAYMENT SCHEDULE:
State will make payment to Contractor in the amount $142,600.00 after Satisfactory Final Acceptance of all deliverables stated herein. DTMB will pay the contractor upon receipt of properly completed invoice(s), which shall be submitted to the billing address on the state issued purchase order not more often than monthly. DTMB accounts payable area will coordinate obtaining agency and DTMB project manager approvals. All invoices should reflect actual work completed by payment date and must be approved by the agency prior to payment. The invoices shall describe and document to the state's satisfaction a description of the work performed, the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense. Payment shall be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

EXPENSES:
The state will not pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:
The designated Contractor (vendor) Project Manager is:

Majid Assemi
Idemia
5515 East LaPalma Ave., Suite 100
Anaheim, CA 92807

The designated Agency Program Manager is:

Michael Ransom
Michigan State Police
Biometrics & Identification Division – Digital Analysis and Identification Section
MSPHQ – Third Floor, A-Wing
7150 Harris Dr
Dimondale, MI 48821
517-420-7156
ransomm@michigan.gov

AGENCY RESPONSIBILITIES:
Provide the physical and logical assets as needed to a working environment.

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:
Contractor staff will work remote from California. If a need shall arise for any in person installation or assistance a contractor staff member will be available.

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:
Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **8**
to
Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Majid Assemi
	714-238-2011
	majid.assemi@idemia.com
	CV0000922

STATE			
Program Manager	Various	MSP
Contract Administrator	Jarrod Barron	DTMB
	(517) 249-0406	
	barronj1@michigan.gov	

CONTRACT SUMMARY			
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-Card	☐ PRC	☐ Other	☐ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
☒	5 Years	☐		June 13, 2027
CURRENT VALUE	**VALUE OF CHANGE NOTICE**	**ESTIMATED AGGREGATE CONTRACT VALUE**		
$8,647,221.00	$5,938,292.00	$14,585,513.00		

DESCRIPTION

Effective 5/24/2022, the parties exercise an option to renew the contract through 6/13/2027 and add $5,938,292.00 to cover ongoing costs. All other terms, conditions, specifications and pricing remain the same. Per contractor, agency, DTMB Procurement and State Administrative Board approval on 5/24/2022.

Internal Note: Ad Board balance after this change notice: $249,999.99.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
MSP	Scott L. Blanchard	517-243-1517	BlanchardS1@michigan.gov
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov

June 14, 2022 - June 13, 2027

Options

Year	Date of Service	Description	Cloud Service (Monthly)	Total Monthly Payment (Imp + Cloud)	Annual Total
Year 6			$90,284		
MQ yearly					
	7/1/2022	MBIS		$90,284	
	8/1/2022	MBIS		$90,284	
	9/1/2022	MBIS		$90,284	
	10/1/2022	MBIS		$90,284	
	11/1/2022	MBIS		$90,284	
	12/1/2022	MBIS		$90,284	
	1/1/2023	MBIS		$90,284	
	2/1/2023	MBIS		$90,284	
	3/1/2023	MBIS		$90,284	
	4/1/2023	MBIS		$90,284	
	5/1/2023	MBIS		$90,284	
	6/1/2023	MBIS		$90,284	
		MQ SW License		$20,702	
	Maintenance for 2 additional workstations			$11,087	
Maintenance for 2 more laptops and 5 large monitors 2021 purchase				$6,128	**$1,121,325**
Year 7			$92,584		
MQ yearly					
	7/1/2023			$92,584	
	8/1/2023			$92,584	
	9/1/2023			$92,584	
	10/1/2023			$92,584	
	11/1/2023			$92,584	
	12/1/2023			$92,584	
	1/1/2024			$92,584	
	2/1/2024			$92,584	
	3/1/2024			$92,584	
	4/1/2024			$92,584	
	5/1/2024			$92,584	
	6/1/2024			$92,584	
		MQ		$20,702	
		BatchScan Maintenace		$9,534	
	Maintenance for 2 additional workstations			$12,415	
Maintenance for 2 more laptops and 5 large monitors 2021 purchase				$6,434	**$1,160,093**

Year 8			$94,941		
MQ yearly					
	7/1/2024			$94,941	
	8/1/2024			$94,941	
	9/1/2024			$94,941	
	10/1/2024			$94,941	
	11/1/2024			$94,941	
	12/1/2024			$94,941	
	1/1/2025			$94,941	
	2/1/2025			$94,941	
	3/1/2025			$94,941	
	4/1/2025			$94,941	
	5/1/2025			$94,941	
	6/1/2025			$94,941	
		MQ		$20,702	
		BatchScan Maintenance		$10,011	
	Maintenance for 2 additional workstations			$12,788	
Maintenance for 2 more laptops and 5 large monitors 2021 purchase				$6,756	**$1,189,549**

Year 9			$97,357		
MQ yearly					
	7/1/2025			$97,357	
	8/1/2025			$97,357	
	9/1/2025			$97,357	
	10/1/2025			$97,357	
	11/1/2025			$97,357	
	12/1/2025			$97,357	
	1/1/2026			$97,357	
	2/1/2026			$97,357	
	3/1/2026			$97,357	
	4/1/2026			$97,357	
	5/1/2026			$97,357	
	6/1/2026			$97,357	
		MQ		$20,702	
	Maintenance for 2 additional workstations			$14,309	
		BatchScan Maintenance		$10,512	
Maintenance for 2 more laptops and 5 large monitors 2021 purchase				$7,094	**$1,220,901**

Year 10			$99,833		
MQ yearly					
	7/1/2026			$99,833	

	8/1/2026			$99,833	
	9/1/2026			$99,833	
	10/1/2026			$99,833	
	11/1/2026			$99,833	
	12/1/2026			$99,833	
	1/1/2027			$99,833	
	2/1/2027			$99,833	
	3/1/2027			$99,833	
	4/1/2027			$99,833	
	5/1/2027			$99,833	
	6/1/2027			$99,833	
		MQ		$20,702	
	Maintenance for 2 additional workstations			$9,238	
		BatchScan Maintenance		$11,038	
Maintenance for 2 more laptops and 5 large monitors 2021 purchase				$7,450	**$1,246,424**

TOTAL **$5,938,292**

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **7**
to
Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Majid Assemi
	714-238-2011
	majid.assemi@idemia.com
	CV0000922

STATE			
Program Manager	Various	MSP
Contract Administrator	Jarrod Barron	DTMB
	(517) 249-0406	
	barronj1@michigan.gov	

CONTRACT SUMMARY			
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022

PAYMENT TERMS	**DELIVERY TIMEFRAME**

ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**	
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
☐		☐		June 13, 2022

CURRENT VALUE	**VALUE OF CHANGE NOTICE**	**ESTIMATED AGGREGATE CONTRACT VALUE**
$8,455,541.00	$191,680.00	$8,647,221.00

DESCRIPTION

Effective 3/15/2021, the parties add $191,680.00 for the MBIS BatchScan Workstation implementation and maintenance services detailed in the attached statement of work. All other terms, conditions, specifications and pricing remain the same. Per contractor, agency, DTMB Procurement and State Administrative Board approval on 3/15/2022.

Internal Note: Ad Board balance after this change notice: $249,999.99.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
MSP	Scott L. Blanchard	517-243-1517	BlanchardS1@michigan.gov
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov

MICHIGAN DEPARTMENT OF TECHNOLOGY,
MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK

Project Title: **AFIS MBIS BatchScan**	**Period of Coverage:**
Requesting Department: **Michigan State Police**	**Date:** **1/31/2022**
Agency Project Manager: **Scott Blanchard**	**Phone:** **517-243-1517**
DTMB Project Manager:	**Phone:**

BACKGROUND:
The Michigan State Police (MSP) has been working to get all fingerprint submissions switched to Livescan which extremely reduced the volume of mailed cards and the need for scanning cards at the MSP. In 2021, the Conviction Set Aside law changed which resulted in more than trippling the number of cards received. The MSP's Automated Fingerprint Identification System (AFIS) contractor, Idemia Identity & Security USA LLC (Contractor) has a new BatchScan, fingerprint card scanner, that will make this process more efficient and faster for our fingerprint technicians.

PROJECT OBJECTIVE:
Purchase the BatchScan and modify the AFIS workflow to accept this process.

SCOPE OF WORK:
Idemia is to provide a BatchScan scanner, software, and workflow changes to AFIS. This scanner will scan a barcode that contains the Transaction Control Number (TCN), which will link to the data file provided by the Criminal History System for each card and will scan the fingerprints at the same time. The flow will then merge the data with the fingerprints and presenting this record to the fingerprint technicians for review and possible modifications to standard image preparation for AFIS and data modifications. The reviewed transaction will then be submitted into AFIS to the standard AFIS flow. To achieve this, the Contractor will provide the following required services:

- Provide BatchScan scanner and user's manual
- Scanner software
- AFIS modified software to allow the scanner to connect, process, and define
- Provide an updated Requirements Definition Document
- Update the Ten-print User's manual to include this process
- Project plan
- Delivery schedule to include
    - Date to install on the Test AFIS
    - Date to install on the Production and DR AFIS
    - User training (if necessary)
    - Validation (session and documentation)

- **Project Management** - Under the direction of the Agency Project Manager, the Contractor will apply requisite technical and management skills and techniques to assure satisfactory, timely completion of project tasks, and deliverables. Progress regarding the status of the tasks and deliverables detailed in the project plan will be reported to the Agency Project

Manager. The Agency Project Manager will approve the deliverables prior to the Contractor receiving payment.

TASKS:
Unless specified otherwise, all tasks and subtasks described in this Statement of Work (SOW) will be performed by the Contractor. The Contractor will conduct all meetings, presentations, and demonstrations remotely, unless otherwise specified by the Contractor's, Agency Project Manager. The Contractor will prepare and deliver all deliverables described in this SOW, using the deliverable numbers and titles indicated. The process for receiving, reviewing, and accepting the deliverables is provided in the acceptance criteria section of this SOW. The MSP expect this to be completed in 2022.

Task 1 – Project Planning
Each task to be performed by both the Contractor and the MSP staff during project implementation and until final acceptance will be specifically addressed in the project plan. The project plan will include the general order in which the tasks and subtasks will be performed (some tasks may be conducted in parallel) and the order in which the deliverables will be produced.

Task 2 – Procurement
Upon delivery of the purchase order the Contractor will initiate programming changes needed for the Michigan AFIS (production, Disaster Recovery (DR) and Test systems) and procure scanner hardware and software.

Task 3 – Implementation
The Contractor will:
1. Deliver and install the scanner hardware and software
2. Implement software on the Test AFIS
3. Provide training
4. Allow adequate time for testing on the Test AFIS as agreed to by the MSP
5. Implement software on the production and DR systems when approved by the MSP
6. Allow adequate testing as agreed to by the MSP

Task 4 – Acceptance

The Contractor Project Manager will work with the Agency Project Manager to determine completion of tasks, subtasks, and deliverables covered in the SOW and project plan for acceptance. Given the current work environment, an email will suffice for formal acceptance.

DELIVERABLES:
Deliverables will not be considered complete until the Agency Project/Program Manager has formally accepted them. Deliverables for this project include:
1. Deliver and install BatchScan scanner and software.
2. Updated AFIS workflow software.
3. Updated documentation to include these changes.
4. Apply these changes to the Test, Production, and Disaster Recovery AFIS.

ACCEPTANCE CRITERIA:
Acceptance criteria for the deliverables include:

Verified workflow was properly modified to accept cards scanned with the BatchScan system. TCN barcode and fingerprint scanned simultaneously, data merge form criminal history file, and fingerprint technician image and data review and allowing updates.

1. Verified modifications to the workflow as defined above.
2. Reviewed and accepted results.
3. Reviewed and accepted reports.
4. Updated documentation to include these changes in the administrative and design manual.

5. Assure searches, flow, and registrations are completed as required.

PROJECT CONTROL AND REPORTS:
A bi-weekly progress report must be submitted to the Agency Project Manager throughout the life of this project. This report may be submitted with the billing invoice. Each bi-weekly progress report must contain the following:

1. **Hours**: Indicate the number of hours expended during the past two weeks, and the cumulative total to date for the project. Also state whether the remaining hours are sufficient to complete the project.
2. **Accomplishments**: Indicate what was worked on and what was completed during the current reporting period.

SPECIFIC DEPARTMENT STANDARDS:
Contractor must adhere to all agency standards, if any, in addition to Department of Technology, Management, and Budget (DTMB) standards.

PRICING AND PAYMENT SCHEDULE:
Payment will be made on an Agency Project Manager acceptance basis. Contractor will invoice the State $138,995 ($59,995 for the MBIS BatchScan Workstation and $79,000 for the MBIS Services for Tier 2 Workflow Change) after Agency Project Manager has formally accepted all deliverables. Contractor will invoice the State for Maintenance costs annually beginning after the 1-Year Warranty. DTMB will pay the Contractor upon receipt of properly completed invoice(s) which will be submitted to the billing address on the state issued purchase order, not more often than monthly. DTMB Accounts Payable will coordinate obtaining Agency Project Manager approvals. All invoices should reflect actual work completed by payment date and must be approved by the Agency Project Manager prior to payment. The invoices will describe and document to the state's satisfaction a description of the work performed, the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense. Payment will be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

Total Costs

BatchScan Workstation and Maintenance	112,680
Services: Tier 2 Workflow Change	79,000
Total	**$191,680**

BatchScan Workstation and Maintenance

Description	Qty	Unit Price	Total
MBIS BatchScan Workstation, including: ◆ BatchScan Software ◆ Control Computer, Monitor, Keyboard ◆ High-speed Scanner with Automatic Document Feeder (ADF) ◆ Installation and On-site Training ◆ **Warranty**: 1 Year On-site ***Advantage*** Solution warranty, 9X5, Next day on-site response and parts replacement ◆ **Freight**	**1**	**$59,995**	**$59,995**
Year 2 - Annual Maintenance *(to start after 1 Year Warranty)* On-site ***Advantage*** Solution, 9X5, Next day on-site response and parts replacement	**1**	**$9,534**	**$9,534**
Year 3 - Annual Maintenance *(to start after 1 Year Warranty)* On-site ***Advantage*** Solution, 9X5, Next day on-site response and parts replacement	**1**	**$10,011**	**$10,011**
Year 4 - Annual Maintenance *(to start after 1 Year Warranty)* On-site ***Advantage*** Solution, 9X5, Next day on-site response and parts replacement	**1**	**$10, 512**	**$10,512**
Year 5 - Annual Maintenance *(to start after 1 Year Warranty)* On-site ***Advantage*** Solution, 9X5, Next day on-site response and parts replacement	**1**	**$11,038**	**$11,038**
Year 6 - Annual Maintenance *(to start after 1 Year Warranty)* On-site ***Advantage*** Solution, 9X5, Next day on-site response and parts replacement	**1**	**$11,590**	**$11,590**
Total Workstation and Maintenance Costs			**$112,680**

Services: Tier 2 Workflow Change

	Description	Qty	Unit Price	Total
AFIS-WFAVRG-00 *TP-IAT-CUSTOM*	**MBIS Services for Tier 2 Workflow Change to include:** ◆ On-site Deployment ◆ On-site Installation and Testing ◆ Documentation on Workflow Change	**1**	**$79,000**	**$79,000**

EXPENSES:
The state will not pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:
The designated Contractor Project Manager is:

Mr. Majid Assemi
Program Management
5515 E. La Palma Avenue
Anaheim, CA 92807
714-238-2011
Majid.Assemi@us.idemia.com

The designated Agency Project Manager is:

Scott Blanchard
Michigan State Police
Biometrics and Identification Division
7150 Harris Drive
Dimondale, MI 48821
517-243-1517
Blanchards1@michigan.gov

AGENCY RESPONSIBILITIES:
- Provide necessary facility resources required for equipment installation and operation including access, space, environmental control, electrical power, and networking.
- Test and verify workflow modifications.
- Review documentation.

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:
Contractor staff will work at their location in Anaheim, CA 92807 and at the MSP Headquarters.

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:
Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **6**
to
Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Majid Assemi
	714-238-2011
	majid.assemi@idemia.com
	CV0000922

STATE			
Program Manager	Various	MSP
Contract Administrator	Jarrod Barron	DTMB
	(517) 249-0406	
	barronj1@michigan.gov	

CONTRACT SUMMARY			
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		June 13, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$8,386,829.00	$68,712.00	$8,455,541.00

DESCRIPTION
Effective 6/11/2021, the parties add $68,712.00 for the equipment, software, and maintenance detailed in the attached cost tables. All other terms, conditions, specifications and pricing remain the same. Per contractor, agency and DTMB Procurement.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
MSP	Scott L. Blanchard	517-243-1517	BlanchardS1@michigan.gov
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov

TOTAL CHANGE NOTICE COSTS	
Equipment	$ 42,300.00
Maintenance	$ 26,412.00
Total	$ 68,712.00

EQUIPMENT COSTS			
Item	Quantity	Price	Total
Laptop (Tenprint SW)	2	$ 19,300.00	$ 38,600.00
32" Monitor	5	$ 530.00	$ 2,650.00
USB Port Replicator	5	$ 210.00	$ 1,050.00
Total			$ 42,300.00

MAINTENANCE COSTS			
Year	# Laptops	Unit Cost	Total
Y1	2	$ -	$ -
Y2	2	$ 3,064.00	$ 6,128.00
Y3	2	$ 3,217.00	$ 6,434.00
Y4	2	$ 3,378.00	$ 6,756.00
Y5	2	$ 3,547.00	$ 7,094.00
			$ 26,412.00

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **5**
to
Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Majid Assemi
	714-238-2011
	majid.assemi@idemia.com
	CV0000922

STATE			
	Program Manager	Various	MSP
	Contract Administrator	Jarrod Barron	DTMB
		(517) 249-0406	
		barronj1@michigan.gov	

CONTRACT SUMMARY			
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		June 13, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$8,326,829.00	$60,000.00	$8,386,829.00

DESCRIPTION
Effective 9/10/2020, the parties add $60,000 for the AFIS and CHS database synchonization enhancements detailed in the attached statement of work. All other terms, conditions, specifications and pricing remain the same. Per contractor, agency, DTMB Procurement and State Administrative Board approval on 9/10/2020.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
MSP	Scott L. Blanchard	517-243-1517	BlanchardS1@michigan.gov
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov

MICHIGAN DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET
IT SERVICES
STATEMENT OF WORK

Project Title: **Idemia Workflow Database Comparison**	**Period of Coverage:**
Requesting Department: **Michigan State Police**	**Date:** **8/25/2020**
Agency Project Manager: **Scott Blanchard**	**Phone:** **517-243-1517**
DTMB Project Manager: **Gordon Mayes**	**Phone:** **517-204-8026**

BACKGROUND:
The Michigan State Police (MSP) purchased a new Automated Fingerprint Identification System (AFIS). MSP has always completed an additional databases comparison with the Criminal History System (CHS) to be sure the two systems were in sync. With this new AFIS the database is more complex and MSP also wants to increase it automation of this process.

PROJECT OBJECTIVE:
The objective of this project is to have Idemia to write a new process that will address the additional complexities of the new system and increase some automated process for us to better, more timely and more efficiently maintain our databases.

SCOPE OF WORK:
IDEMIA will provide software utilities and report function. Input to the IDEMA software utility will be an industry standard file format file generated by the CHS that consists of a list of State ID Number, Transaction Control Number and a set of descriptors (name, race, sex, date of birth, AFIS flag, Palm flag, and photo flag) to update the person record in the AFIS database. A privileged system administration will run this utility. The utility will update the records in the MBIS with logically delete or seal records based on the input file provided by the CHR system. The output of the IDEMIA utility will be a text file that lists records in the AFIS database with the AFIS or Palm Available flags set. This process will also make determination of records that need to be deleted. IDEMIA will provide a report that lists all the records with logical-delete flag set and expired. The software utility run by system administrator will delete records from the AFIS database.

TASKS:
Technical support is required to assist with the following tasks:

1. Make the appropriate updates to Michigan State Police existing system workflow documentation
2. Configure the workflow changes and perform integration testing using the IDEMIA clone system to verify the updated workflow functionality
3. Deploy the workflow change to Michigan State Police test system
4. Perform acceptance testing
5. Put the workflow updates into production

DELIVERABLES:
Deliverables will not be considered complete until the Agency Project Manager has formally accepted them. Deliverables for this project include:

1. Updated workflow process and utilities.
2. Updated documentation to include these changes.
3. Apply these changes to the Test, Production and Disaster Recover AFIS.

ACCEPTANCE CRITERIA:
Acceptance criteria for the deliverables include:

Verified workflow was properly modified to accept the file from CHS and correctly make comparisons and updates to the AFIS. MSP will create test records and defined know results for the testing process. Provide output reports of the comparison results and processes taken. Provide output file for updates to CHS.

1. Verified modifications to the workflow as defined above.
2. Reviewed and accepted results.
3. Reviewed and accepted reports.
4. Updated documentation to include these changes in the administrative and design manual.

PROJECT CONTROL AND REPORTS:
A bi-weekly progress report must be submitted to the Agency and DTMB Project Managers throughout the life of this project. This report may be submitted with the billing invoice. Each bi-weekly progress report must contain the following:

1. **Hours**: Indicate the number of hours expended during the past two weeks, and the cumulative total to date for the project. Also state whether the remaining hours are sufficient to complete the project.
2. **Accomplishments**: Indicate what was worked on and what was completed during the current reporting period.
3. **Funds**: Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

SPECIFIC DEPARTMENT STANDARDS:
Agency standards, if any, in addition to DTMB standards.

PAYMENT SCHEDULE:
A one-time $60,000 payment will be made on a Agency Project Manager acceptance basis following delivery and acceptance of the work. DTMB will pay CONTRACTOR upon receipt of properly completed invoice(s) which shall be submitted to the billing address on the State issued purchase order not more often than monthly. DTMB Accounts Payable area will coordinate obtaining Agency and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date, and must be approved by the Agency and DTMB Project Manager prior to payment. The invoices shall describe and document to the State's satisfaction a description of the work performed, the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense. Payment shall be considered timely if made by the DTMB within forty-five (45) days after receipt of properly completed invoices.

EXPENSES:
The State will NOT pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:
The designated Contractor Project Manager is:

Mr. Majid Assemi
Program Management
5515 E. La Palma Avenue
Anaheim, CA 92807
714-238-2011
Majid.Assemi@us.idemia.com

The designated Agency Program Manager is:

Scott Blanchard
Michigan State Police
Biometrics and Identification Division

MSP HQ
7150 Harris Drive
Dimondale, MI 48821
517-243-1517
Blanchards1@michigan.gov

The designated DTMB Program Manager is:

Gordon Mayes
DTMB
Agency Services
MSP HQ
7150 Harris Drive
Dimondale, MI 48821
517-204-8026
MayesG1@michigan.gov

AGENCY RESPONSIBILITIES:

1. Test and verify workflow modifications.
2. Review and verify reports.
3. Review documentation

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:
Contractor staff will work at its work location in Anaheim, CA 92807.

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:
Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing. No overtime will be permitted.

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES

Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **4**

to

Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Majid Assemi
	714-238-2011
	majid.assemi@idemia.com
	CV0000922

STATE			
Program Manager	Various		
Contract Administrator	Jarrod Barron	DTMB	
	(517) 249-0406		
	barronj1@michigan.gov		

CONTRACT SUMMARY			
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-Card	☐ PRC	☐ Other	☐ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
☐		☐		June 13, 2022
CURRENT VALUE	**VALUE OF CHANGE NOTICE**	**ESTIMATED AGGREGATE CONTRACT VALUE**		
$8,236,515.00	$90,314.00	$8,326,829.00		

DESCRIPTION

Effective 6/3/2020, the parties add $90,314 for maintenance and support for two MBIS Card Capture workstations (2 HP desktop, 2 Monitors, 2 Epson Scanners) and two Printers per the existing contract pricing and service level agreement. All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Procurement approval.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
MSP	Scott L. Blanchard	517-243-1517	BlanchardS1@michigan.gov
DTMB	Gordon Mayes	517-204-8026	MayesG1@michigan.gov

CHANGE ORDER

The purpose of this Change Request is to modify the Michigan MBIS Cloud configuration to include Maintenance and Support agreement for two MBIS Card Capture workstations (2 HP desktop, 2 Monitors, 2 Epson Scanners) and two Printers. The annual maintenance price listed in the following table:

Start Date	End Date	Maintenance Price
6/3/2020	9/30/2020	$3,511.00
10/1/2020	9/30/2021	$11,213.00
10/1/2021	9/30/2022	$11,773.00
10/1/2022	9/30/2023	$12,362.00
10/1/2023	9/30/2024	$12,980.00
10/1/2024	9/30/2025	$13,628.00
10/1/2025	9/30/2026	$14,309.00
10/1/2026	6/13/2027	$10,538.00

For this change, IDEMIA (formerly MorphoTrak, LLC) will provide maintenance support (hardware and software).

Contract Price:

Change Order **# MSP-007** Amount:	**$**	**90,314.00**
Total:	**$**	**90,314.00**

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
to
Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue , Suite 100
	Anaheim, CA 92807
	Doug Meier
	714-683-3169
	douglas.meier@morpho.com
	CV0000922

STATE			
	Program Manager	Scott Blanchard	MSP
		517-284-3168	
		BlanchardS1@Michigan.gov	
	Contract Administrator	Sean Regan	DTMB
		(517) 243-8459	
		regans@michigan.gov	

CONTRACT SUMMARY

AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		June 13, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$8,183,315.00	$53,200.00	$8,236,515.00

DESCRIPTION

Effective March 4, 2019, the Michigan State Police are adding $53,200.00 to this contract to migrate the GW2GW VPN connection to the State of Michigan Express Route connection to Azure for the Automated Fingerprint Identification System, per the below Statement of Work.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Procurement approval.

CHANGE ORDER APPROVAL

Per your request, the following change order is presented for the State's consideration.

Problem Description: Gateway to gateway (GW2GW) disconnects every 24 hours.

Proposed Change: Migrate current GW2GW VPN connection to State of Michigan Express Route connection to Azure. Telecom to build an isolated segment in the express route for the MSP traffic. Configure routing in the SOM network to route the ABIS traffic through the new connection. In this new plan, the IP addresses mapping will remain the same.

Work to be Performed:

1. Update the network documentation
2. Review the new network documentation with DTMB and agree with the network mapping.
3. Implement configuration changes to the network.
4. Test the new network connections.
5. Implement the network changes on the Production environment using Express Route

Timeframe: Implement the changes within 90 days of change order approval.

Roles and Responsibilities:

Michigan State Police / DTMB/MSP AFIS	**IDEMIA**
	Update documentations with new changes
Participate in the review	Review changes with DTMB and MSP AFIS
Provide bandwidth of 200 Mbps Network Isolation Configure routing in the SOM network	Configure the network – • Add new keys • Add routes • Turn off existing VPNs
• Provide a workstation for testing • Participate in Testing • Test and agree with the performance of the system	Test new configuration
Provide staff during testing	Manage testing activities

Payment Milestone: 100% shall be payable upon successful implementation.

CHANGE ORDER APPROVAL

Contract Price:

Change Order **# MSP-005** Amount:	**$**	**53,200.00**
Total:	**$**	**53,200.00**

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**
to
Contract Number **071B7700122**

CONTRACTOR	
	IDEMIA IDENTITY & SECURITY USA LLC
	5515 East La Palma Avenue
	Anaheim, CA 92807
	Doug Meier
	714-683-3169
	douglas.meier@morpho.com
	CV0000922

STATE			
Program Manager	Scott Blanchard	MSP
	517-284-3168	
	BlanchardS1@Michigan.gov	
Contract Administrator	Sean Regan	DTMB
	(517) 243-8459	
	regans@michigan.gov	

CONTRACT SUMMARY			
AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		June 13, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$8,183,315.00	$0.00	$8,183,315.00

DESCRIPTION

Effective December 11, 2018, The Michigan State Police are adding ABIS Tenprint Terminals to this Contract, please see attached documentation for individual workstation pricing. Please note the Regional Support Manager has been changed to Mr. Tony Morris.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Procurement approval.

IDEMIA

CHANGE ORDER APPROVAL

Per your request, the following individual workstation pricing is established for Contract # 071B7700122. Prices quoted below are valid to the contract expiration date of June 13, 2022. Pricing includes shipping and onsite installation, but does not include individual training if required or taxes if applicable. A separate quote will be provided for training upon request.

Workstation Description:

ABIS Tenprint Terminal consisting of:

Desktop PC
Flatbed Scanner
B/W Card Printer / Color Network Printer – Please specify
Tenprint Application Software License

Workstation	Price	Y1 Maint	Y2 Maint	Y3 Maint	Y4 Maint	Y5 Maint
Tenprint	$28,100	WARR	$ 5,339	$ 5,606	$ 5,886	$ 6,181

ABIS Tenprint Reviewer Laptop Terminal consisting of:

Laptop (for remote work)
Tenprint Application Software License

Workstation	Price	Y1 Maint	Y2 Maint	Y3 Maint	Y4 Maint	Y5 Maint
Tenprint Reviewer	$19,300	WARR	$ 3,064	$ 3,217	$ 3,378	$ 3,547

ABIS Latent Terminal consisting of:

Desktop PC
Latent Flatbed Scanner
Latent Camera
Color Printer
Latent Application Software License

Workstation	Price	Y1 Maint	Y2 Maint	Y3 Maint	Y4 Maint	Y5 Maint
Latent	$44,700	WARR	$ 8,493	$ 8,918	$ 9,364	$ 9,832

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT
Department of Technology, Management, and Budget

525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**

to

Contract Number **071B7700122C**

NEW CONTRACTOR	
	Idemia Identity & Security USA LLC
	5515 East La Palma Avenue
	Anaheim, CA 92807
	Doug Meier
	714-683-3169

STATE CONTACT

Program Manager	Scott Blanchard	MSP	Contract Administrator	Sean Regan	DTMB
	517-284-3168			(517) 243-8459	
	BlanchardS1@Michigan.gov			regans@michigan.gov	

CONTRACT SUMMARY

AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS)

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
June 14, 2017	June 13, 2022	2 - 5 Year	June 13, 2022

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
P-Card	Direct Voucher (DV)	☐ Other	☐ Yes	☒ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		June 13, 2022

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$8,100,507.00	$82,808.00	$8,183,315.00

DESCRIPTION

Effective August 27th, 2018, the Michigan State Police are adding $82,808.00 to this contract to modify the Michigan MBIS Cloud configuration to include Primary and Disaster Recovery MQSeries hosts in support of the State's Criminal History System (CHS). The cost per year is priced out in the below quote at $20,702.00.
Please note the vendor MorphoTrak, LLC merged with it's affilate, IDEMIA Identity & Security USA LLC. IDEMIA Identity & Security USA LLC will be the contracting entity and has agreed to all current contracts between MorphoTrack, LLC and the State of Michigan.
All other terms, conditions, specifications, and pricing remain the same. Per contractor and agency agreement and DTMB procurement approval.

⟨⟨⟩⟩ IDEMIA

CHANGE ORDER APPROVAL

The purpose of this Change Request is to modify the Michigan MBIS Cloud configuration to include Primary and Disaster Recovery MQSeries hosts in support of the State's Computer Criminal History (CCH) system.

For this change, IDEMIA (formerly MorphoTrak, LLC) will provide two (2) servers at the designated Azure Cloud "production" (primary site) center and two (2) servers at the designated Azure Disaster Recovery (secondary site) "cloud" center. All administrative and backup services associated with the operation of the "cloud" services will be performed by IDEMIA as part of its responsibilities. Two (2) servers are required at each site to meet the State's High Availability (HA) and uptime requirement.

The minimum configuration of the servers is as follows:

2 x VCPU, 8GB Memory
1 x 100GB OS Disk
1 x 100GB Data Disk

Michigan State DTMB is responsible for providing the necessary MQ Series licenses and any license updates when made available.

The price listed below is an annual reoccurring cloud service fee.

IDEMIA

CHANGE ORDER APPROVAL

Contract Price:

Change Order # **MSP-001** Amount:	**$**	**20,702.00**
Total:	**$**	**20,702.00**

STATE OF MICHIGAN
ENTERPRISE PROCUREMENT

Department of Technology Management and Budget

525 W. Allegan St., Lansing, Michigan 48913
P.O. Box 30026 Lansing, Michigan 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **071B7700122**

between

THE STATE OF MICHIGAN

and

CONTRACTOR	
	MorphoTrak, LLC
	5515 East La Palma Avenue, Suite 100
	Anaheim, CA 92807
	Doug Meier
	(714) 688-3169
	Douglas.Meier@morpho.com
	Tax ID (last four digits only)

STATE			
	Program	Scott Blanchard	MSP
		(517) 284-3168	
		BlanchardS1@michigan.gov	
	Contract	Simon Baldwin	DTMB
		(517) 284-6997	
		BaldwinS@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Automated Biometric Identification System (ABIS)			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
6/14/2017	6/13/2022	(2) 5-Year	
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45			
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card	☐ Direct Voucher (DV)	☐ Other	☐ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			
MISCELLANEOUS INFORMATION			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**8,100,507.00**

FOR THE CONTRACTOR:

____
Company Name

____
Authorized Agent Signature

____
Authorized Agent **(Print or Type)**

____
Date

FOR THE STATE:

____
Signature

Jeff Brownlee, Director of Sourcing Operations
Name & Title

DTMB Procurement
Agency

____
Date

STATE OF MICHIGAN

This Hosted Software Contract (this "**Contract**") is agreed to between the State of Michigan (the "**State**") and MorphoTrak, LLC ("**Contractor**"), a California limited liability company. This Contract is effective on June 14, 2017 ("**Effective Date**"), and unless earlier terminated, will expire on June 13, 2022 (the "Term").

This Contract may be renewed for up to two (2) additional five (5) year periods. Renewal must be by written notice from the State and will automatically extend the Term of this Contract.

1. **Definitions.** For the purposes of this Contract, the following terms have the following meanings:

"**Acceptance**" has the meaning set forth in **Section 13.5**.

"**Acceptance Tests**" means such tests as may be conducted in accordance with **Section 13** and the Statement of Work to determine whether the Software meets the material requirements of this Contract and the Documentation.

"**Affiliate**" of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term "control" (including the terms "controlled by" and "under common control with") means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

"**Allegedly Infringing Materials**" has the meaning set forth in **Section 27.3(b)(ii)**.

"**API**" means all Application Programming Interfaces and associated API Documentation thatis specific to the State's information technology infrastructure and custom developed and provided by Contractor, and as updated from time to time, to allow the Software to integrate with Contractor's Software and various Third-Party Software.

"**Authorized Users**" means all Persons authorized by the State to access and use the Software only in connection with this Contract.

"**Business Day**" means a day other than a Saturday, Sunday or other day on which the State is authorized or required by Law to be closed for business.

“Business Owner” is the individual appointed by the State to (a) act as the State’s representative in all matters relating to the Contract, and (b) co-sign off on notice of Acceptance for the Software. The Business Owner will be identified in the Statement of Work.

“**Business Requirements Specification**” means the initial specification setting forth the State’s business requirements regarding the features and functionality of the Software, as set forth in the Statement of Work.

“**Change**” has the meaning set forth in **Section 3.2**.

“**Change Notice**” has the meaning set forth in **Section 3.2(b)**.

“**Change Proposal**” has the meaning set forth in **Section 3.2(a)**.

“**Change Request**” has the meaning set forth in **Section 3.2**.

“**Confidential Information**” has the meaning set forth in **Section 21.1**.

“**Configuration**” means State-specific changes made by the Contractor to the Software without Source Code or structural data model changes occurring.

“**Contract**” has the meaning set forth in the preamble.

“**Contract Administrator**” is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party’s Contract Administrator will be identified in the Statement of Work.

“**Contractor**” has the meaning set forth in the preamble.

“**Contractor’s Bid Response**” means the Contractor’s proposal submitted in response to the RFP.

“**Contractor Personnel**” means all employees and independent contractors of Contractor or any Permitted Subcontractors involved in the performance of Services hereunder.

“**Contractor’s Test Package**” has the meaning set forth in **Section 12.2**.

“**Customization**” means State-specific changes made by Contractor to the Software requiring changes to the Source Code.

“**Deliverables**” as further expressly described herein means the Software offered as hosted Services, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in the Statement of Work.

“**Dispute Resolution Procedure**” has the meaning set forth in **Section 31.1**.

“**Documentation**” means user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

“**Effective Date**” has the meaning set forth in the preamble.

“**Fees**” means collectively, the License Fees, Implementation Fees, and Support Services Fees.

“**Financial Audit Period**” has the meaning set forth in **Section 29.1**.

“**Force Majeure**” has the meaning set forth in **Section 31.1**.

“**Harmful Code**” means any: (a) virus, trojan horse, worm, backdoor or other software or hardware devices the effect of which is to permit unauthorized access to, or to disable, erase, or otherwise harm, any computer, systems or software; or (b) time bomb, drop dead device, or other software or hardware device designed to disable a computer program automatically with the passage of time or under the positive control of any Person, or otherwise prevent, restrict or impede the State's or any Authorized User's use of such software.

“**HIPAA**” has the meaning set forth in **Section 20.1**.

“**Hosting Environment**” means, collectively, the Microsoft Azure Government platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in the Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software and system architecture and configuration.

“**Implementation Fees**” has the meaning set forth in **Section 17.2**.

“**Implementation Plan**” means the schedule included in the Statement of Work setting forth the sequence of events for the performance of Services under the Statement of Work, including the Milestones and Milestone Dates.

“**Integration Testing**” has the meaning set forth in **Section 13.1(c)**.

“**Intellectual Property Rights**” means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable Law in any jurisdiction throughout the world.

“**Key Personnel**” means any Contractor Personnel identified as key personnel in the Statement of Work.

“**Law**” means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement or rule of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction.

“**License Agreement**” has the meaning set forth in **Section 4**.

“**License Fee**” has the meaning set forth in **Section 17.1**.

“**Loss or Losses**” means all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable outside attorneys' fees and the third party costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

“**Maintenance Release**” means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide or make available to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“**Milestone**” means an event or task described in the Implementation Plan under the Statement of Work that must be completed by the corresponding Milestone Date.

“**Milestone Date**” means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under the Statement of Work.

“**New Version**” means any new version of the Software that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“**Nonconformity**” or **“Nonconformities”** means any material failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

“**Open-Source Components**” means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

“**Open-Source License**” has the meaning set forth in **Section 5**.

“**Permitted Subcontractor**” has the meaning set forth in **Section 10.4**.

“**Person**” means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

“**Pricing**” means any and all fees, rates and prices payable under this Contract, including pursuant to any Schedule or Exhibit hereto.

“**Pricing Schedule**” means the schedule attached as **Schedule D**, setting forth the License Fees, Implementation Fees, Support Services Fees, and any other fees, rates and prices payable under this Contract.

“**Project Manager**” is the individual appointed by each party to (a) monitor and coordinate the day-to-day activities of this Contract, and (b) for the State, to co-sign off on its notice of Acceptance for the Software. Each party’s Project Manager will be identified in the Statement of Work.

“**Representatives**” means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

“**RFP**” means the State’s request for proposal designed to solicit responses for Services under this Contract.

“**State**” has the meaning set forth in the preamble.

“**State Data**” has the meaning set forth in **Section 20.1**.

“**State Materials**” means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“**State Resources**” has the meaning set forth in **Section 11.1(a)**.

“**Services**” means any of the services Contractor is required to or otherwise does provide under this Contract, the Statement of Work, and the Service Level Agreement.

“**Service Level Agreement**” means the service level agreement attached as **Schedule B** to this Contract, setting forth Contractor’s obligations with respect to the hosting, management and operation of the Software.

“**Site**” means the physical location designated by Contractor for delivery and installation of the Software.

“**Software**” means Contractor’s software in the hosted environment and deployed in the State environment set forth in the Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Customizations or Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract and the License Agreement.

"**Source Code**" means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to provide maintenance for the Software.

"**Specifications**" means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, RFP or Contractor's Bid Response, if any, for such Software, or elsewhere in the Statement of Work.

"**Statement of Work**" means the statement of work entered into by the parties and attached as **Schedule A** to this Contract.

"**Stop Work Order**" has the meaning set forth in **Section 25**.

"**Support Services**" means the Software maintenance and support services Contractor is required to or otherwise does provide to the State under the Service Level Agreement.

"**Support Services Fees**" has the meaning set forth in **Section 17.3**.

"**Technical Specification**" means, with respect to any Software, the document setting forth the technical specifications for such Software and included in the Statement of Work.

"**Term**" has the meaning set forth in the preamble.

"**Test Data**" has the meaning set forth in **Section 12.2**.

"**Testing Period**" has the meaning set forth in **Section 13.1(b)**.

"**Test Results**" has the meaning set forth in **Section 12.2**.

"**Third Party**" means any Person other than the State or Contractor.

"**Third Part License**" has the meaning set forth in **Section 5**.

"**Third-Party Software**" means software, content, and technology, in any form or media, in which any Person other than the State or Contractor owns any Intellectual Property Right, but excluding Open-Source Components.

"**Transition Period**" has the meaning set forth in **Section 24.3**

"**Transition Responsibilities**" has the meaning set forth in **Section 24.3**.

"**Unauthorized Removal**" has the meaning set forth in **Section 10.3(b)**.

"**Unauthorized Removal Credit**" has the meaning set forth in **Section 10.3(c)**.

"**User Data**" means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, processed, generated or output by any device, system or network by the State except that User Data does not include the Software, Documentation, Services, Deliverables, or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input.

2. **Schedules**. All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Service Level Agreement
Schedule C	License Agreement
Schedule D	Pricing Schedule
Schedule E	Disaster Recovery Plan
Schedule F	Terms for On-Site Workstations

3. **Statement of Work**. Contractor shall provide Services and Deliverables pursuant to the executed Statement of Work entered into under this Contract. The Statement of Work shall not be effective unless signed by each party's Contract Administrator or higher ranking officer. The term of the Statement of Work shall commence on the parties' full execution of the Statement of Work and terminate upon the earlier of: (i) when the parties have fully performed their obligations, or (ii) upon the natural expiration or earlier termination of this Contract. The terms and conditions of this Contract will apply at all times to the Statement of Work. The State shall have the right to terminate such Statement of Work as set forth in **Section 24**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under the Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statement of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

3.1 Statement of Work Requirements. The Statement of Work will include the following:

(a) names and contact information for Contractor's Contract Administrator, Project Manager and Key Personnel;

(b) names and contact information for the State's Contract Administrator, Project Manager and Business Owner;

(c) a detailed description of the Services to be provided under this Contract, including any training obligations of Contractor;

(d) a detailed description of the Software to be provided under this Contract, including the:

(i) version and release number of the Software;

(ii) Business Requirements Specification;

(iii) Technical Specification;

(iv) The Hosting Environment; and

(v) a description of the Documentation to be provided;

(e) the Project Management Methodology (PMM) that will be utilized;

(f) an Implementation Plan that follows the PMM, including all Milestones, the corresponding Milestone Dates and the parties' respective responsibilities under the Implementation Plan;

(g) the due dates for payment of Fees and any invoicing requirements, including any Milestones on which any such Fees are conditioned, and such other information as the parties deem necessary;

(h) disclosure of all Third-Party Software and Open-Source Components (each identified on a separate exhibit to the Statement of Work), in each case accompanied by such related documents as may be required by this Contract;

(i) a detailed description of all State Resources required to complete the Implementation Plan.

3.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to the Statement of Work, including changes to the Services and Implementation Plan (each, a "**Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all mutually agreed upon Changes in accordance with this **Section 3.2**.

(a) As soon as reasonably practicable, and in any case within twenty (20) Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change ("**Change Proposal**"), setting forth:

(i) a written description of the proposed Changes to any Services or Deliverables;

(ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under the Statement of Work;

(iii) any additional State Resources Contractor deems necessary to carry out such Changes; and

(iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect any increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within thirty (30) Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by the State's Contract Administrator and will constitute an amendment to the Statement of Work to which it relates; and

(c) If the parties fail to enter into a Change Notice within fifteen (15) Business Days following the State's response to a Change Proposal, the State may, in its discretion:

(i) require Contractor to perform the Services under the Statement of Work without the Change;

(ii) require Contractor to continue to negotiate a Change Notice;

(iii) initiate a Dispute Resolution Procedure; or

(iv) notwithstanding any provision to the contrary in the Statement of Work, terminate this Contract under **Section 24.2**.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with the Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best commercial efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

4. **Contractor Software License**. Contractor hereby grants to the State and its Authorized Users the right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract and the License Agreement set forth in **Schedule C** (the "**License Agreement**"), as such license is limited to carrying out the purposes of this Contract.

5. **Third-Party Software Licenses**. Any use hereunder of Third-Party Software shall be governed by, and subject to, the terms and conditions of the applicable Third-Party Software license agreement ("**Third-Party License**"). As of the effective date of this Contract, Contractor shall identify and describe in an exhibit to the Statement of Work any Third-Party Software being used in connection with the Services.

6. **Open-Source Licenses**. Any use hereunder of Open-Source Components shall be governed by, and subject to, the terms and conditions of the applicable open-source license ("**Open-Source License**"). As of the effective date of this Contract, Contractor shall identify and describe in an exhibit to the Statement of Work each of the Open-Source Components of the Software, and include an exhibit attaching all applicable Open-Source Software Licenses or identifying the URL where these licenses are publicly available.

7. **Software Implementation**.

7.1 Implementation. Contractor will deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the express criteria set forth in the Statement of Work.

7.2 Site Preparation. Contractor is responsible for ensuring the relevant Hosting Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in the Statement of Work, prior to installation of the Software, to give the State sufficient time to prepare for purposes of end user acceptance testing.

8. **Hosting and Support**.

8.1 Availability. Contractor will maintain the Availability Requirement set forth in the Service Level Agreement attached as **Schedule B** to this Contract.

8.2 Support Services. Contractor shall provide the State with the Support Services and maintain the Support Service Level Requirement set forth in the Service Level Agreement attached as **Schedule B** to this Contract.

9. **Data Privacy and Information Security**.

9.1 Undertaking by Contractor. Contractor shall comply with all security requirements set forth in the Service Level Agreement attached as **Schedule B** to this Contract. In addition, and without limiting Contractor's obligation of confidentiality as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to: (a) ensure the security and confidentiality of the State Data; (b) protect against any anticipated threats or hazards to the security or integrity of the State Data; (c) protect against unauthorized disclosure, access to, or use of the State Data; (d) ensure the proper disposal of State Data; and (e) ensure that all Contractor Representatives comply with all of the foregoing.

9.2 To the extent that Contractor has access to the State's computer system, Contractor must comply with the State's Acceptable Use Policy, see http://michigan.gov/cybersecurity/0,1607,7-217-34395_34476---,00.html. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing the State's system. The State reserves the right to terminate Contractor's access to the State's system if a violation occurs.

9.3 Right of Audit by the State. Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Services and from time to time during the term of this Contract. During the providing of Services, on an ongoing basis from time to time and with seven (7) days notice, the State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. In lieu of an on-site audit, upon request by the State, Contractor agrees to complete, within forty-five (45) calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.

9.4 Audit Findings. With respect to State Data, Contractor must implement any reasonably required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program. To the extent any such safeguards require Contractor as a result in a material change in scope to the Services, Contractor shall inform the State Contract Administrator in writing and the parties will follow the Change control process in Section 2.2 of this Contract.

9.5 State's Right to Termination for Deficiencies. The State reserves the right, at its sole election, to immediately terminate this Contract or the Statement of Work without limitation and without liability if the Contractor fails or has failed to meet its material obligations under this **Section 9** and does not cure such failure within thirty (30) days of the State's written notice of Deficiencies under this Section8.

10. **Performance of Services**. Contractor will provide all Services and Deliverables in a timely, professional and workmanlike manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement of Work.

10.1 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

(i) ensure that such Contractor Personnel have the legal right to work in the United States;

(ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and

(iii) upon request, perform background checks on all Contractor Personnel who have access to State Data prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks on Contractor Personnel.

(c) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

10.2 Contractor's Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor's Project Manager, who will be considered Key Personnel of Contractor. Contractor's Project Manager will be identified in the Statement of Work.

(a) Contractor's Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;

(ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor's Project Manager [or her/his designee if unavailable (e.g. due to illness, disability, etc.)] must attend all regularly scheduled meetings as set forth in the Implementation Plan, and will otherwise be available as set forth in the Statement of Work.

(c) Contractor will maintain the same Project Manager throughout the Term of this Contract, unless:

(i) the State requests in writing the removal of Contractor's Project Manager;

(ii) the State consents in writing to any removal requested by Contractor in writing;

(iii) Contractor's Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Contractor will promptly replace its Project Manager on the occurrence of any event set forth in **Section 10.2(c)**. Such replacement will be subject to the State's prior written approval.

10.3 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State's Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment.

(c) It is further acknowledged that an Unauthorized Removal may interfere with the timely and proper completion of this Contract, to the potential loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 24.1**, Contractor will issue to the State an amount equal to $10,000 per individual (each, an "**Unauthorized Removal Credit**").

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection (c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

10.4 Subcontractors. Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any Third Party to perform Services. The State's approval of any such Third Party (each approved Third Party, a "**Permitted Subcontractor**") does not relieve Contractor of its representations, warranties or obligations under this Contract. The parties acknowledge that any Subcontractors identified within the SOW will be deemed approved. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such Permitted Subcontractor (including such Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, shall be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(c) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

11. **State Obligations**.

11.1 State Resources and Access. The State is responsible for:

(a) providing the State Materials and such other resources as may be specified in the Statement of Work (collectively, "**State Resources**"); and

(b) providing Contractor Personnel with such access to State facilities as is necessary for Contractor to perform its obligations on a timely basis as set forth in the Statement of Work.

11.2 State Project Manager. Throughout the Term of this Contract, the State will maintain a State employee to serve as the State's Project Manager under this Contract. The State's Project Manager will be identified in the Statement of Work. The State's Project Manager will be available as set forth in the Statement of Work.

12. **Pre-Delivery Testing**.

12.1 Testing By Contractor. Before delivering and installing the Software, Contractor must:

(a) test the Software to confirm that it is fully operable, meets all applicable Specifications and will function in accordance with the Specifications and Documentation when properly installed in the Hosting Environment;

(b) scan the Software using industry standard scanning software and definitions to confirm it is free of Harmful Code; and

(c) remedy any Non-Conformity or Harmful Code identified and retest and rescan the Software.

12.2 Test Data and Estimates. Unless otherwise specified in the Statement of Work, Contractor shall provide to the State all test data and testing scripts used by Contractor for its pre-delivery testing ("**Test Data**"), together with the results Contractor expects to be achieved by processing the Test Data using the Software ("**Test Results**," and together with Test Data, "**Contractor's Test Package**").

13. **Acceptance Testing; Acceptance**. Unless otherwise set forth in the Statement of Work, the following Section will control Acceptance Testing of the Software:

13.1 Acceptance Testing.

(a) Unless otherwise specified in the Statement of Work, upon installation of the Software, Acceptance Tests will be conducted as set forth in this **Section 13** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation. The State may, but is not obligated, to perform its own pretest on the Software utilizing Contractor's Test Package. If the State does perform a pretest, and Contractor's Test Package does not successfully pass the Test Data or Test Estimate scripts as described by Contractor, the State, at its discretion, is not obligated to move into the formal Acceptance Tests set forth in this Section. The State may elect to send Contractor's Test Package back to Contractor to correct any problems encountered with the Test Data or Test Results.

(b) All Acceptance Tests will take place at the designated Site(s) in the Hosting Environment described in the Statement of Work, commence on the Business Day following installation of the Software and be conducted diligently for up to fifteen (15) Business Days, or such other period as may be set forth in the Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in the Statement of Work or, if the Statement of Work does not specify, the State, provided that:

(i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

(ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.

(c) Upon delivery and installation of any Customization, Configuration or API to the Software under the Statement of Work, additional Acceptance Tests will be performed on the configured Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 13.1**, **Section 13.3**, and **Section 13.4**.

(d) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within ten (10) Business Days, use its reasonable efforts to correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

13.2 <u>Notices of Completion, Non-Conformities, and Acceptance</u>. Within fifteen (15) Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either party and identifies any Non-Conformities, the parties' rights, remedies, and obligations will be as set forth in **Section 13.3** and **Section 13.4**.

(b) If such notice is provided by the State, is signed by the State's Business Owner and Project Manager, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have up to fifteen (15) Business Days to use the Software in the Hosting Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Non-Conformities, on the completion of which the State will, as appropriate:

(i) notify Contractor in writing of Non-Conformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Section 13.3** and **Section 13.4**; or

(ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State's Business Owner and Project Manager.

13.3 <u>Failure of Acceptance Tests</u>. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in the Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within thirty (30) Business Days following, as applicable, Contractor's:

(a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or

(b) receipt of the State's notice under **Section 13.1(a)** or **Section 13.2(c)(i)**, identifying any Non-Conformities.

13.4 <u>Repeated Failure of Acceptance Tests</u>. If Acceptance Tests identify any Non-Conformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 13**;

(b) accept the Software as a nonconforming deliverable, propose a Change Request proposing the Fees for such Software to be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and the Statement of Work and terminate this Contract for cause in accordance with **Section 24.1**.

13.5 <u>Acceptance</u>. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) will occur on the date that is the earliest of the State's delivery of a notice accepting the Software under **Section 13.2(b)**, or **Section 13.2(c)(ii)**.

14. **Training**. Contractor shall provide training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in the Statement of Work. Upon the State's request, Contractor shall timely provide training for additional Authorized Users or other additional training on all uses of the Software for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

15. **Maintenance Releases; New Versions**

15.1 <u>Maintenance Releases</u>. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

15.2 <u>New Versions</u>. Provided that the State is current on its Support Services Fees, during the Term, Contractor shall provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

15.3 <u>Installation</u>. Subject to Section 14.4, the Contractor will install maintenance releases in the hosted environment.

15.4 <u>Testing By Contractor</u>. Before delivering and installing the Maintenance Releases and New Versions of the Software, Contractor must:

(a) test the Software to confirm that it is fully operable, meets all applicable Specifications and will function in accordance with the Specifications and Documentation when properly installed in the Operating Environment;

(b) scan the Software using industry standard scanning software and definitions to confirm it is free of Harmful Code; and

(c) remedy any Non-Conformity or Harmful Code identified and retest and rescan the Software.

16. **Source Code Escrow**

16.1 <u>Escrow Contract</u>. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release.

17. **Fees**

17.1 <u>License Fee</u>. In consideration of, and as payment in full for, the rights and license to use the Software, Third-Party Software, and any associated Documentation as provided in this Contract and the applicable license agreements, the State shall pay to Contractor the license fees (the "**License Fee**") set forth on the Pricing Schedule, subject to and in accordance with the timetable and other provisions of the Statement of Work and this **Section 17**.

17.2 Implementation Fees. In consideration of, and as payment in full for, Contractor's provision of implementation services as provided in this Contract and the Statement of Work, the State shall pay to Contractor the implementation fees (the "**Implementation Fees**") set forth on the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable timetable and other provisions of the Statement of Work and this **Section 17**.

17.3 Support Service Fees. In consideration of Contractor providing the Support Services as required under the Service Level Agreement, the State shall pay to Contractor the Support Services fees (the "**Support Service Fees**") set forth in the Pricing Schedule, subject to and in accordance with the terms and conditions of this Contract, including the applicable provisions of the Service Level Agreement and this **Section 17**.

17.4 Firm Pricing/Fee Changes. All Pricing set forth in this Contract is firm and will not be increased, except as otherwise expressly provided in this **Section 17.4**.

(a) The License Fee will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

18. **Invoices and Payment**.

18.1 Invoices. Contractor will invoice the State for Fees in accordance with the requirements set forth in the Statement of Work, including any requirements that condition the rendering of invoices and the payment of Fees upon the successful completion of Milestones. Contractor must submit each invoice in both hard copy and electronic format, via such delivery means and to such address as are specified by the State in the Statement of Work. Each separate invoice must:

(a) clearly identify the Contract to which it relates, in such manner as is required by the State;

(b) list each Fee item separately;

(c) include sufficient detail for each line item to enable the State to satisfy its accounting and charge-back requirements;

(d) for Fees determined on a time and materials basis, report details regarding the number of hours performed during the billing period, the skill or labor category for such Contractor Personnel and the applicable hourly billing rates; and

(e) include such other information as may be required by the State as set forth in the Statement of Work.

18.2 Payment. Invoices are due and payable by the State, in accordance with the State's standard payment procedures as specified in 1984 Public Act no. 279, MCL 17.51, *et seq.*, within forty-five (45) calendar days after receipt, provided the State determines that the invoice was properly rendered. The

State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at http://www.michigan.gov/cpexpress to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment.

18.3 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables purchased under this Contract are for the State's exclusive use.

18.4 Service Availability Credits. Contractor acknowledges and agrees that any credits assessed under the Service Level Agreement: (a) are a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from not meeting the Availability Requirement or the Support Service Level Requirements, which would be impossible or very difficult to accurately estimate; and (b) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract or be payable to the State upon demand. Credits may not exceed the total amount of Fees that would be payable for the relevant service period in which the credits are assessed.

18.5 Payment Disputes. The State may withhold from payment any and all payments and amounts the State disputes in good faith, pending resolution of such dispute, provided that the State:

(a) timely renders all payments and amounts that are not in dispute;

(b) notifies Contractor of the dispute prior to the due date for payment, specifying in such notice:

(i) the amount in dispute; and

(ii) the reason for the dispute set out in sufficient detail to facilitate investigation by Contractor and resolution by the parties;

(c) works with Contractor in good faith to resolve the dispute promptly; and

(d) promptly pays any amount determined to be payable by resolution of the dispute.

Contractor shall not withhold any Services or fail to perform any obligation hereunder by reason of the State's good faith withholding of any payment or amount in accordance with this **Section 18.5** or any dispute arising therefrom.

18.6 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

19. Intellectual Property Rights

19.1 Ownership Rights in Software

(a) Subject to the rights and licenses granted by Contractor in this Contract and the License Agreement, and the provisions of **Section 19.1(b)**:

(i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights in and to the Software, the Services and all other Deliverables, including but not limited to all modifications, improvements, and derivative works based thereon, as well as all new inventions, innovations, discoveries, works of authorship, and other things developed, made and created arising out of and relating to Contractor's activities in furtherance of this Contract; and

(ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software, Documentation or any of the other items in 18.1(a)(i) above as a result of this Contract.

(b) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

19.2 Rights in Third-Party Software. Ownership of all Third-Party Software, and all Intellectual Property Rights therein, is and will remain with its respective owners, subject to any express licenses or sublicenses granted to the State under this Contract and the Third-Party Licenses.

19.3 Rights in Open-Source Components. Ownership of all Intellectual Property Rights in Open-Source Components shall remain with the respective owners thereof, subject to the State's rights under the applicable Open-Source Licenses.

19.4 Ownership Rights in API. The State is and will be the sole and exclusive owner of all right, title, and interest in and to all API custom-developed by the Contractor for the State, including all Intellectual Property Rights in and to the API. In furtherance of the foregoing:

(a) Contractor will create all API as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any API or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such API, including all Intellectual Property Rights in and to the API; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the API.

20. **State Data**.

20.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as State Confidential Information, includes: (a) User Data; and (b) any other data collected, used, processed, stored, or generated by the State in connection with the Services, including but not limited to (i) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and (ii) personal health information ("**PHI**") collected, used, processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This **Section 20.1** survives termination or expiration of this Contract.

20.2 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. Contractor must: (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, the Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This limited license includes the right of Contractor to store State Data in a third party owned and controlled hosted environment (i.e., that is, the cloud) and the transmission of the State Data over third party communication lines. This **Section 20.2** survives termination or expiration of this Contract.

20.3 Data Retention. Specific data retention requirements for the State will be set forth in the Statement of Work.

20.4 Discovery. Contractor shall immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State's use of the Software. Contractor shall notify the State by the fastest means available and also in writing. In no event shall Contractor provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor shall not respond to subpoenas, service of process, FOIA requests, and other legal requests related to State Data without first notifying the State and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for review, revision and approval

20.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, or integrity of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable: (a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State; (c) in the case of PII or PHI, at the State's sole election, (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or (ii) reimburse the State for any costs in notifying the affected individuals; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution; (g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and (i) provide to the State a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination. Notwithstanding the foregoing contractor' aggregate liability shall not exceed $2,000,000.00 under this section. This **Section 19.5** survives termination or expiration of this Contract.

21. **Confidential Information**. Each party acknowledges that it may be exposed to or acquire communication or data of the other party that is confidential in nature and is not intended to be disclosed to third parties. This **Section 21** survives termination or expiration of this Contract.

21.1 Meaning of Confidential Information. The term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked “confidential” or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked “confidential” or with words of similar meaning; or, (c) should reasonably be recognized as confidential information of the disclosing party. The term “Confidential Information” does not include any information or documentation that was or is: (a) in the possession of the State and subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party’s proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). Notwithstanding the above, in all cases and for all matters, State Data is deemed to be Confidential Information.

21.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor’s subcontractor is permissible where: (a) the subcontractor is a Permitted Subcontractor; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and (c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State’s Confidential Information in confidence. At the State’s request, any of the Contractor’s Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 21.2**.

21.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

21.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

21.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within ten (10) Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. If Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and certify the same in writing within ten (10) Business Days from the date of termination to the other party.

22. **HIPAA Compliance**. The State and Contractor must comply with all applicable obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if applicable and reasonably necessary to keep the State and Contractor in compliance with HIPAA.

23. **ADA Compliance**. The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. Contractor's Service Software must comply, where relevant, with level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

24. **Termination, Expiration, Transition**. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

24.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) The State may terminate this Contract for cause, in whole or in part, if Contractor,: (i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel; (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or (iii) breaches any of its material duties or obligations under this Contract; and Contractor fails to cure any of the aforementioned material breach events within thirty (30) days of the date the State provided Contractor with written notice specifically describing the applicable event . Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If Contractor fails to cure its material breach within the cure period and the State terminates this Contract under this **Section 24.1**, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 24.2**.

(c) Where the Contract was terminated by the State for an uncured material breach, the State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. If the State itself is not alleged to be in breach of this Contract, then: (a) Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Support Services Fees; and (b) Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, reasonable attorneys' fees, court costs, and any reasonable out of pocket costs the State incurs to procure the Services from other sources. The State shall undertake all reasonable efforts under applicable law to mitigate its damages.

24.2 Termination for Convenience. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must: (a) cease performance immediately, or (b) continue to perform in accordance with **Section 24.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs for services provided prior to termination. Notwithstanding the foregoing, if the termination is for non-appropriation, the State will pay for all reasonable costs to the extent funds are available.

24.3 Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to: (a) continuing to perform the Services at the established Contract rates and payment terms; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all State Data, it being acknowledged and agreed to by Contractor that return of State Data will be in the usable format specified by the State in this Contract and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees to Contractor – it being the responsibility of the subsequent contractor to convert the format the State Data specified in this Contract to any different format); and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Contract is automatically extended through the end of the Transition Period.

24.4 Survival. This **Section 24** survives termination or expiration of this Contract.

25. **Stop Work Order**. The State may, at any time, order the Services of Contractor fully or partially stopped for its own convenience for up to ninety (90) calendar days at no additional cost to the State. The State will provide Contractor a written notice detailing such suspension (a "**Stop Work Order**"). Contractor must comply with the Stop Work Order upon receipt. Within 90 days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate this Contract as provided in Section 24. The State will not pay for any Services, Contractor's lost profits, or any additional compensation during a stop work period.

26. **Contractor Representations and Warranties**.

26.1 Authority. Contractor represents and warrants to the State that:

(a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;

(c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and

(d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor, its legal successors in interest and permitted assignees in accordance with its terms.

26.2 Bid Response. Contractor represents and warrants to the State that:

(a) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other bidder to the RFP; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;

(b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's Bid Response, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

(c) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous five (5) years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

(d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

26.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(d) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable Law;

(ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or

(iii) require the provision of any payment or other consideration to any third party;

(e) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software or Documentation as delivered or installed by Contractor does not or will not knowingly:

(i) infringe, misappropriate or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable Law;

(f) as provided by Contractor, the Software does not or will not at any time during the license term contain any:

(i) Harmful Code; or

(ii) Open-Source Components or operate in such a way that it is developed or compiled with or linked to any Open-Source Components, other than Open-Source Components specifically described in the Statement of Work.

(g) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and

(h) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(i) when used in the Hosting Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all material respects, in conformity with this Contract and the Documentation; and

(j) no Maintenance Release or New Version, when properly installed by Contractor in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

26.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THIS CONTRACT.

27. **Indemnification**

27.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all third party actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including reasonable outside attorney's fees incurred to establish the right to indemnification), arising out of or relating to: (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract; (b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any Third Party; and (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

27.2 Indemnification Procedure. The State will promptly notify Contractor in writing upon receipt of any third party action or claim if defense and indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the reasonable satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel at its own expense; and to (iv) waive its right to defense and indemnification by retaining control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Contractor has no duty to defend or indemnify the State if the State settles the third party action or claim without obtaining Contractor's prior express written approval from Contractor's

Chief Executive Officer and General Counsel. Any litigation activity on behalf of the State or any of its subdivisions, under this **Section 27**, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

27.3 Infringement Remedies.

(a) The remedies set forth in this **Section 27.3** are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

(b) If any Software or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

(i) procure for the State the right to continue to use such Software or component thereof to the full extent contemplated by this Contract; or

(ii) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Software and all of its components non-infringing while providing fully equivalent features and functionality.

(c) If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(i) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under the Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and

(ii) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to six (6) months to allow the State to replace the affected features of the Software without disruption.

(d) If Contractor directs the State to cease using any Software under **subsection (c)**, the State may terminate this Contract for cause under **Section 24.1**.

(e) Contractor will have no liability for any claim of infringement to the extent resulting from:

(i) Contractor's compliance with any designs, specifications, or instructions of the State; or

(ii) modification of the Software by the State without the prior knowledge and approval of Contractor; or

(iii) combination of the Software by the State with any other product, service or item not provided by Contractor; or

(iv) the State's continued use of the Software after Contractor notified the State and offered the State replacement non-infringing software;

unless the claim arose against the Software independently of any of the above specified actions.

28. **Damages Disclaimers and Limitations.**

28.1 Disclaimer of Damages. NEITHER PARTY WILL BE LIABLE TO THE OTHER, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

28.2 Limitation of Liability. IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED GREATER OF (I) $5,000,000.00 (II) FEES UNDER THIS CONTRACT FOR THE PREVIOUS 12 MONTHS DURING WHICH THE INCIDENT OCCURRED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

29. **Records Maintenance, Inspection, Examination, and Audit**.

29.1 Right of Audit. The State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain, and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for four (4) years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

29.2 Right of Inspection. Within ten (10) calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within forty-five (45) calendar days.

29.3 Application. This **Section 29** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract, along with such parties' legal successors in interest and permitted assignees.

30. **Insurance**

30.1 Required Coverage.

(a) **Insurance Requirements.** Contractor must maintain the insurances identified below and is responsible for all deductibles. All required insurance must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by an company with an A.M. Best rating of "A" or better and a financial size of VII or better.

Insurance Type	Additional Requirements
Commercial General Liability Insurance	
Minimal Limits: $1,000,000 Each Occurrence Limit $1,000,000 Personal & Advertising Injury Limit $2,000,000 General Aggregate Limit $2,000,000 Products/Completed Operations Deductible Maximum: $50,000 Each Occurrence	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 2010 07 04 and CG 2037 07 0.
Umbrella or Excess Liability Insurance	
Minimal Limits: $5,000,000 General Aggregate	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds.
Workers' Compensation Insurance	

Minimal Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimal Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimal Limits: $2,000,000 Each Occurrence $2,000,000 Annual Aggregate	Contractor must have their policy: (1) endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds; and (2) cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

(b) The minimum limits are not intended, and may not be construed to limit any liability or indemnity of Contractor to any indemnified party or other persons.

(c) If any of the required policies provide claim-made coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of contract work; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the contract of work; and (c) if coverage is canceled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

(d) Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or purchase order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

30.2 Non-waiver. This **Section 30** is not intended to and is not be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

31. **Dispute Resolution**.

31.1 Unless otherwise specified in the Statement of Work, the parties will endeavor to resolve any Contract dispute in accordance with **Section 31** (the "**Dispute Resolution Procedure**"). The initiating party will reduce its description of the dispute to writing (including all supporting documentation) and deliver it to the responding party's Project Manager. The responding party's Project Manager must respond in writing within five (5) Business Days. The initiating party has five (5) Business Days to review the response. If after such review resolution cannot be reached, both parties will have an additional five (5) Business Days to negotiate in good faith to resolve the dispute. If the dispute cannot be resolved within a total of fifteen (15) Business Days, the parties must submit the dispute to the parties' Contract Administrators. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

31.2 Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' Contract Administrators, and either Contract Administrator concludes that resolution is unlikely, or fails to respond within fifteen (15) Business Days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This **Section 31** does not limit the State's right to terminate this Contract.

32. **General Provisions**

32.1 Force Majeure.

(a) Force Majeure Events. Subject to **Subsection (b)** below, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached this Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

(b) State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under this Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate this Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the State terminates this Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under this Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

32.2 Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents to provide further assurances and perform such acts as may be necessary to give full effect to the terms of this Contract.

32.3 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for or bind the other party in any manner whatsoever.

32.4 Media Releases. News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates must not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

32.5 Notices. All notices, requests, consents, claims, demands, waivers and other communications under this Contract must be in writing and addressed to the parties as follows (or as otherwise specified by a party in a notice given in accordance with this **Section 32.5**):

If to Contractor:

Doug Meier, Sr.

5515 East La Palma Avenue, Suite 100

Anaheim, California 92807

Email: douglas.meier@morpho.com

Attention: Doug Meier, SR. Program Manager

If to State:

Simon Baldwin

525 W. Allegan, 1st Floor, Lansing, MI

Email: BadwinS@michigan.gov

Attention: Simon Baldwin, Category Specialist, IT

Notices sent in accordance with this **Section 32.5** will be deemed effectively given: (a) when received, if delivered by hand (with written confirmation of receipt); (b) when received, if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by e-mail (with confirmation of transmission), if sent during normal business hours of the recipient, and on the next Business Day, if sent after normal business hours of the recipient; or (d) on the fifth (5^{th}) day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid.

32.6 Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

32.7 Assignment. Contractor may not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this Contract, in each case whether voluntarily, involuntarily, by operation of law or otherwise, without the State's prior written consent. The State has the right to terminate this Contract in its entirety or any Services or the Statement of Work hereunder, pursuant to **Section 24.1**, if Contractor delegates or otherwise transfers any of its obligations or performance hereunder, whether voluntarily, involuntarily, by operation of law or otherwise, and no such delegation or other transfer will relieve Contractor of any of such obligations or performance. For purposes of the preceding sentence, and without limiting its generality, any merger, consolidation or reorganization involving Contractor (regardless of whether Contractor is a surviving or disappearing entity) will be deemed to be a transfer of rights, obligations, or performance under this Contract for which the State's prior written consent is required. Any purported assignment, delegation, or transfer in violation of this **Section 32.7** is void. Notwithstanding the foregoing, the State consents to this Contract being performed by Contractor's legal successor in interest following Advent International's acquisition of the Morpho security division of companies from the Safran Group. Contractor shall notify State in writing following the closing of the Advent – Safran acquisition and the details of the entity that will be the legal successor in interest to MorphoTrak, LLC. Contractor is responsible for any changes in FEIN numbers and registering for payment with the State.

32.8 No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

32.9 Amendment and Modification; Waiver. No amendment to or modification of this Contract is effective unless it is in writing, identified as an amendment to this Contract and signed by both parties Contract Administrator or higher ranking officer. Further, certain amendments to this Contract may require State Administrative Board Approval. No waiver by any party of any of the provisions of this Contract will be effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Contract, no failure to exercise, or delay in exercising, any right, remedy, power, or privilege arising from this Contract will operate or be construed as a waiver. Nor will any single or partial exercise of any right, remedy, power or privilege under this Contract preclude the exercise of any other right, remedy, power or privilege.

32.10 Severability. If any term or provision of this Contract is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability will not affect any other term or provision of this Contract or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal or unenforceable, the parties hereto will negotiate in good faith to modify this Contract so as to effect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

32.11 Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in the Michigan Court of Claims. Complaints against the State must be initiated in Ingham County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or forum non conveniens. Contractor must appoint agents in Michigan to receive service of process.

32.12 Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to seek equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this **Section 32.12**.

32.13 Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., and the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, et seq., Contractor and its Permitted Subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, or mental or physical disability. Breach of this covenant is a material breach of this Contract.

32.14 Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

32.15 Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

32.16 Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to "intellectual property," and all Software and Deliverables are and will be deemed to be "embodiments" of "intellectual property," for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the "**Code**"). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar Laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate shall become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in the State's possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract. In no event, however, will the State's license rights to the Software be expanded from the limited license to use the Software as expressly provided herein.

32.17 Compliance with Laws. Contractor and its Representatives must comply with all applicable laws in connection with this Contract.

32.18 Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

32.19 Entire Agreement. This Contract, together with all Schedules, Exhibits, and the Statement of Work constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Contract, the Schedules, Exhibits, and the Statement of Work, the following order of precedence governs: (a) first, this Contract, excluding its Exhibits and Schedules, and the Statement of Work; and (b) second, the

Statement of Work as of the Effective Date; and (c) third, the Exhibits and Schedules to this Contract as of the Effective Date. NO TERMS ON CONTRACTOR'S OR THE STATE'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE OTHER PARTY OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE PARTIES AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

ARTICLE ISCHEDULE A - STATEMENT OF WORK (SOW)

Glossary	
Name	**Definition**
24x7x365	Means 24 hours a day, seven days a week, and 365 days a year (including the 366th day in a leap year).
ABIS	Automated Biometric Identification System
Additional Service	Means any Services/Deliverables within the scope of the Contract, but not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
ARCH	Add Images to Archive
Blanket Purchase Order	An alternate term for Contract as used in the States computer system.
Business Critical	Any function identified in any Statement of Work as Business Critical.
Business Day	Whether capitalized or not, shall mean any day other than a Saturday, Sunday or State-recognized legal holiday (as identified in the Collective Bargaining Contract for State employees) from 8:00am EST through 5:00pm EST unless otherwise stated.
CAR	Criminal Ten-Print Submission
CCH	Computerized Criminal History
Chronic Failure	Defined in any applicable Service Level Agreements.
CHS	Criminal History System
CJIS	Criminal Justice Information Services
CLEMIS	Courts and Law Enforcement Management System
CNA	Criminal Ten-Print Submission (No Answer Necessary)
CONV	Palm Conversion, Manual Entry
COOP	Continuity of Operations
Days	Means calendar days unless otherwise specified.
DEK	Known Deceased
Deliverable	Physical goods and/or commodities as required or identified by a Statement of Work
DEU	Unknown Deceased
DHS	Department of Homeland Security
DOB	Date of Birth
DTMB	Michigan Department of Technology, Management and Budget
EBTS	Electronic Biometric Transmission Specification
EFS	Extended Feature Set

Environmentally preferable products	A product or service that has a lesser or reduced effect on human health and the environment when compared with competing products or services that serve the same purpose. Such products or services may include, but are not limited to, those that contain recycled content, minimize waste, conserve energy or water, and reduce the amount of toxics either disposed of or consumed.
ERRA	Administrative Transaction Error
ERRI	Image Transaction Error
ERRL	Latent Transaction Error
Error	Synonymous with “Deficiency”
ERRT	Ten-Print Transaction Error
FBI	Federal Bureau of Investigation
FFT	Fast Fourier Transform
FISR	Fingerprint Image Submission Response
Hazardous material	Any material defined as hazardous under the latest version of federal Emergency Planning and Community Right-to-Know Act of 1986 (including revisions adopted during the term of the Contract).
IAFIS	Integrated Automated Fingerprint Identification System
Incident	Any interruption in Services.
ISO	International Standards Organization
IT	Information Technology
JPEG	Joint Photographic Experts Group
Key Personnel	Any Personnel designated as Key Personnel.
KP-LT	Known Palm to Latent
LCMS	Latent Case Management System
LFFS	Latent Friction Ridge Feature Search
LPNQ	Latent Penetration Query
LPNR	Latent Penetration Query Response
MAP	Miscellaneous Applicant Civil
MID	Mobile Identification
MPR	Missing Persons
MSP	Michigan State Police
NEC	NEC Corporation of America, Inc.
New Work	Any Services/Deliverables outside the scope of the Contract and not specifically provided under any Statement of Work, that once added will result in the need to provide the Contractor with additional consideration.
NFF	National Fingerprint File
NFIQ	NIST Fingerprint Image Quality

NFUF	Non-Federal Applicant User Fee
NGI	Next Generation Identification
NIST	National Institute of Standards and Technology
ORI	Originating Agency
Ozone-depleting substance	Any substance the Environmental Protection Agency designates in 40 CFR part 82 as: (1) Class I, including, but not limited to, chlorofluorocarbons, halons, carbon tetrachloride, and methyl chloroform; or (2) Class II, including, but not limited to, hydro chlorofluorocarbons
PDF	Portable Data Format
Post-Consumer Waste	Any product generated by a business or consumer which has served its intended end use, and which has been separated or diverted from solid waste for the purpose of recycling into a usable commodity or product, and which does not include post-industrial waste.
Post-Industrial Waste	Industrial by-products that would otherwise go to disposal and wastes generated after completion of a manufacturing process, but do not include internally generated scrap commonly returned to industrial or manufacturing processes.
QC	Quality Check
Recycling	The series of activities by which materials that are no longer useful to the generator are collected, sorted, processed, and converted into raw materials and used in the production of new products. This definition excludes the use of these materials as a fuel substitute or for energy production.
Reuse	Using a product or component of municipal solid waste in its original form more than once.
RISC	Repository for Individuals of Special Concern
RPIS	Rapid Fingerprint Identification Search
RPISR	Rapid Fingerprint Identification Search Response
Services	Any function performed for the benefit of the State.
Shall	Shall is equivalent to must where referenced in this Contract
SID	State Identification Number
SNAP	Statewide Network of Agency Photos
Source reduction	Any practice that reduces the amount of any hazardous substance, pollutant, or contaminant entering any waste stream or otherwise released into the environment prior to recycling, energy recovery, treatment, or disposal.
SRE	Submission Results-Electronic
SRL	Search Results-Latent
State Location	Any physical location where the State performs work. State Location may include state-owned, leased, or rented space.
Subcontractor	A company Contractor delegates performance of a portion of the Services to, but does not include independent contractors engaged by Contractor solely in a staff augmentation role.
TCN	Transaction Control Number
TD	Ten-Print Delete

TD-P	Ten-Print Delete Palm
TD-S	Ten-Print Deletion Slap
TI	Ten-Print Inquiry
TLI	Ten-Print to Latent Inquiry
TOT	Type of Transaction
TPIS	Ten-Print Fingerprint Image Search
TP-LT	Ten-Print to Latent
TPRR	Ten-Print Rap Sheet Response
TP-TP	Ten-Print to Ten-Print
TU	Ten-Print Update
UAF	User Authentication File
ULM	Unsolved Latent Match
ULW	Universal Latent Workstation(s)
Unauthorized Removal	Contractor's removal of Key Personnel without the prior written consent of the State.
UPS	Uninterruptable Power Supply
Waste prevention	Source reduction and reuse, but not recycling.
Waste reduction and Pollution prevention	The practice of minimizing the generation of waste at the source and, when wastes cannot be prevented, utilizing environmentally sound on-site or off-site reuse and recycling. The term includes equipment or technology modifications, process or procedure modifications, product reformulation or redesign, and raw material substitutions. Waste treatment, control, management, and disposal are not considered pollution prevention, per the definitions under Part 143, Waste Minimization, of the Natural Resources and Environmental Protection Act (NREPA), 1994 PA 451, as amended.
Workstation	Fully functioning ABIS workstation and workstation peripherals as defined in paragraph 1.001, subparagraph 1, 2 and 3, this SOW and paragraph 2a, b and c, Schedule F - Terms for On-Site Workstations.
Work in Progress	A Deliverable that has been partially prepared, but has not been presented to the State for Approval.
Work Product	Refers to any data compilations, reports, and other media, materials, or other objects or works of authorship created or produced by the Contractor as a result of an in furtherance of performing the services required by this Contract.

(a) 1.000 Project Identification

1.001 Project Request

The Michigan State Police (MSP) with assistance of the Department of Technology Management and Budget (DTMB), has issued this Contract to provide a web enabled, Automated Biometric Identification System (ABIS) solution as well as any hardware, software and peripherals that are need to support the new ABIS solution.

MorphoTrak LLC must provide the solution as a vendor owned and supplied ABIS solution and Vendor hosted at Vendor location, including disaster recovery site. This solution must have two (2) facilities meeting CJIS security requirements and meeting industry standards for disaster recovery requirements, this must include appropriate location and distance between facilities.

In order to support the ABIS, the Vendor must provide ABIS workstations and workstation peripherals and ongoing support of the following:

1. ABIS Ten-print Terminal
    - Desktop(11)
    - Laptop (2) for remote work
    - Flatbed scanners (11)
    - High Speed Duplex Scanner (2) Equivalent or better than Epson Expression 10000 XL
    - Black and White Printers (11)
    - Color Network Printer (1)
2. ABIS Latent Terminal
    - Desktop (18)
    - Latent Flatbed Scanner (18)
    - Latent Camera (18)
    - Color Printer (17)
3. Card Print
    - Desktop, if necessary (1)
    - Printer (1)

During the Term of the Contract, Contractor will be responsible for the maintenance and support of the above listed equipment in accordance with the SLA without any further cost to the State.

1.002 Background

The State of Michigan installed the first Michigan Automated Fingerprint Identification System (AFIS) in 1988. This system services fingerprint identification, both latent and ten-print, for the entire state. At the time of installation, Michigan converted 724,000 ten-print fingerprint cards. Today, Michigan has over 3.2 million persons on the AFIS, with about 4.5 million records on the AFIS archive system.

The ABIS is a critical component of MSP's existing infrastructure. The ABIS is responsible for managing the arrest, fingerprint, mug shot and message flow between the State of Michigan and the FBI's AFIS, Michigan's Criminal History System (CHS), Michigan's Statewide Network of Agency Photos (SNAP), for all of the 620 plus law enforcement agencies of Michigan and all of the public and private entities that are required to submit fingerprint checks by law.

Michigan has 20 sites across the state that have ABIS terminals to access ABIS for ten-print and/or latent searches that are used to search the state and Federal Bureau of Investigation (FBI) AFIS. These sites include MSP Headquarters Lansing, Michigan which houses the ABIS and ten-print operations, seven MSP Labs, and twelve local agency ABIS Latent sites. Michigan has over 600 live scan devices connected to the state ABIS.

Contractor will implement, and support a new Automated Biometric Identification System (ABIS) that will:

- Provide a biometric and web enabled, standards-based open architecture that:
    - Enables implementation of state-of-the-art ABIS (e.g., ten-print, palm print, latent, mobile fingerprint identification searches) applications and workflows including integration with the current live scan fingerprint, mug shot, and Criminal History systems. See Appendix 1 Existing Systems Report.
    - Enable and support Latent FBI AFIS access, searching, verification, and retrieval.
    - Enables the incremental enhancements of applications and workflows for but not limited to, fingerprinting, iris and voice biometric tool sets.
    - Allows, to the maximum extent possible, use of nonproprietary hardware, database software, and open-standards application software interfaces.
    - Stores integrated subject biometric data (captured via the various biometric tool sets) that enables online inquiries and reporting based on integrated subject biometric data.
- Be sized for planned growth.
- Utilize ANSI/NIST/FBI/MSP record constructs.
- Conform to national and international biometric standards.
- Provide configurable administrative controls.
- Manage the orchestration and transaction integrity of all subcomponents of the ABIS Solution.
- Manage and control biometric data using subject biometric identifiers as keys.
- Provide efficient and cost-effective storage and retrieval.
- Detect and notify defined MSP staff promptly when systems, applications, equipment, or networks are interrupted or when there is a loss of power.
- Provide for migration of fingerprints, palm and latent, and mug shots from already existing State systems.

(b) 1.100 Scope of Work and Deliverables

(A) 1.101 In Scope

The Scope of Work to be provided by the Contractor under the Contract consists of two phases each detailed in its own section of this Statement of Work (SOW):

I. System Implementation
    - Project Management
    - Functional and Technical Requirements
    - System Hardware and Software Design and Development
    - Implementation
    - Training

II. System Operations & Support

- Customer Support
- Hosting
- Maintenance and support

All work performed under the Contract shall be performed within the territory of the United States and shall be performed by United States citizens or lawful permanent residents of the United States. No State data (including without limitation biometric data, identity history data, biographic data, property data, and case/incident history data, as defined in the Criminal Justice Information Services (CJIS) Security Policy) or information shall be communicated to anyone who is not a United States citizen or lawful permanent resident of the United States, or without written permission of MSP. State data shall not be stored, accessed from, or transmitted to anyone without State's written permission provided in advance. State shall have the right, from time to time, to designate certain subsets of State data as being subject to additional storage, access, or transmission restrictions at its sole discretion.

Contractor shall perform, complete, and deliver all work, however denoted, as set forth in this SOW. Also defined herein are those tasks and subtasks that involve participation of both Contractor and State. Unless otherwise specified as an obligation of the State, Contractor shall perform all tasks and subtasks and provide all deliverables as defined herein. A deliverable shall only be deemed complete upon State's approval and acceptance, irrespective of the number of attempts it takes Contractor to provide a successful deliverable.

All of the Requirements, whether specifically referenced or not in this SOW, shall apply to Contractor's deliverables under the resultant Contract.

A more detailed description of the software, services (work) and deliverables sought for this project is provided in Section 1.104, Work and Deliverables.

(B) 1.102 Out Of Scope

Staff Augmentation

(C) 1.103 Environment

The links below provide information on the State's Enterprise information technology (IT) policies, standards and procedures which includes security policy and procedures, eMichigan web development, and the State Unified Information Technology Environment (SUITE).

All services and products provided under this Contract must comply with all applicable State IT policies and standards. Contractor is required to review all applicable links provided below and state compliance in their response.

Enterprise IT Policies, Standards and Procedures:
http://michigan.gov/dtmb/0,4568,7-150-56355_56579_56755---,00.html

All software and hardware items provided by the Contractor must run on and be compatible with the DTMB Standard Information Technology Environment. Additionally, the State must be able to maintain software and other items produced as the result of the Contract. Therefore, non-standard development tools may not be used unless approved by DTMB. The Contractor must request, in writing, approval to use non-standard software development tools, providing justification for the requested change and all costs associated with any change. The DTMB Project Manager must approve any tools, in writing, before use on any information technology project.

It is recognized that technology changes rapidly. The Contractor may request, in writing, a change in the standard environment, providing justification for the requested change and all costs associated with any change. The State's Project Manager must approve any changes, in writing, and DTMB, before work may proceed based on the changed environment.

Enterprise IT Security Policy and Procedures:

http://www.michigan.gov/documents/dmb/1210.32.pdf

http://www.michigan.gov/documents/dmb/1325_193160_7.pdf

http://www.michigan.gov/documents/dmb/1335_193161_7.pdf

http://www.michigan.gov/documents/dmb/1340_193162_7.pdf

The State's security environment includes:

- DTMB Single Login.
- DTMB provided SQL security database.
- Secured Socket Layers.
- SecureID (State Security Standard for external network access and high risk Web systems)

DTMB requires that its single - login security environment be used for all new client-server software development. Where software is being converted from an existing package, or a client-server application is being purchased, the security mechanism must be approved in writing by the State's Project Manager and DTMB Office of Enterprise Security.

ADA Compliance:
Contractor shall comply with and adhere to the Accessibility Standards of Section 508 of the Rehabilitation Act of 1973, including any more specific requirements set forth in an applicable Statement of Work. See DTMB Policy at
http://www.michigan.gov/documents/dmb/1650.00_209567_7.pdf?20151026134621.

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. The State is requiring that Contractor's solution conform, where relevant, to level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. Contractor may provide a description of conformance with the above mentioned specifications by means of a completed Voluntary Product Accessibility Template for WCAG 2.0 (WCAG 2.0 VPAT) or other comparable document. Contractor may consider, where relevant, the W3C's Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT) for non-web software and content. Any additional compliance requirements shall be specified in the Statement of Work.

The State Unified Information Technology Environment (SUITE):
Includes standards for project management, systems engineering, and associated forms and templates – must be followed: http://www.michigan.gov/suite

Agency Specific Technical Environment

Specifications, Standards, and Guides
The MSP uses a Windows 7 environment. Currently use a Local Government Network (LGNet) connection to provide the secure connection to the Michigan AFIS.

Interfaces, required for the successful implementation of the system, are documented in the Appendix 1 Existing Systems Report. Contractor shall maintain all and any interfaces that are required to support this system.

As part of Maintenance support, Contractor shall maintain Interfaces with state and national services through the Wide Area Network (WAN) using FBI EBTS-conformant transactions and international transactions via the CJIS gateway.

Data transmitted between an AFIS terminal and the central AFIS must have the ability to be encrypted in flight/transit. Encryption in flight should be the most current FIPS certification (currently 140-2) with the certificate numbers provided upon audit. Additionally, there should be FBI approved print quality printers able to interface with all operations.

The Contractor must comply with the following standards for the new ABIS:

- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) ANSI/NIST-ITL 1-2011 Data Format for the Interchange of Biometric and Forensic Information, dated November 2011.
- Electronic Biometric Transmission Specification (EBTS), IAFIS-DEL-01078-10.4, dated May 25, 2010.
- FBI Criminal Justice Information Services (CJIS) CJISD-ITS-DEL-08140-5.0, CJIS Security Policy, Version 5.3, dated January 2010.
- Michigan Electronic Biometric Transmission Specification (EBTS).

Contractor must stay in compliance with the State's current computing environment at no additional cost.

(D) 1.104 Work And Deliverables

I. System Implementation

REQUIREMENTS

Specific requirements are also listed in Schedule A, Attachment 1 – Requirements.

FUNCTIONAL REQUIREMENTS

This section lists the suggested baseline functional requirements for the new MSP ABIS environment. These baseline requirements are broken down into each of the typical functional areas of biometric identification, including ten-print, National Fingerprint File (NFF) compliance, and Ten-print to Latent Inquiry (TLI), Latent Inquiry (LI), ABIS latent entry management, and rapid/mobile ID.

1. Ten-Print Requirements

Ten-print identification service specifications are organized under one of the four categories below.

Input – Ten-print identification transaction data is transmitted as Electronic Biometric Transmission Specification (EBTS) files or paper forms (e.g., inked cards) to the ABIS for preprocessing. Inked forms will be converted to appropriate EBTS transactions, and they will be handled by the requirements below.

Processing – The ABIS processes identification transactions received from the various live scan devices and external systems. The various biometric modality data (fingerprint and palm prints) will be sent to the appropriate back-end matchers.

Output – The ABIS prepares responses to all transactions received (from live scans, other systems, etc.). If the transaction failed to pass the various checks above, it will have already produced an error message in the Input stage, above.

NFF Compliance – The ABIS solution ingests and processes transactions and produces all of the requisite responses in line with participation in the NFF system.

MSP AFIS Transactions Supported

TOT	Transaction Name
CAR	Criminal Ten-Print Submission
MAP	Miscellaneous Applicant Civil
TPIS	Ten-Print Fingerprint Image Search (Mobile ID)
DEK	Known Deceased
DEU	Unknown Deceased
MPR	Missing Persons
AMN	Amnesia Victim
CNA	Criminal Ten-Print Submission (no answer necessary)
NFUF	Non-Federal Applicant User Fee
RPIS	Rapid Fingerprint Identification Search
RPISR	Rapid Fingerprint Identification Search Response

TOT	Transaction Name
CONV	Palm Conversion, Manual Entry
ARCH	Add Images to Archive
FIS	Biometric Image Submission
ERRI	Information Transaction Error Response
ERRT	Tenprint Transaction Error Response
ERRA	Administrative Transaction Error Response

2. Ten-Print to Latent Inquiry Service Requirements

All identification transactions containing fingerprint or palm print records will be automatically searched against the unsolved latent. This search occurs in the course of the input phase of ten-print identification services. TLI identification service specifications are organized under one of the three categories below.

Input – The input TOTs are listed in the table above. They can originate within ABIS or the FBI's Next Generation Identification (NGI) system. If they start within ABIS, they are sent to the appropriate owner of the unsolved latent print. If they originate at the FBI, they are sent to ABIS and in turn distributed to the owner where the latent was enrolled in the unsolved latent file.

Processing – If an unsolicited latent match response is received from the FBI, it is logged, added to the ANSI/NIST Archive, and forwarded to the appropriate owner. It is anticipated that only one candidate will be returned per unsolved latent match (ULM) transaction.

Output – The ABIS will permit the examiner to document the results of the examination of the ULM and associated friction ridge material.

3. Latent Inquiry Service Requirements

Latent inquiry (LI) searches use latent fingerprint and palm print samples collected at crime scenes, disaster victim fingerprints, and fingerprints from deceased subjects collected by morgues, to determine whether the subject has been previously encountered and enrolled in the ABIS. External agencies, using Universal Latent Workstations (ULWs), can also submit LI searches. LI identification service specifications are organized under one of the four categories below.

Input

Collection will typically start with:

- A crime scene technician or investigator collecting images or other friction ridge samples at a crime scene.
- A forensic scientist examining an item of evidence (e.g., an unfired round in a gun) and imaging a latent fingerprint or palm print.

- A medical examiner collecting friction ridge samples from a deceased person.
- A disaster response team providing services for instances where fingerprints are typically collected from whatever portions of a hand that can be found and used – this is different from an Identification Service search of good quality ten-prints collected at the morgue post mortem using the known deceased (DEK) or unknown deceased (DEU) TOT for a TEN-PRINT TO TEN-PRINT (TI) Identification search.

In each case, along with an image, other case-related information will be supplied, such as date collected, unique identification number of the image or sample, the point of contact where results should be reported, collection location, crime type, or morgue case type, etc. The images and information will be entered though a workstation and transmitted to the ABIS via a latent entry. The ABIS will provide tracking of the processing of the latent through all searches to include maintaining a log of searches, image processing, candidates, etc. The ABIS will provide the ability for examiners to query status and other attributes of latent submittals and cases as well as to return to open cases as often and whenever they see fit. Transactions entered through ULWs from external agencies will be entered through the ABIS for tracking and reporting purposes.

Processing

The examiner will forward the latent transactions with the impression and tracking information to the ABIS for forensic processing as a Latent Friction Ridge Feature Search (LFFS) transaction type.

- The ABIS will queue the latent transaction for a latent examiner to select and process, or if the transaction originated from a ULW or cross-jurisdictional partner, it will be auto-launched without any examiner action – as a lights-out remote search. Since the ABIS will not know whether the remote submitter made an identification, these submittals will not be automatically forwarded to the FBI; rather, the agency will have to resubmit them for forwarding.
- The examiner will perform pre-search steps (rotate, crop, mark, and edit minutiae, etc.) before submitting a search. This will be performed using latent editing software integrated into the ABIS software, to include Photoshop.
- The examiner will be able to limit the search by crime type, finger or palm position, geographical region where the crime was committed, and other traditional parameters or elect to use no search limitations. The ABIS will search the record against known records as well as against unsolved latent records. The known record files for latent searches to run against, sometimes referred to as the “latent cognizant files,” will contain up to three instances of known fingerprints and one of palm prints enrolled in the system rather than just a single set of best images.

Output

The ABIS will prepare responses to all LI transactions received. The examiners will be given the opportunity to forward unsolved latents to the FBI, add them to the ABIS unsolved latent file, edit and resubmit them, or save them for future work. If there is a match, then the identity of the subject is returned to the submitting agency. If there is no match and the latent sample is selectively added to the unsolved latent file, it will be reverse-searched against all subsequent transactions that include fingerprint and palm print data.

ULW Functionality

The ABIS will support and process latent transactions, as required and requested, as ULW transactions to the FBI and other biometric identification systems.

4. Rapid/Mobile ID Requirements

This workflow is for the rapid searching of the ABIS and, in turn, the FBI. If no identity is determined at the ABIS, the transaction can be submitted to the FBI as a ten-print fingerprint image search (TPIS), for a 2-minute FBI turnaround, against the entire NGI repository. Rapid/mobile ID service specifications are organized under one of the three categories below.

Input – The rapid/mobile data will be transmitted as EBTS files. These will be rapid turnaround transactions set to the highest priority by the ABIS, if not already set as such by the submitting device. In the ABIS all records will be parsed for compliance with the EBTS. Transactions that fail the parsing test will be logged and returned to the submitting device with an ERRT response.

Processing – The ABIS will process rapid/mobile ID transactions received at the highest system priority level. The fingerprint images will be feature extracted and searched "without enrollment." Matcher results will be made available via EBTS responses. Based on the submittal data, the transaction may or may not be forwarded to the FBI for further searching against its NGI system.

Output – The ABIS will prepare responses to all rapid/mobile ID transactions received. If the transaction failed to pass the various checks above, then it will have already produced an error message, pursuant to the EBTS.

5. General ABIS Requirements

See Schedule A, Attachment 1, Requirements for general system functional requirements.

TECHNICAL REQUIREMENTS

This section provides the system technical requirements for the new ABIS environment. The technical requirements are organized as follows:

- Capacity requirements – capability to store some number of a class of items such as:
  - Enrolled transactions.
  - Searchable feature-based data sets online in matchers.
- Performance requirements – number of events and units of time such as:
  - Throughput as expressed in transactions turned around in a period of time.
  - Average transaction response time.
- Accuracy requirements – matcher capability.
  - Ten-print to ten-print accuracy.
  - Ten-print to latent accuracy.
  - Latent to ten-print accuracy.
  - Palm latent to known palm accuracy.
  - Criminal known palm to latent accuracy.
- Safety requirements.
- Security requirements.
- Environmental requirements – such as uninterruptible power supplies (UPSs) and office environment noise levels
- Hardware requirements – capacities and performance of workstations and printers.
- Backup/recovery/availability requirements.
- Interface requirements.
- Standards requirements.
- Administrative functions requirement.

The subsections that follow delineate these requirements and will refer to the tables provided below.

1. Storage Capacity Requirements

Storage capacities are relevant to the following areas of the ABIS architecture, including:

ANSI/NIST Archive.
The templates/features loaded in the matchers.

Current MSP Sizing and Growth

Ref.	Record Type	01/2015 Number	Historical Annual Growth Rate
1	Ten-Print – Card	4,010,992	7%
2	Ten-Print – Palm	736,614	35%
3	Ten-Print – Slap	2,264,798	20%
4	Latent – Card	59,040	n/a
5	Latent – Case	40,416	n/a
6	Latent – Palm	3,577	n/a
7	Archive – TCNs	6,786,346	12%
8	Archive – SIDs	3,288,952	7%
9	Archive – SIDs Deleted	20,497	n/a

The ABIS will be designed to accommodate an ANSI/NIST Archive of all input and output transactions through the life of the contract. The addition of response TOTs will make the capacity requirements larger than the storage of input transactions only. Note that most response transactions generated by the ABIS are smaller than the corresponding input transactions. The vendor will have to perform the appropriate design analysis to determine the design requirements in terms of terabytes as a function of transaction type using the data specified in this document.

At the initial operating point of the ABIS, all existing records will have been loaded into the ABIS, to include loading them into the ANSI/NIST Archive, the matchers, any other repositories, and the master index.

2. Performance Requirements

The ABIS will meet performance (throughput and response time) requirements as specified.

Throughput Requirements

The ABIS throughput requirements cover all three of the primary current types of services:

- Ten-print services
- Archive Services
- Latent services
- Rapid/mobile ID services.

MSP AFIS Transactions Supported

TOT	Transaction Name
CAR	Criminal Ten-Print Submission
MAP	Miscellaneous Applicant Civil
TPIS	Ten-Print Fingerprint Image Search (Rapid/Mobile ID)
DEK	Known Deceased
DEU	Unknown Deceased
MPR	Missing Persons
AMN	Amnesia Victim
CNA	Criminal Ten-Print Submission (no answer necessary)
NFUF	Non-Federal Applicant User Fee
RPIS	Rapid Fingerprint Identification Search
RPISR	Rapid Fingerprint Identification Search Response

The ABIS throughput rates will grow over the life of the system. The following table projects the growth for the initial contract:

MSP AFIS Transaction Counts and Throughput

Ref.	MSP Record Type	Peak Hour	Per Day	Per Year
1	Ten-Print Submissions	500	5,500	2,000,000
2	Ten-Print Cold Searches	275	2,200	n/a
3	Ten-Print to Latent Inquiries	500	5,500	n/a
4	Palm Submissions	n/a	1,000	n/a
5	Latent Inquiries	n/a	100	n/a
6	Latent Palm Inquiries	n/a	50	n/a
7	Mobile ID Inquiries	n/a	1,500	n/a
8	Mobile ID Inquiries	n/a	3,000	n/a

The throughput requirements are defined in the table below. Throughput requirements are for concurrent ingestion and processing of identification, forensic, and tactical transactions.

Response Time Requirements
The response time for ABIS transactions is a function of the transaction type (identification, forensic, and tactical [rapid/mobile ID]). The response times do not include any human interaction times.

The table below provides the response times per class of transaction, while the Response Time Requirements table defines the requirements for providing these response times.

Response Times Per Transaction Type

Transaction Class Type	Response Requirement Under Peak Load
Ten-print to Ten-Print (TI)	5 minutes
Ten-print to Latent (T/LI)	20 minutes
Latent to Ten-print (LI)	20 minutes
Palm Latent to Know Palm	20 minutes
Know Palm to Latent Palm	20 minutes
Rapid/Mobile ID	2 minutes

The response time requirements stated below are for 95 percent of the transactions in any period, as there are always some outliers caught up in a data processing system and they should not be considered in the performance testing. Testing will be done against the initial repository load using a test set with a mixture of all transaction types at the peak rates calculated using the table above.

3. Accuracy Requirements

The matcher accuracy will vary as a function of the class of service (identification, forensic, and tactical (rapid/mobile ID) and the quality of the input images. Identification service accuracy requirements are typically higher than those for forensic services, as the input images are typically of better quality for live scan enrollments than for latent lifts.

Accuracy terms-of-art have been undergoing an evolutionary change for the past few years. While reliability, true accept rate, false reject rate, and other terms are often used for access control systems and other biometric modalities (such as facial recognition), a consensus has developed in the international standards community around the terms ***true match rate*** and ***failure to match rate*** when discussing friction ridge matching on a large scale.

For this project, accuracy will include three accuracy terms:

True Match Rate – The probability that a true match will be found when it is in the background reference file (also known as a repository). This term replaces older terminology such as matcher reliability or true accept rate.

Failure to Match Rate – The probability that a search will not return a true match when the true match is in the reference file. The failure to match rate is 100 percent minus the true match rate. While not explicitly stated in the requirements, it will be calculated during testing and reported.

Selectivity – The number of candidates that will be examined to determine the true match rate. While the system administrators will be able to selectively change the length of candidate lists by transaction class and by threshold scores during testing, system accuracy will be measured using the selectivity numbers shown in the table that follows.

Accuracy Rates by Transaction Type

Transaction Type	Selectivity	True Match Rate
TEN-PRINT TO TEN-PRINT (TI)	1	99.9%
Mobile ID (with fewer than 10 prints)	8	99.9%
TEN-PRINT TO LATENT (T/LI)	10/25	93%/100%
Criminal KP-LT	10/25	93%/100%
LATENT TO TEN-PRINT (LI)	10/25	93%/100%
Palm LT-KP	10/25	93%/100%

Contractor will collaborate with MSP to create a test data set that is representative of typical activities in the current environment.

Contractor acknowledges the MSP’s stated requirement for a true match rate of 93% / 100% for latent test searches. Contractor will meet the required latent accuracy assuming the criteria below are met, using the following characteristics for the test data set:

- For Ten-print vs Ten-print (TPTP) the number of search records should be 10,000 records, with 50 percent of those searches with mated records in the background tenprint database.
- For Latent vs Tenprint (LTTP) the number of search records should be 100 records each with an expected mate in the background ten-print database. The NIST Fingerprint Image Quality (NFIQ) average score should be one for mated tenprints, and a minimum 15 simultaneous minutiae for mated records.
- For Palm vs Latent Palm (PPUP) the number of search records should be 100 records each with a mated record in the unsolved latent palm database and a minimum 15 simultaneous minutiae for mated records.

- For Tenprint vs Latent (TPUL) the number of search records should be 100 records each with a mated record in the unsolved latent finger database and a minimum 15 simultaneous minutiae for mated items. The NFIQ average score of mated tenprints should be one.

MorphoBIS includes a tool for testing system accuracy for both lights-out matching, and best practices accuracy testing. Accuracy test data is stored in a separate accuracy test database. This data is injected into the MSP MorphoBIS system for accuracy testing and is removed from the system after test completion. The accuracy test tool is set up when the system is configured. The database with the accuracy test tool contains the following:

- Search prints (agreed upon by Contractor and the MSP), which contain both friction ridge images and expert encoded features. The expert encoded features are reserved for best practices testing.
- Target prints (agreed upon by Contractor and the customer), which contain friction ridge images only.

The following procedure is used to conduct an accuracy test:

- The accuracy test tool injects the target print images into the MorphoBIS database, and the target print images are automatically processed to obtain features. These features are temporarily stored in the MorphoBIS matchers.
- The accuracy test tool injects the search print images into the MorphoBIS workflow, and the search images are automatically processed to obtain features for lights-out searching. The lights-out searches are launched using the automatically generated features, match reports are generated, and the results are collected and compared against the lights-out service levels. The lights-out searches are processed "without add," that is, without adding the search images to the database, and the generated match reports reflect the appropriate selectivity figures.
- The accuracy test tool injects the search print images into the MorphoBIS workflow a second time, but this time including the expert encoded features, applied using best practices. These best practice searches are launched using the expert encoded features, match reports are generated, and the results are collected and compared against the best practices service levels. The best practices searches are processed without add and the generated match reports reflect the appropriate selectivity.
- Since both the lights-out and best practices searches are processed without add, the search prints are not retained in the Contractor database.
- Upon completion of the accuracy tests, the accuracy test tool removes the target print images from the MorphoBIS database and matchers, restoring the system to its original state.

The steps listed above are repeated when the next accuracy test is conducted.

4. Safety Requirements

The intent is to ensure that safe equipment is used and that it is installed properly in terms of grounding (e.g., any power strips used at the ABIS workstations must be certified and be installed and used correctly).

5. Security Requirements

All configuration items that process, transmit, or store digital information delivered as part of the ABIS will require some level of information security, as the system is connected to the FBI's criminal justice network, and the CJIS security requirements must be complied with, including user and administrator login rules, audit trail requirements, and reporting capabilities.

Information security includes ensuring data confidentiality, integrity, and availability – and thus antivirus protection is to be included in the systems to the extent to which commercial antivirus packages are available for the operating systems selected by the vendor.

6. Environmental Requirements

There are ABIS-imposed environmental requirements on all workstations and workstation peripherals such as printers.

The system design will include the capability to meet the following power/voltage conditioning and related availability requirements as well as noise-level requirements. These requirements address sustainment of power during blackouts and brownouts and noise levels in an office environment.

7. Hardware Requirements

This subsection provides the form and fit requirements for the ABIS. The requirements are for the workstations and card printers to be delivered to ABIS sites, to include the locations and number of units per site.

8. Backup/Recovery/Availability Requirements

This subsection provides the backup/recovery/availability requirements for the ABIS. To support these, there are requirements for the ability to backup and restore the system or any of its major data components.

There are two sets of requirements:

- Backup and recovery.
- Availability and restoration.

Backup and Recovery

The ABIS will need to be backed up (data and system configurations) frequently for Continuity of Operations (COOP) considerations. The ABIS shall have a 2 hours maximum of Recovery Point Objective (RPO) and 2 hours maximum of Recovery Time Objective (RTO).

To achieve these requirements, Vendor will use locally and geographically redundant storage solutions for both database and server configurations, so that the database and servers can be restored within the RPO and RTO requirements.
In addition to locally and geographically redundant storage of the database and servers configurations, database backups will be performed on the central site and media will be stored or housed copied off-site from the central site (primary and disaster sites) to the disaster recovery site to increase the likelihood of their availability in case of a natural or man-made disaster. These backup files will be created on the primary site, then moved / copied to the disaster recovery site. The solution will propose and provide backup services and media utilizing the most contemporary means and medium available.

Service Availability and Restoration Requirements

Given that the ABIS will operate under a COOP plan to include a disaster recovery site, it is anticipated that ABIS services will have a very high level of continuous availability.

The availability of all ABIS services is set at 99.8 percent per month without any allowance beyond 99.8 percent for scheduled outages or switchover from the primary to the disaster recovery site (or vice versa). Service availability of 99.8 percent leaves a little less than 90 minutes a month for service outages at the ABIS level. The vendor is free to roll scheduled outages between the primary and disaster recovery sites to preclude as many ABIS service outages as possible. The purposes of the disaster recovery site are to:

- Provide for fast recovery for failed equipment and localized power outages at the primary site – 99.8 percent availability is a requirement. This includes provision of any and all necessary power conditioning and alternative power sourcing to maintain the availability requirement.
- Provide the basis for recovery of services in the event of a catastrophic failure at the primary site (fire, explosion, radioactive contaminations, etc.).

9. Interface Requirements

The key interfaces/exchanges that are operational and required in the MSP environment are described in the table below.

Ref.	Interface/Exchange	Interface Specifications Available?	Reference Document
External Systems			
1	DHS US-Visit	Yes	FBI EBTS
2	FBI NGI	Yes	FBI EBTS
3	CLEMIS	Yes	Michigan EBTS (June 25, 2014)
Internal Systems			

Ref.	Interface/Exchange	Interface Specifications Available?	Reference Document
4	CCH	Yes	Technical System Design Document
5	SNAP	Yes	DataWorks Plus Document
6	Live Scan Terminals	Yes	Michigan EBTS
7	Latent Terminals	Yes	Michigan EBTS, FBI EBTS
8	Mobile ID	Yes	MSP Mobile ID Submission to MSP and FBI Repository for Individuals of Special Concern (RISC)

10. Standards Requirements

The current standards and models that are applicable, operational, and required in the current IAFIS environment include:

- Michigan Electronic Biometric Transmission Specification (EBTS), June 25, 2014.
- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- Electronic Biometric Transmission Specification (EBTS), IAFIS-DOC-01078-9.4.
- IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- NIST Best Practice Recommendation for the Capture of Mugshots. Version 2.0. September 23, 1997.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.0, CJIS Security Policy, Version 5.3, dated 8/4/2014.

11. Administrative Functions Requirements

Regardless if the Contractor is Hosting or not, the Contractor will be responsible for back up and restoration. The system administrators (vendor staff and MSP staff) will be responsible for ensuring the integrity of information in the system, creating and maintaining user accounts, exporting files in response to ad hoc requests, and generating reports, as appropriate.

In addition to the normal administrative tasks described further below, there is one added set of requirements associated with testing new and modified TOTs.

The TOT testing specifications are organized under one of these three categories:

Input – ABIS administrators use this workflow to test new and modified TOTs. The TOTs can be any of those ingested by or created as output by any other workflow. They may be sent to the ABIS. The format is the normal TOT name with a T appended to it (***T) to signal all systems that it is a test transaction and thus should not be added to any system.

Processing – The ABIS will process locally all test transactions received.

Output – The ABIS will prepare responses to all test transactions received.

This table lists the TOTs associated with this requirement.

<u>Test Transaction TOTs Supported</u>

TOT	Transaction Name
***T	Test transaction version of any workflow TOT.

All test transactions will be parsed for compliance with the ABIS EBTS. Transactions that fail the parsing test will be logged and returned with an ERRT response. Successful transactions (i.e., those that pass the parser checks) will be forwarded to the originator.

Administrative tasks will start with a system administrator logging into a workstation connected to the ABIS. The system administrators will deal with system error messages, assist in recovering from problems, and generate problem reports via e-mail, 24/7 help desk calls, or other means.

REPORTS

Reports to be provided are associated with Admin Function 21, (Schedule A, Attachment 1, Requirements, System Administrator Functions, Requirement 21):

Transactions processed on ABIS will include the ability to select from the following display options *by workflow and TOT*:

- Number of transactions received and processed.
- Number of hit/no-hit transactions.
- Number of transactions sent to the FBI (and other national databases), number of responses received, and percentage of responses that were hits.
- Number of transactions by day/week/month/quarter/year and average hour versus peak hour.
- Number of transactions processed by crime type.
- Selectable date ranges.

The ABIS shall support the latent examiners and system administrators in selectively reporting on latent case management status over the life of the system or any selected shorter period of time to include at a minimum:

- Number of open and closed cases.
- Number of cases closed due to a match.
- Expiration of associated data due to statute of limitations or other reasons.
- Average number of latent images per open case.
- Maximum number of latent images per case.
- Percentage of capacity used at various levels.
- Number of cases within 90, 60, and 30 days of eclipsing their associated statute of limitations.
- Average number of minutiae per latent finger or palm.
- Maximum and minimum number of minutiae per latent finger or palm.
- Number of searches executed.
- Average number of searches executed per latent image.

In addition the ABIS will allow the ABIS system administrator to generate reports on capacities and sizes, to include by selectable date:

- Criminal, ID slaps, and/or tactical submissions by:
    - Number of individuals in databases and/or archives by ten-print, known palms, unknown palms, and unsolved latent records.
    - Number of fingers in databases and/or archives by ten-print, known palms, facial images, and unsolved latent records (fingerprints and palm prints).

- Sex of individuals in databases and/or archives by ten-print, known palms, and facial images.
- Average image quality (using NFIQ and vendor metrics) for rolled fingerprints and flats for databases or archives by finger and averaged across both hands.

- For databases, archives, and matchers:
  - Sizes and usage by selectable date.
  - Capacity available by selectable date.
  - Projected need for additional capacity by date.
- Administrative reports for each ABIS matcher, to include at a minimum:
  - Matcher number and name – types of data contained in the matcher.
  - Number of individuals enrolled in each matcher.
  - Number of individuals with one record, two records, or three records in the matcher.
  - Average minutiae per record.
  - Average NFIQ score per finger per image.
  - Average compression rates per image.
- Administrative reports for all of the ABIS reflecting the following information, at a minimum:
  - Number of persons authorized to access the ABIS.
  - Number of persons who have administrator access.
  - Number of persons who have ten-print access.
  - Number of persons who have latent print access.
  - Number of live scans.
  - Number of ORIs.
  - Number of workstations (by type).

SYSTEM REQUIREMENTS REVIEW

Contractor shall conduct a System Requirements Review (SRR). Upon completion of the SRR, based on the results of the System Requirements definition activity, Contractor may recommend changes to the State System Requirements Specifications for consideration by State.

Contractor shall analyze State's System Requirements and validate the requirements of the specifications. Contractor shall document the deficiencies in State's System Requirements, if any, and recommend changes to the areas in which those changes would correct deficiencies or otherwise benefit the State (e.g., enhance the overall functionality, performance, or reliability of systems or services; reduce costs; shorten the schedule; or reduce project risk).

Contractor shall document any recommended changes to State's System Requirements Specifications and support these recommendations (e.g., with cost-benefit analyses).

Contractor shall provide to State with System Requirements Specifications and the rationale for any recommended changes. Contractor shall update State's System Requirements Specifications with any changes resulting from actions assigned by State as a result of the SRR and all approved changes.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-02: System Requirements Specifications.
- DEL-07: Agenda.
- DEL-08: Presentation Materials.
- DEL-09: Minutes.

SYSTEM HARDWARE AND SOFTWARE DESIGN AND DEVELOPMENT

Perform System Design and Development

Contractor shall design and develop the System to satisfy the System Requirements Specifications [DEL-02] and meet the required standards specified in section 1.103 Environment, Specifications, Standards, and Guides. Contractor shall design, develop, and provide all hardware, software, and data components of the System, with the exception of the operational data that is to be provided by State.

Contractor shall, to the maximum extent possible, use non-proprietary hardware and software in developing and implementing the ABIS. Equipment for remote sites recommended by Contractor must be available commercially from third-party vendors as well as through the Contractor. Installation of ABIS software, shall be the sole responsibility of the Contractor.

Contractor shall conduct a System Design Review (SDR) and present to State for approval. The System design shall:

- Be complete down to the line replaceable unit (LRU) level for all hardware items and through the computer software unit (CSU) level for all developed software;
- In the case of COTS software, be complete through the level of licensed software products (LSPs);
- Identify the functions performed by, performance required of, and interfaces supported by each CSU (for developed software) and each LSP (for COTS software);
- Document the number and interconnection of all LRUs and identify the software components loaded on each LRU;
- Document the bandwidth, memory, and throughput of each LRU;
- Describe the interfaces supported by each CSU, LSP, and LRU;
- Specify any standards with which each CSU, LSP, and LRU complies; and
- Include complete work flows for all operational user and administrative functions.

As part of the SDR, Contractor shall present evidence (e.g., results of analyses, computer model and simulation results, benchmark results, and vendor-supplied specifications) to demonstrate that the design satisfies the requirements of State's System Requirements Specifications [DEL-02] and the required standards set forth in section 1.103 Environment, Specifications, Standards, and Guides. Contractor shall deliver a Requirements Verification Traceability Matrix [DEL-30] documenting mapping between (i) the requirements contained in the System Requirements Specifications and the major subsystems or components of the design, and (ii) the requirements contained in the System Requirements Specifications and the methods of verification indicated in Contractor's response to the System Requirements Specifications set forth in the System Requirements Specifications.

Upon successful conclusion of the SDR and written approval of the design by State Project Managers, Contractor may begin development and/or procurement of System software and hardware.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-05: Migration Plan
- DEL-07: Agenda
- DEL-08: Presentation Materials.

- DEL-09: Minutes.
- DEL-12: Database Design Document.
- DEL-13: Interface Design Document.
- DEL-14: System Design Document.
- DEL-15: Bill of Materials.
- DEL-17: Training Plan.
- DEL-18: Installation Drawings.
- DEL-22: COOP Plan.
- Test Plan [DEL-28]: at SDR, with updates at Test Readiness Review.
- DEL-30: Requirements Verification Traceability Matrix

IMPLEMENTATION

Contractor shall implement, test, and support State's acceptance of the technology to be utilized in the provision of work as provided in the System Requirements. All products, services, and systems developed and/or delivered by Contractor shall comply with the System Requirements and the standards and guides set forth in section 1.103 Environment, Specifications, Standards, and Guides.

Contractor shall provide all equipment and software necessary to satisfy the System Requirements at the proposed operational primary site and the proposed COOP disaster recovery site (COOP site). Contractor shall provide all necessary equipment and software at remote sites to provide an equal level of service and functionality as replacement of all existing equipment under the current Biometric Identification Services agreement, including, as applicable, servers, communications gear, workstations, printers and other equipment identified in the System Requirements.

Contractor shall provide State and its remote sites with a comprehensive set of user, system, training and management documentation. Contractor shall deliver those items identified in the list of deliverables set forth in this SOW. Contractor shall provide the documentation in both electronic and hard-copy formats. User documentation shall describe the components, functions, and operations of each workstation type. Each ABIS workstation shall be provided with online user documentation that is resident on the workstation or accessible via the agency's internal networks.

All deliverables shall be subject to State approval and acceptance in order to satisfy the terms and conditions of the Contract.

Contactor's Implementation Communication Plan:

Meeting	Freq.	Participants / Recipients	Delivery Method	WBS Reference
Project Kickoff Meeting	One or more as required by MSP	Contractor project team and MSP project team	In person - at MSP facility with conference call set up for any remote project team members	1.5
Planned Results / Deliverables: Introduction of project team members, assignment of roles and responsibilities, agreement on high-level project scope, and review of the Integrated Master Schedule *[DEL-03]* and the Project Management Plan *[DEL-01]*. **Outcome**: Updates to the Integrated Master Schedule *[DEL-03]* and the Preliminary Project Management Plan *[DEL-01]* and Meeting Minutes.				

<table>
<tr><th>Meeting</th><th>Freq.</th><th>Participants / Recipients</th><th>Delivery Method</th><th>WBS Reference</th></tr>
<tr><td>System Requirements Review (SRR)</td><td>Once</td><td>All key Contractor and MSP team members</td><td>In person - at MSP facility with conference call set up for any remote project team members</td><td>2.5</td></tr>
<tr><td colspan="5">Planned Results / Deliverables: Follow a specified agenda with specific discussion points to understand the System Requirements and proposed solution.
Outcome: Agreement on and signed approval of System Requirements Specifications [DEL-02]. Sufficient information to draft the Design Documents.</td></tr>
<tr><td>System Design Review (SDR)</td><td>Once</td><td>Contractor project team and MSP project team</td><td>In person - at MSP facility with conference call set up for any remote project team members</td><td>2.10</td></tr>
<tr><td colspan="5">Planned Results / Deliverables: Follow a specified agenda with specific discussion points regarding the Design Documentation and Project Plans. Documentation of all line-replaceable hardware units, computer software units, licensed COTS software, interfaces, workflows, and functionality.
Outcome: Agreement on and signed approval of the Design Documents and Project Plans, and understanding of how all solution requirements will be met. Contractor engineers will start the work needed to configure the system according to the approved Design Documents.</td></tr>
<tr><td>Product Test Readiness Review (PTRR)</td><td>Once prior to FAT</td><td>Contractor project team and MSP project team</td><td>In person - at Contractor facility (Anaheim, CA) with conference call set up for any remote project team members</td><td>10.3</td></tr>
<tr><td colspan="5">Planned Results / Deliverables: Review of the Test Reports from Contractor’s Contract Testing, and MSP verification that Contractor has the MorphoBIS sufficiently ready for the FAT.
Outcome: MSP approval to proceed with FAT, or identification of issues to be resolved prior to FAT.</td></tr>
<tr><td>Pre-Ship Review (PSR)</td><td>Once</td><td>Contractor project team and MSP project team</td><td>In person - at Contractor facility (Anaheim, CA) with conference call set up for any remote project team members</td><td>11.2</td></tr>
<tr><td colspan="5">Planned Results / Deliverables: Demonstration of fixes related to FAT issues. Review of the updated BOM [DEL-15], Installation Plan [DEL-16], Training Plan [DEL-17], Installation Drawings [DEL-18], Training Material [DEL-19], COOP Plan [DEL-22], and draft Version Description Document [DEL-26].
Outcome: Agreement on and signed approval of the associated documents, and MSP approval to ship.</td></tr>
<tr><td>System Test Readiness Review (STRR)</td><td>Once, prior to SAT</td><td>Contractor project team and MSP project team</td><td>In person - at MSP facility with conference call set up for any remote project team members</td><td>13.2</td></tr>
</table>

Meeting	Freq.	Participants / Recipients	Delivery Method	WBS Reference
Planned Results / Deliverables: Review of the results of Contractor's Engineering Site Testing, and MSP verification that Contractor has the MorphoBIS sufficiently ready for the SAT. **Outcome:** MSP approval to proceed with the SAT, or identification of issues to be resolved prior to the SAT.				
Operational Readiness Review (ORR)	Once	Contractor project team and MSP project team	In person - at MSP facility(s)	15.2
Planned Results / Deliverables: Review of the results of Contractor's SAT, including re-testing of fixes. Determine the readiness of the system(s), facilities, and personnel to initiate the UAT. **Outcome:** MSP approval to proceed with the UAT, or identification of issues to be resolved prior to the UAT.				
Final Acceptance Review (FAR)	Once	Contractor project team and MSP project team	In person - at MSP facility with conference call set up for any remote project team members	22
Planned Results / Deliverables: Verification of any UAT fixes required for Final Acceptance, and authorization to put the system into full production mode. **Outcome**: Sign-off of the Final Acceptance Certification by the MSP. Execution of the Transition Plan to bring the system into full production mode and to allow the decommissioning of the old MSP system (includes a residual data migration). The System Operation Phase begins.				
Project Management Reviews	Monthly, at a minimum, more frequently after PTRR	MSP PgM and any relevant team members	In person - at MSP facility with conference call set up for any remote project team members	Various
Planned Results / Deliverables: Follow a specified agenda with specific discussion points to understand the project status, issues, actions, deficiencies, and upcoming tasks. **Outcome**: Meeting Minutes *[DEL-09]* and updates to the Integrated Master Schedule *[DEL-03]*.				

SYSTEM SETUP

System Setup provides for the setup and security of the new ABIS environment.

Provide Data/Property Management and System Security

Contractor shall develop, document, and implement comprehensive procedures for the management of data, documentation, and State property (any equipment, hardware and software that belongs to the State). Data management shall encompass all data and documentation produced by Contractor under the Contract, procured by Contractor under the Contract, and received from State for use on the Contract.

Contractor shall maintain access to State staff, the remote site administrators, FBI auditors, and other authorized personnel to inspect the repository, the log of transactions and performance/throughput rates, and user-level access history in order to allow State to generate predefined (canned) reports as well as ad hoc reports.

Contractor shall take reasonable security precautions approved by State, by providing among others the necessary software updates, to ensure the ABIS, including its related hardware, software, data, and third-party components, is maintained in accordance with contemporary best business practices, including performing antivirus updates, software updates, configuration management, backup/restore/recovery, system logging and report generation. Contractor shall take reasonable security precautions as approved by State to ensure State's primary site and COOP site physical security.

All Contractor-supplied facilities or systems shall provide protection and control of all State information, equipment, documentation, and network access.

Contractor shall be responsible for all primary site and COOP site personnel, and exercise all rights, responsibilities, and prerogatives associated therewith, as necessary to provide work under this Contract. Contractor's personnel shall be subject to the security provisions under this Contract.

Contractor shall comply with all provisions of the FBI CJIS Security Policy as specified in section 1.103 Environment; Specifications, Standards, and Guides.

Contractor shall take reasonable precautions to prevent the loss of or alteration to State's data. Accordingly, Contractor shall keep backup copies of all of State's data in a safe and secure off-site facility approved by State.

Contractor shall not utilize, or provide to third parties, State's database without prior written approval of State.

Contractor shall be responsible for ensuring that appropriate encryption or other security methods are implemented to guarantee the secure transmission of data in the ABIS, as further provided elsewhere in the Contract including the System Requirements Specifications [DEL-02].

Contractor shall work with State, and remote site agencies to achieve end-to-end security for all components that make up the ABIS. Contractor shall document its security program in a Security Plan [DEL-10].

Contractor shall also notify State in writing within 5 calendar days of Contractor's knowledge of the existence of any intrusions or other security problems or breaches that may affect the integrity of the system data or any other State data.

Deliverables:

Contractor shall document and provide the following deliverable(s):

- DEL-01: Project Management Plan.
- DEL-10: Security Plan.
- DEL-22: COOP Plan.
- DEL-32: Data and Property Management Plan.

ACCEPTANCE TESTS

The purpose of testing will be to verify that Contractor's product meets or exceeds all System Requirements Specifications [DEL-02].

Contractor shall develop and execute a comprehensive test program, spanning all phases of development and all levels of assembly of the system(s). Contractor shall develop a Test and Evaluation Master Plan (TEMP) [DEL-04], which shall:

- Govern all levels of testing, from the unit level through the fully assembled and integrated (with external systems) system;
- Govern all phases of testing, from unit testing through completion of system acceptance;
- Govern formal user acceptance testing; and
- Include the coordinated and complete testing with the live scan replacement equipment (subject of a separate but concurrent procurement) with the new ABIS, understanding that acceptance testing at each stage from Factory Acceptance Test (FAT) through to User Acceptance Test (UAT) will not be completed until Live scan and ABIS components are successfully tested together.

For unmodified hardware and software, vendor-supplied test results may be substituted for verification of requirements below the level of the fully integrated system.

The purpose of the FAT is to ensure that the basic capabilities are available and work in a factory setting, and that the documentation associated with the system reflects the design and is usable (e.g., one typically uses the start-up and shut-down procedures to verify that they can be used, as written, to perform the intended function). These tests are oriented toward verifying as much functionality, hardware, interface requirements, performance requirements, accuracy requirements, and documentation as possible.

FAT is typically run with scripts to ensure agreement among the stakeholders on the input and expected results and to ensure that the tests are repeatable. After successful passage of the

FAT at Contractor's facility, Contractor will be given permission to ship the system to the operational site(s).

The converted biometric database (known and unknown friction ridge files as well as related feature sets, pointers, and tables) will be audited as part of the primary site configuration FAT. Accuracy tests will employ these repositories, while the search records will be data sets prepared by State and having known image quality (ten-print only), minutiae counts (latents and their mates only) and mate or no-mate status information.

Conduct FAT

Contractor shall conduct FAT for the fully assembled and integrated system for both the primary site and the COOP site (disaster recovery site) levels. FAT shall include all tests necessary to confirm that all requirements of the System Requirements Specifications [DEL-02] have been satisfied and to demonstrate compliance with required standards listed in section 1.103 Environment, Specifications, Standards, and Guides. FAT shall also include all tests necessary to demonstrate satisfaction of those requirements from any (provider-developed) subordinate specifications.

Contractor shall prepare a FAT Plan [DEL-28] and FAT Procedures [DEL-21] and submit them for approval. FAT shall be conducted in accordance with the approved FAT Plan [DEL-28] and FAT Procedures [DEL-21]. FAT may be conducted as a part of integration testing or as a separate phase of the test program, subject to State approval. Contractor shall conduct Product Test Readiness Reviews (PTRRs) prior to the conduct of FAT. State will witness the execution of all FATs.

The results of FAT shall be documented in a FAT Report(s) [DEL-06]. Contractor shall conduct a Pre-Ship Review (PSR) to demonstrate the FAT success, to determine the readiness of the system(s) for delivery first to primary site and then secondly to the COOP site, and to secure State authorization to ship the system components and configurations.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-06: FAT Report.
- DEL-07: Agenda.

- DEL-08: Presentation Materials.
- DEL-09: Minutes.
- DEL-16: Installation Plan.
- DEL-17: Training Plan.
- DEL-18: Installation Drawings.
- DEL-19: Training Materials.
- DEL-21: FAT Procedures.
- DEL-22: FAT COOP Plan.
- DEL-26: Version Description Document.
- DEL-28: FAT Plan.

Conduct SAT

The purpose of the System Acceptance Test (SAT), which is also known as System-level Integration Test (SIT), is:

- To demonstrate that the equipment was installed correctly and operates at the functional and performance levels verified at FAT;
- To verify the requirements that could not be verified at the factory (such as operations using a remote site's network);
- To verify the performance requirements (throughput, accuracy, and reliability) with the full initial data load, multiple workstations, etc., to the extent that they have not already been signed off on at FAT; and
- To verify that the integrated sum, including remote site testing, is at least as functional as the sum of the individual parts and to verify that end-to-end work flows execute as anticipated – the actual verification of the correctness of the end-to-end work flows, to include all the processing at each step, is normally deferred to UAT.

The SAT is also script-based, with scripts built up from those used at FAT, ensuring that all additional requirements are allocated to specific test scenarios and that the scripts still ensure repeatability. Repeatability often requires cleaning out files and buffers that were changed as the result of a test step when the changed data is no longer needed by the system.

The SAT will include COOP activities. The minimum COOP activities that must be demonstrated include backing up and restoring data as well as using the COOP site for primary processing, then restoring the entire system, ensuring that the repositories and matchers are current and identical across the two sites. Verification of the COOP-related procedures will be a critical part of the SAT.

Contractor will prepare the SAT Plan [DEL-28] in cooperation with State. Contractor shall prepare SAT Procedures [DEL-21] and submit them for State approval. Contractor shall conduct the SAT in accordance with State-approved SAT Plan and approved SAT Procedures [DEL-21]. Contractor shall conduct a System Test Readiness Review (STRR) prior to the conduct of the SAT. State will witness the execution of all SAT(s).

Contractor shall document the results of the SAT in the SAT Report(s) [DEL-06]. Upon completion of the SAT, Contractor shall conduct an Operational Readiness Review (ORR) to determine the readiness of the system(s), facilities, and personnel to initiate the UAT and to secure State authorization to initiate operations.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-06: SAT Report.
- DEL-07: Agenda.
- DEL-08: Presentation Materials.
- DEL-09: Minutes.
- DEL-15: Bill of Materials.
- DEL-16: Installation Plan.
- DEL-17: Training Plan.
- DEL-18: Installation Drawings.
- DEL-19: Training Materials.
- DEL-21: SAT Procedures.
- DEL-22: SAT COOP Plans.
- DEL-26: Version Description Document.
- DEL-28: SAT Plan.

Conduct UAT

The purpose of UAT is final validation of the required business functions and flow of the system, under real-world usage of the system, by demonstrating that the delivered products and services are adequate for their intended purpose. UAT procedures will include both scripts and normal operations to see how the end-to-end work flows operate across the entire system, including the interfaces to the FBI. UAT will be planned to provide a realistic and adequate exposure of the system to all reasonably expected events. This includes things that might not happen in a normal period, such as a full backup and restore, switchover to the COOP site and a full suite of report generation events.

By this point in the project, State and Contractor will have verified most or all of the accuracy, performance, and capacity requirements. UAT will not be focusing on system problems (e.g., screening and reporting misspellings or software crashes), as those issues will be required to have been corrected by then.

Contractor will prepare a UAT Plan [DEL-28]. The UAT Plan will be reviewed and approved by State. State staff will conduct UAT. Contractor shall provide the facilities, equipment, and personnel to analyze results of concurrent operations, to identify discrepancies between results of the legacy system(s) and results of Contractor-delivered ABIS system(s), to resolve those discrepancies and, when those discrepancies result because of a failure of Contractor-delivered system(s), to meet the requirements, and to perform corrective maintenance.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-06: UAT Report.
- DEL-07: Agenda.
- DEL-08: Presentation Materials.
- DEL-09: Minutes.
- DEL-21: UAT Procedures.
- DEL-22: UAT COOP Plan.
- DEL-26: Version Description Document.
- DEL-28: UAT Plan.

SYSTEM MIGRATION

System Migration describes the migration requirements for the ABIS operational environment.

Install Sites

Contractor shall conduct site surveys and analyses to determine the facilities requirements (e.g., heating, air-conditioning, lighting, electrical power, structural loading, and physical access) for the facilities housing the replacement equipment at proposed primary site, COOP site, and remote sites. Contractor shall review the network configuration at each remote site to ensure that the equipment to be installed is compatible with existing network topologies. Contractor shall document any incompatibilities between the ABIS equipment to be installed and the facilities or networks and identify in an Installation Survey Report [DEL-27] any required facilities or network modifications to be made by State.

Contractor shall prepare a Version Description Document [DEL-26] with the complete instructions necessary to install and configure all hardware, software, and data associated with each deployment. The document will include site-specific installation information [DEL-27].

Contractor shall prepare an Installation Plan [DEL-16] to document the necessary installation tasks, responsibilities, schedule, resource requirements, equipment layout, cabling, and testing to verify correct installation of equipment and software at the primary site, COOP site and remote sites. Contractor shall prepare Installation Drawings [DEL-18] to define equipment layout and cabling.

Contractor shall (subject to State approval) deliver and install the equipment and software deliveries at the primary site, COOP site, and remote sites. Contractor shall check the installation and perform the necessary data conversions to prepare the equipment and software to support all testing and operations.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-16: Installation Plan.
- DEL-18: Installation Drawings.
- DEL-26: Version Description Document.
- DEL-27: Installation Survey Report.

Convert and Load Data

Production of the operational database will involve: (1) the conversion of the legacy database and (2) the loading of this data into the operational database.

Convert Existing Data

Contractor shall ingest and process all existing electronic ten-print, palm-print, and latent records and convert (i.e., feature extract) them to the appropriate internal feature format. The latents shall be converted into the Extended Feature Set (EFS) format.

For electronic card images, if Type 7 and/or Type 16 data appears in the card image set, it shall be recorded as a Type 20 record.

Contractor shall convert friction ridge images (and some paper forms) into ANSI/NIST-compliant image files and load them onto the system at the primary site with all appropriate transaction-related information, all available for search and retrieval based on ANSI/NIST and FBI/MSP EBTS record types and field definitions. As part of Maintenance, the Contractor shall supply friction ridge matching (known and unknown finger and palm) when transactions are submitted using ANSI/NIST-compliant transactions that conform to EBTS.

Contractor shall perform feature extraction on all ten-print records for use in the matchers. Contractor shall cross-search all transactions to determine all transactions that share unique identities, link them together as single identities, and assign a state identification (SID) to each unique identity. Contractor shall use any existing State person ID codes and will retain all SID numbers in indexing the ten-print repository. For cases in which new matches are found, the list of candidates shall be presented to State for review.

Contractor shall create and maintain one best image quality record and up to three (3) of best incident records for matching purposes. For cases in which three or more transactions are present at a state level for a subject, Contractor shall use the NIST Fingerprint Image Quality (NFIQ) software to quality-rate each finger image. Based on image quality scores, Contractor shall develop a “best image set” as a composite record for each of these identities at the state level. Contractor shall load all available feature sets for up to three transactions for each identity, the composite and the three most recent transactions, at the state level. The known ten-print file shall be loaded into the matchers for testing and Operational Use, with pointers to the appropriate transaction control number (TCN), and SIDs.

For cases in which multiple palm transactions are present for a subject, Contractor shall use the most recent palm-print transaction based on the state that submitted it to extract features for the matchers for that state. After performing feature extraction on all palm records for use in the matchers, Contractor shall use any existing State person ID codes and will retain all SID numbers in indexing the palm-print repository at the state level. The known palm file shall be loaded into the matchers for testing and operational use, with pointers to the appropriate TCN, and SID.

Contractor shall perform feature extraction for all, up to three (3) incidents per SID. This must include rolled and slap prints. Demographics must also be pulled to populate the AFIS database(s). These may need to be pulled from the current AFIS NIST archive, the FBI, or converted from fingerprint cards. An electronic feature extraction of palm prints must be completed from the current AFIS NIST archive. All project plans, time estimates, and costs related to these tasks must be included in the vendor’s proposal. Currently MSP has roughly 770,000 SIDs not on the current AFIS archive, of these 524,000 should be able to be pulled from the FBI, leaving roughly 248,000 SIDs needed to be converted from paper cards.

Contractor shall ingest all unsolved latent images and generate feature sets, either by auto-extracting them or by converting the corresponding existing feature sets to the EFS format. The preference is the use of the already encoded feature sets as the basis of re-encoding into the EFS format. The unsolved latent file shall be loaded into the matchers for testing and operational use, with pointers to the appropriate latent case numbers and related information loaded into the latent case management system.

Contractor shall preserve agency feature encoding through use of NIST Type 9 records saved by State staff to facilitate conversion to Contractor’s feature set. If NIST Type 9 records are not achievable, Contractor’s auto-feature function may be conditionally acceptable on the provided latent images, subject to State approval.

Contractor will contract with Mentalix for conversion of paper card files. Contractor retains full responsibility for the performance of card conversion services. Mentalix (subcontractor) personnel will be subject to the same contractual background checks and performance requirements as Contractor employees.

Deliverables:

Contractor shall provide the following deliverable(s):

- Copies of converted existing data.

Load Data

Contractor shall load all of the images and extracted features into the appropriate databases onto the system at the primary site and the COOP site with the appropriate TCN and SID.

Contractor shall deliver two copies of the output media for future use by State in any system or process of its choosing. As part of this task, Contractor shall:

- Cross-search all loaded ten-print records and provide a digital report of all possible unanticipated matches for use in consolidating records;
- Search all loaded ten-print records against the loaded latent records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record;
- Search all loaded palm-print records against the loaded latent records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record;
- Search all loaded latent records against the loaded ten-print records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record; and
- Search all loaded latent records against the loaded palm-print records and provide a digital report of all possible matches for use in identifying a known person associated with a latent record.

At the end of the initial data load, Contractor shall produce a detailed report in accordance with the following requirements:

- The number of records converted, to include a count of modalities (fingers, and palms) of the converted records.
- Any problems encountered, by record number (i.e., any conversion assigned number), TCN, problem type, and resolution.

- All records not successfully converted by record number and TCN, if available.
- Records that were identified as being from the same subject (i.e., multiple enrollments) sorted by TCN.
- Records that are forward or reverse searched and that are strong candidates for identifying latent impression sources, sorted by state.
- Average image quality for known ten-print by enrollment type, hand and finger position, by state, using the NFIQ tool.
- The results of a conversion audit.

Deliverables:

Contractor shall provide the following deliverable(s):

- Copies of data as noted above.

Conduct Migration Planning

Contractor shall develop a Migration Plan [DEL-05] that identifies the activities, events, and resources (tools, data, facilities, personnel, and other resources) required to migrate from the legacy AFIS to the replacement ABIS environment provided under the Contract. The plan will identify the sources (i.e., Contractor, State or specific state remote sites) of all resources and specify when those resources will be required.

Contractor shall assist the State remote sites in planning their migration from the legacy AFIS system to the replacement ABIS provided hereunder.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-05: Migration Plan

System Configuration Planning and Management

State ABIS devices are geographically dispersed over a large area. This dispersion poses unique problems related to problem reporting; test, diagnosis, and deployment of patches and revisions; and other aspects of configuration management. A Configuration Management Plan [DEL-29] and process will allow for efficient and effective management of these unique problems.

Contractor shall document and implement a Configuration Management Plan [DEL-29] for performing configuration control and processes that shall address unique problems efficiently and effectively. Configuration control and management performed by Contractor shall accomplish the following:

- Establish a controlled configuration for each hardware and software component at the primary site, the COOP site, and each remote site;
- Maintain current copies of the deliverable documentation and code;
- Give State access to the documentation and code under configuration control; and
- Control the preparation and dissemination of changes to the master copies of the deliverable software and documentation placed under configuration control so that they reflect only approved changes.

Contractor shall generate management records and status reports on all products composing the controlled configuration for each hardware and software component at the primary site, the COOP Site, and each remote site. The status reports shall:

- Make changes to controlled products traceable;
- Serve as a basis for communicating the status of configuration identification software; and
- Serve as a vehicle for ensuring that delivered documents describe and represent the associated software.

Contractor shall participate in State configuration control meetings. State configuration control meetings will establish and control the requirements baseline [DEL-02] throughout the performance of the Contract and will control the operational baseline (deployed hardware, software, databases and documentation) once the ABIS becomes operational.

Contractor shall prepare a Version Description Document [DEL-26] comprising the complete instructions necessary to install and configure all hardware, software, and data associated with each deployment, including site-specific installation information for the duration of the term of the Contract.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-02: System Requirements Specifications.
- DEL-26: Version Description Document.
- DEL-29: Configuration Management Plan.

COOP Planning

Contractor shall perform the necessary planning; deliver a COOP Plan [DEL-22]; provide or utilize the necessary facilities, equipment, supplies, data and documentation; and conduct the training necessary to establish a viable COOP Plan capability that ensures the performance of Contractor's essential functions during any emergency or situation that may disrupt normal operations and leave the primary site facilities damaged or inaccessible.

The purpose of COOP planning is to assure that the capability exists to continue essential provider functions across a variety of potential emergencies as well as when maintenance or upgrade activities might impact ABIS system use. A COOP Plan should account for:

- Ensuring the continuous performance of State's essential functions/operations during an emergency;
- Protecting essential facilities, equipment, records, and other assets;
- Reducing or mitigating disruptions to operations; and
- Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

The COOP capabilities provided by Contractor under this Contract shall be:

- Maintained as an active-active site;
- Capable of providing 100 percent of the ABIS services (in the event of the loss of the primary site) both with and without warning/scheduling; and
- Continuously operational in a load-balanced environment during normal operations.

At a minimum, the COOP Plan provided by Contractor shall contain the following:

- Plans and procedures.
- Identification of essential functions.

- Alternate facilities.
- Interoperable communications.
- Vital records and databases.
- Tests, training and monthly exercises/drills.

The COOP Plan should be developed and documented to ensure that, when implemented, it will provide for continued performance of essential State functions under all reasonably foreseen circumstances. At a minimum, the COOP Plan shall also:

- Delineate essential functions and activities.
- Outline a decision process for determining appropriate actions in implementing COOP plans and procedures.
- Establish a roster of fully equipped and trained emergency provider and State personnel with the authority to perform essential functions and activities.
- Include procedures for employee advisories, alerts, and COOP Plan activation, with instructions for relocation to predesignated facilities, with and without warning, during duty and non-duty hours. This includes providing for personnel accountability throughout the duration of the emergency and providing for continuous operational status in an active-active environment.
- Establish reliable processes and procedures to acquire resources necessary to continue essential functions and sustain operations similar to that of the primary site for up to 30 days.

Essential functions are defined as those functions that enable Contractor to provide vital services, under any and all circumstances.

Deliverables:

Contractor shall provide the following deliverable(s):

- DEL-22: COOP Plan.

Upon the successful completion of UAT through COOP Plan, State will conduct a Final Acceptance Review (FAR) to determine whether Contractor has satisfied the terms and conditions of this SOW and to accept the system into operations. The determination will be based upon the delivery of deliverables and plan items that comply with the requirements of the Contract, the satisfactory performance of all SOW activities, and the successful demonstration (through the FAT, SAT, and

UAT process) that the delivered systems and data satisfy the requirements of the System Requirements Specifications [DEL-02].

SYSTEM TRAINING

Contractor shall develop User Manuals [DEL-11] addressing all user functions for all user types (e.g., ten-print and latent examiners, system administrators, maintenance personnel). User documentation shall describe the components, functions, and operations of each server and workstation type. Operations descriptions shall include a list and description of all error conditions, as well as the associated error messages displayed and the action required of the operator for each error condition. Each ABIS workstation shall be provided with online user documentation that will be resident on the workstation or accessible via the agency's internal networks. Vendor must supply all documentation in hardcopy and electronic formats, electronic format must be in Microsoft Word.

Deliverables:

- Training Plan [DEL-17]
- Training Materials [DEL-19] including, via example, computer-based training, videos, guides, and manuals, and conduct on-site user training as required to support testing, deployment, and operations.

Contractor shall conduct four types of courses as follows:

- Ten-Print Workstation Baseline – This course will cover all ABIS ten-print functionality associated with the new ABIS. The course will provide hands-on instruction on the ten-print workstation for manual and automated ten-print processing. "Hands-on" requires that each student have access to a fully functional workstation and training database during the training sessions. This requirement applies to both the Ten-Print Workstation Baseline training and the Latent Workstation Baseline training described below. The course will cover ten-print manual and automated work flows, displays, data entry, quality assessment, and all functionality. In addition, the course will cover the basic and administrative user functions of the NIST archive. This course will also include the method by which NIST standard fingerprint transactions can be run against non-State agency AFISs. This course will also cover palm-print and slap-print entry and quality assessment functions. This course will need to be conducted on-site enough times initially to accommodate approximately 15 examiners and at least once yearly, for the duration of the Contract, to accommodate up to 15 examiners.

- Latent Workstation Baseline – This course will cover all ABIS latent functionality associated with the new ABIS. The course will provide hands-on instruction on the latent workstation and latent case management system. The course will cover latent manual work flows, displays, data entry, quality assessment, and all functionality. In addition, the course will cover the basic user functions of the NIST archive. This course includes the method by which NIST standard latent transactions can be run against non-State member agency AFISs. The course will include instruction in best practices for ensuring optimum accuracy. This course will also cover latent palm-print and slap entry, quality assessment, and matching functions. This course will need to be conducted on-site enough times initially to accommodate approximately 65 examiners and at least once yearly thereafter, for the duration of the Contract, to accommodate up to 65 examiners.
- MSP Help Desk – This course will provide an overall view of technical aspects of the ABIS and provide methods to manage and resolve minor incidents quickly and effectively. This course will need to be conducted on-site initially to accommodate approximately 12 participants and at least once yearly, for the duration of the Contract, for approximately eight (8) participants, to accommodate new help desk personnel and keep existing staff current.
- Managers and Supervisors – This course will cover ABIS management functions. The course will need to be conducted on-site and provide hands-on instruction for up to eight (8) managers and supervisors on accessing and producing management reports, creating user accounts, and performing audits and inquiries using the tools provided by the system.

Should State remote sites require additional training beyond that required above, such training will be provided at no additional cost to the State.

On an annual basis and at no additional cost to the State, the Contractor will provide up to 3 State personnel to attend Contractor's annual training conferences.

Upgrades and new versions to the system that affect end-user functionality include training at no additional cost (e.g. classroom or online training, training flier, release features, etc.)

Training is provided in a variety of formats for product installation, use, and administration for a variety of levels (e.g. basic, advanced, refresher, etc.)

All training manuals, training plans and other documentation provided become the property of the State.

Contractor's Training Descriptions:

Ten-Print Workstation (Morpho Card Capture Workstation)

MSP Training Requirements	Contractor Course Overview
• Hands-on • All workflows • GUIs / displays • Data entry • Quality assessment • Palm print identification • Non-MSP AFIS searching	This course teaches the skills necessary to use and deliver training on the Card Capture workstation's operation and includes: • Best practices recommendations. • Ten-print / palm card scanning. • Descriptor data entry. • Quality control. • Searches – Ten-print and palm print. • Handling exceptions and errors. • "Lights out" processing. • Submitting NIST searches to remote AFISs.
Baseline Training: Three classes with up to six students each (18 total) – Two-day duration per class Refresher and new training options at least yearly to an equal number of students	

Latent Workstation (Morpho Latent Expert Workstation)	
MSP Training Requirements	**Contractor Course Overview**
• Hands-on • All workflows • GUIs / displays • Data entry • Quality assessment • Best-practices for accuracy • Latent palms • All functionality • Non-MSP AFIS searching	This course teaches the skills necessary to use and deliver training on the Latent workstation's operation and includes: • Best practices recommendations. • Latent entry. • Identification – Ten-print latent and palm latent. • Minutiae encoding and placement. • Deleting and editing minutiae. • Enhancing fingerprint images. • Quality control. • Searches. • Handling exceptions and errors. • "Lights out" processing. • Submitting NIST searches to remote AFISs.
Baseline Training: Thirteen classes with up to ten students each (65 total) – three-day duration per class Refresher and new training options at least yearly to an equal number of students	

Managers and Supervisors System Administration Training	
MSP Training Requirements	**Contractor Course Overview**
• Hands-on • Creating accounts • Accessing / producing reports • System audits and inquiries	This hands-on course teaches the skills necessary to use and deliver training on management system administration and includes: • User management, including adding, removing users, and changing user roles. • Report generation. • Statistical reporting, including accuracy and productivity. • Understanding the Home Page menu.
Baseline Training: Two classes with up to five students each (10 total) – one-day duration per class	

Help Desk System Administration Training	
MSP Training Requirements	**Contractor Course Overview**
• Hands-on • Technical overview • Incident Management	This hands-on course teaches the skills necessary to use and deliver training on Help Desk system administration and includes: • Linux and Windows Operating Systems. • Database maintenance and management. • System monitoring and troubleshooting. • Report generation. • Statistical reporting to include accuracy and productivity. • Workstation and peripheral operations. • System performance tools. • Understanding the Home Page menu. • Monitoring network traffic. • System and security functions.
Baseline Training: Three classes with up to five students each (15 total) – three days' duration per class Refresher and new training to accommodate new staff and keep staff current	

Contractor's Training Materials:

Manual	Topics
MorphoBIS System Administrator Guide	• System Overview • Startup and Shutdown • Subsystem Directories • User Accounts • Backup and Restore • Reports • System Utilities • Database Management • Morpho Central Viewer
Morpho Card Capture User Guide	• Log On / Log Off • Workflow Selection

Manual	Topics
	• Acquiring Card Images • Editing a Card • Case Submission
Morpho Latent Expert User Guide	• Log On / Log Off • Case Explorer • Case View • Latent Case • Capture Evidence • Evidence • Latent Encoding • Search Submission • Latent Associations • Case Attachments • Latent Automation
Morpho Reviewer User Guide:	• Home Page • Quality Control • Database Maintenance • Comparing Records • Verification • Charting • Descriptor Data Entry • Submitting FBI Transaction Requests
Morpho Archive Service User Guide	• Introduction • Searching the Archive • Viewing Search Results

System Operation & Support

Phase II - Contractor shall provide all facilities, equipment, software and personnel required to deliver the services to satisfy the system operation and support phase of the project for primary site, COOP site, and remote sites as set forth in this SOW, Contractor must also comply with Exhibit 1, Vendor Managed Hosting Services.

Contractor must meet system availability requirement of at least 99.8 percent for all Services, measured monthly, and in accordance with the terms of the Contract.

SUPPORT SERVICES

Contractor's Support Services responsibilities shall include, but are not limited to tracking and responding to problems reported, resolving Errors, and controlling configuration of software and hardware baselines, on-site and remotely as necessary.

Contractor must back up (data and system configurations) daily for COOP considerations. Copies of the backup media must be stored off site from the primary site and COOP site to increase the likelihood of their availability in the event of a natural or man-made disaster.

Contractor shall be responsible for all upgrades to the installed operating system(s), database management systems, and application software to ensure that the services conform to future approved FBI EBTS interface specifications and that no service is running on a suite of software no longer supported by the licensing Contractor.

Contractor shall provide access to a well-maintained and indexed repository of all enrolled transactions, stored and retrievable in FBI EBTS formats. Functionality must include: the ability to update, delete, retrieve and print appropriate card formats and other forms or link enrolled transactions.

The Contractor shall provide reports on the status of the system, the services delivered, and repository and transaction volumes.

Contractor must provide services including, but not be limited to, those listed below:

- Contractor's Customer Support for State help desk staff shall made be available during support hours (24 hours per day, seven days per week, including State holidays) for ABIS software, hardware and ten-print site equipment; and from 8:00 am to 5:00 pm EST Monday – Friday for remote latent sites.

- State designated staff shall have access to Contractor's Customer Support through the Web-based trouble ticketing system, or telephone/email. The trouble ticketing system shall provide the State a simple method to submit, track and update issues that require escalation to Contractor's Customer Support. The authorized State contacts will each receive an account and training on the ticketing system.
- Contractor's telephone number shall be managed by an automated system to quickly connect State staff with the appropriate Customer Support personnel.
- Contractor's automated system must include voice mail functionality.
- Severity levels for Errors shall be assigned according to Section 5.4(a) of Exhibit 1 Vendor Managed Hosting Services.
  Contractor shall respond within the period specified in Section 5.4(b) of Exhibit 1 Vendor Managed Hosting Services.
- Contractor's Customer Support shall work with State's Project Manager and State's technical support staff on correcting Errors and keep such State personnel informed regarding the updates and scheduled time frames to ensure that all maintenance windows are clearly communicated and the requirements of this SOW are met.
- Deficiency correction, time frames, and Service Credits for failure to timely correct any deficiencies are as specified in Exhibit 1, Sction 5.4. Support Service Level Requirements.

Software Updates

Contractor shall maintain software keeping current with new technology standards through third-party software upgrades, enhancements, updates, patches, bug fixes, etc. in accordance with this SOW and in coordination with State's Project Manager. By definition, such software updates shall include, but is not be limited to, enhancement, minor and major version releases, and other improvements and modifications to the software (including application software).

Maintenance services include compatibility with any and all interfaces provided by Contractor. Prior to the installation of any third-party software, or any update thereto, Contractor shall test and ensure such third-party software's compatibility with the then-current version of the software. Contractor shall ensure that the software is compatible with all required or critical updates to third-party software, including without limitation service and compatibility packs and security patches, promptly upon their release.

System Environment

As part of maintenance services, Contractor shall also provide maintenance of the server software that is part of the server environment for the solution, including but not limited to operating system software, database software, and other software installed in the server environment that is not application software. Contractor shall update, upgrade, replace and/or maintain such server software components during the term of the Contract to comply with the system requirements and the warranties specified in this Contract and to be compatible with the application software, including any application modifications provided by Contractor under the Contract.

Contractor shall provide software updates to the server software to keep current with new technology standards, software updates to the application software and other application modifications, all in coordination with State's Project Manager.

Contractor shall also provide maintenance of the server hardware components surrounding the software, including but not limited to all equipment and networking components and other hardware upgrades. Contractor shall repair, upgrade, replace and/or maintain these server hardware components during the term of the Contract to comply with the system requirements and the warranties specified in this Contract and to be compatible with the software including any application modifications provided by Contractor under the Contract.

Furthermore, Contractor shall, during the term of the Contract, maintain the solution's compatibility with State's client environment by providing, among others, software updates to the software and hardware upgrades to the solution hardware.

Technology Refresh and Enhancements

As part of Maintenance and Support services, Contractor shall propose functional and processing requirements for, and implement, future upgrades. Contractor shall also identify and make recommendations concerning the operation of the existing system, including but not limited to ensuring that the service levels are maintained and that Contractor is performing other duties as agreed to by State and Contractor under the Contract.

Contractor and State shall conduct semi-annual Operational Program Management Reviews (OPMRs) to guarantee that the hardware and software are adequate for State purposes and are consistent with then-current technology used in similar systems. Such evaluations shall include reviewing the available technology applicable to the ABIS, both from Contractor and third parties, and reviewing pending and implemented changes in NIST, EBTS, and other standards applicable to State or its remote sites. As may be required from time to time, Contractor and State shall determine any hardware or software changes that are needed to respond to such developments and to provide migration paths for such functional or technology updates. Such changes shall be provided at no cost to State beyond the service fees payable by State to Contractor.

As part of maintenance services, Contractor shall provide all hardware refreshes required during the entire term of the resultant Contract. Prior to commencing hardware refresh, Contractor shall submit for State approval technology refreshment specifications, which shall incorporate technological upgrades that are necessary to maintain ABIS performance at the requisite service levels and to improve such performance, including through additional functionality or in response to changes in technology, regulations or standards applicable to law enforcement promulgated by the FBI or Department of Homeland Security. Contractor shall furnish agendas, presentation materials, minutes and technical reports.

Scheduled Downtime and Preventive Maintenance

Contractor shall provide all maintenance services, including installation of software updates and hardware upgrades, during scheduled downtime, during late evening hours or early morning hours in order to avoid high volume times, including the weekend as the optional day for downtime, as agreed to by State. Scheduled downtime for performing preventive maintenance or other maintenance services at any site shall not exceed 90 minutes for each site in any month, unless agreed to in advance by State. Contractor is required to maintain electronic report of downtime events and provide monthly.

Contractor will perform a documented preventive maintenance procedure for all equipment and software they provide. Contractor shall periodically dispatch maintenance personnel to clean, inspect, and adjust the equipment and replace defective or worn parts thereof at the manufacturer's recommended frequency in order to keep the equipment in good operating condition. Contractor shall carry out periodic maintenance tasks on all electronic components they provide to ensure they are operating at maximum capability. Such maintenance shall be scheduled to be performed, at a minimum, once a month during hours agreed to by State.

Response and Resolution Monitoring

The Errors under this Contract may be identified either as a result of Contractor's use of its own monitoring system or discovered by State. Upon discovery of an Error by State, State will report the Error to Contractor's customer support for resolution.

Contractor shall maintain an electronic report log that indicates the Error report number, Error description, the time that the Error call was received, the Severity Level assigned, all actions taken, and the time that the Error was corrected. The Error report log shall be maintained in a database that is remotely accessible by State personnel.

Contractor may attempt to correct the problem by phone or remote access. If Contractor is unable to correct the problem in this manner, Contractor must begin on-site repair, depending on the availability of the site where the equipment resides. All situations that prevent the initiation of on-site repair will be documented in Contractor's electronic report log and reported to State.

Contractor shall provide State with direct access at any time to the data collected as a result response time monitoring. Whenever requested by State, Contractor shall provide State with reports and/or download that data along with all applicable documentation that may be necessary for State to independently monitor the response time of the system.

Contractor and State Responsibilities:

Contractor Responsibility	MSP Responsibility
System Operations Report	
• • Capacity and throughput reports. • Conduct semi-annual Operational Program Management Reviews.	• • Run system operation reports. • Participate in Operational Program Management Reviews.
LAN / WAN Administration and Supervision	
N / A	• Provide all LAN / WAN administration, supervision and support.
User Management	

Contractor Responsibility	MSP Responsibility
	• System administrators will perform user management actions, including: – Creating users. – Establishing and modifying user access rights. – Enabling and disabling user accounts. – Deactivating users.
Help Desk	
• Provide Call Center support accoding to your service level agreement, including a toll-free number and e-mail access. • Record and track all service calls in our database. • Provide dial-in support, as needed. • Dispatch local Customer Support Engineers, as required, in accordance with your service level agreement.	N / A
Delivery of Consumables	
N / A	• Responsible for all consumables to maintain operations of local workstations (for example, ink cartridges and paper)
System Monitoring	
• System administrators will monitor key components of the system, including: – Services, interfaces and databases. – Detecting sudden activity peaks and scaling system dynamically to make sure transactions are processed according to service level agreement. – Monitoring cloud services consumptions and alerting customer if usage exceeds expected levels.	• MSP System Administrator will be responsible for monitoring: – In-process transactions. – Notifications when an abnormal event is detected with regard to in-process transactions.

Contractor Responsibility	MSP Responsibility
– Notifications when an abnormal event is detected with regard to responsibilities outlined above.	
System and Transaction Management	
• System administrators will manage key components of the system, including: – Stopping and re-starting all services, interfaces, and databases of the system. – Maintaining system configuration information according to the Data and Property Management Plan *[DEL-32]*	• MSP System Administrator will be responsible for transactions management, including: – Stopping and re-starting all transactions in the system. – Enabling and purging transactions. – Changing transaction priority.
Storage Space Monitoring	
• Monitor storage usage, system capacity, and throughput and take appropriate action.	N / A
Data Backup Management	
• Perform daily / weekly backups of the system databases and verify the backups. • Responsible for making sure backup data is stored in a different geo-location than primary system (for example, Virginia, if main system is hosted in Iowa).	N/A

Table 1: Responsibilities for System Warranty and Maintenance Tasks

<table>
<tr><th>Contractor Responsibility</th><th>MSP Responsibility</th></tr>
<tr><td colspan="2">Hardware Preventive Maintenance</td></tr>
<tr><td>Perform all necessary preventive hardware maintenance for hardware and software provided by the Contractor.</td><td>Perform all necessary preventive hardware maintenance, for hardware and software (OS) provided by MSP such as any MSP provided network equipment.</td></tr>
<tr><td colspan="2">Software Preventive Maintenance</td></tr>
<tr><td>Perform log analysis, software updates, and load any software updates and upgrades required to ensure software is current and performing according to specification.</td><td>Confirm which software updates may be loaded, and approve the schedule. Coordinate with Contractor before loading “office related software” on an AFIS workstation.</td></tr>
<tr><td colspan="2">Anti-Virus</td></tr>
<tr><td>Run Windows anti-virus software on workstations prior to shipping, and on the backend system.
Assist MSP IT personnel with implementation of anti-virus update schema.
Pay for virus software updates.</td><td>Manage Workstation virus protection after the system is installed, including definition downloads, virus checking, and reporting.</td></tr>
<tr><td colspan="2">Performance Analysis and Tuning</td></tr>
<tr><td>Conduct monthly reviews of system capacity, usage, performance indicators, and event logs to identify potential problems before they happen.
Routinely evaluate performance indicators, make recommendations for altering system parameters and configurations to maintain optimum performance. Implement approved changes.
Semi-annually, conduct Operational Program Management Reviews.
Provide System Performance Report [DEL-31] and Technical Report [DEL-20].
After State acceptance, provide a Technical Refresh at Year 6 and Year 12 if the Contract utilzies available option years.</td><td>Participate in Operational Program Management Reviews.
Review and approve configuration changes.
Provide facility and IT support, as required, for updates, upgrades, and system refresh activities.</td></tr>
<tr><td colspan="2">Remedial Maintenance Support</td></tr>
<tr><td>Repair, replace, or upgrade hardware, as necessary, to ensure that all hardware is performing according to specification within the terms and conditions of the service level agreement.</td><td>N / A</td></tr>
</table>

Contractor Responsibility	MSP Responsibility
• Perform log analysis and technical investigations, as necessary, to diagnose system events. • Produce software updates and fixes within the conditions of the warranty and / or service level agreement. This may include source code analysis and patch creation. • Test and install software updates and fixes in the test environment within the terms and conditions of the warranty and / or service level agreement	
Spares Management	
• Maintain and manage an appropriate inventory of spare parts, and install spare parts, as necessary, in the event of a system failure.	N / A
Data Management	
• As necessary, perform record analysis to address issues, such as missed identifications or other record processing anomalies. • If the need arises, Contractor will be responsible for restoring system data to correct any data loss or corruption of the permanent databases within the limits of the service level agreement.	• Notify Contractor of any known anomalies, such as missed identifications.

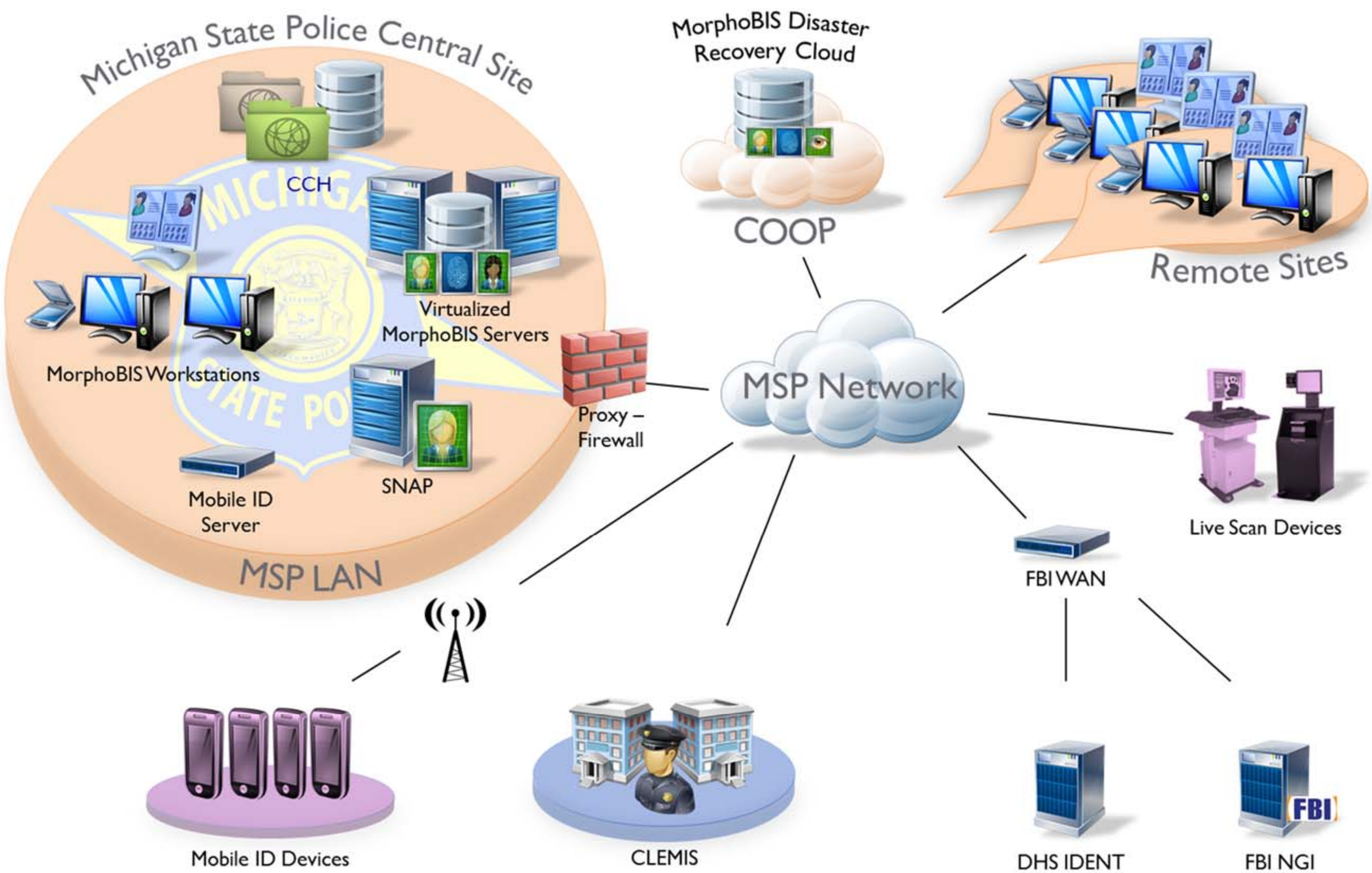
Continuity of Operations

As part of system maintenance, Contractor shall also be responsible for the provision of Continuity of Operations (COOP) services.

As part of COOP services, Contractor shall perform the functions; provide or utilize the facilities, equipment, supplies, data, and documentation; and conduct the training and exercises/drills specified in the COOP to maintain a viable COOP capability that ensures the performance of Contractor's essential functions during any emergency or situation that may disrupt normal operations and leave Contractor facilities damaged or inaccessible. Contractor shall be subject to the following requirements, which shall be contained in and are incorporated into the COOP Plan:

- Contractor shall have complete responsibility for restoration of the system.

- Any system error (as defined in the Service Level Agreements (SLA)) resulting from the actions or inactions of the Contractor shall require response times as defined in the SLAs, and failure to meet these requirements will result in the assessment of corresponding credits as defined.
- In the event of the declaration of a natural disaster, Contractor shall be required to maintain hourly communication with State about the outage and steps taken to restore the system in accordance with the disaster recovery plan and solution.
- Contractor shall be required to make a declaration of a disaster and invoke the Disaster Recovery Plan within 12 hours from the disruption of the operational environment or precipitating event.
- Contractor shall restore the system data to a point within 24 hours before the declaration of the disaster by State or Contractor.
- State shall be able to log on to the disaster recovery site within 48 hours of the declaration of the disaster by State or Contractor.
- Contractor shall have at a minimum 50 percent capacity within 48 hours and 100 percent capacity within 96 hours of the declaration of the disaster by State or Contractor.
- Contractor's failure to make a declaration of a disaster within 12 hours shall result in the incident and deemed unscheduled downtime.



Michigan State Police Central Site
CCH
MorphoBIS Workstations
Virtualized MorphoBIS Servers
Mobile ID Server
SNAP
Proxy – Firewall
MSP LAN
MorphoBIS Disaster Recovery Cloud
COOP
Remote Sites
MSP Network
Live Scan Devices
FBI WAN
Mobile ID Devices
CLEMIS
DHS IDENT
FBI
FBI NGI

(c) 1.200 Roles and Responsibilities

1.201 Contractor Staff, Roles And Responsibilities

A. Contractor Staff

Contractor shall establish a formal Contractor Program Management Office (PMO) responsible for executing the total effort required under the Contract. A clear line of program authority shall exist among all organizational elements, including subcontractors. Roles, responsibilities, authority structures, and reporting requirements shall be established for each organizational element.

The competence of the personnel the Contractor proposes for this project will be measured by the candidate's education and experience with particular reference to experience on similar projects as described in this Statement of Work. The Contractor will commit that staff identified in its proposal will actually perform the assigned work. All staff will be subject to full background checks.

The contractor will submit a letter of commitment for Key Personnel, signed by the identified resource, stating their commitment to work for the contractor/subcontractor on this project contingent on award of the bid. If the identified personnel are currently assigned to a State project the contractor should provide a letter signed by the State Project Manager releasing the individual from the project upon execution of the contract.

The State has identified the following as key personnel for this project:

- Project Manager
- Single Point of Contact (SPOC)
- Technical Lead
- *Systems Engineer*
- *Lead Trainer*
- Trainer

Proposed Resource Name:	Stephanie Leonard
Proposed Classification:	Project Manager
Key Personnel:	**Yes** ☒ or No ☐
Percentage of time resource will be allocated to project:	100%

Proposed Resource Name:	Douglas Meier
Proposed Classification:	Single Point of Contact (SPOC)
Key Personnel:	**Yes** ☒ or No ☐
Percentage of time resource will be allocated to project:	20%

Proposed Resource Name:	Won Kang
Proposed Classification:	Technical Lead
Key Personnel:	**Yes** ☒ or No ☐
Percentage of time resource will be allocated to project:	100%

Proposed Resource Name:	Alexis Alvarez
Proposed Classification:	Systems Engineer
Key Personnel:	**Yes** ☒ or No ☐
Percentage of time resource will be allocated to project:	50%

Proposed Resource Name:	Jim Kester
Proposed Classification:	Lead Trainer
Key Personnel:	**Yes** ☒ or No ☐

Percentage of time resource will be allocated to project:	Mr. Kester will be 100% allocated to the MSP ABIS project for approximately 4 weeks during the training phase of the project.

Proposed Resource Name:	Mike French
Proposed Classification:	Trainer
Key Personnel:	**Yes** ☒ or No ☐
Percentage of time resource will be allocated to project:	Mr. French will be 100% dedicated to the MSP ABIS project for approximately 4 weeks during the latent training phase of the project.

The Contractor will provide sufficient qualified staffing to satisfy the deliverables of this Statement of Work.
This would include, at a minimum, a Project Manager, Technical Lead and a person to which issues that may arise can be escalated, Single Point of Contact (SPOC). These shall all be separate individuals. A trainer will also need to be designated. These individuals will be those designated to interact directly with the State to insure a smooth transition to the new system. The project manager will coordinate all of the activities of the Contractor personnel assigned to the project and create all reports required by the State.

The Contractor's project manager responsibilities include at minimum:

- Shall be available to State management on a 24/7 basis.
- Manage all defined Contractor responsibilities in this Scope of Services
- Manage Contractor’s subcontractors, if any
- Develop the project plan and schedule, and update as needed
- Serve as the point person for all project issues
- Coordinate and oversee the day-to-day project activities of the project team
- Assess and report project feedback and status
- Escalate project issues, project risks, and other concerns
- Review all project deliverables and provide feedback
- Proactively propose/suggest options and alternatives for consideration
- Utilize change control procedures
- Prepare project documents and materials
- Manage and report on the project’s budget

The Contractor's Technical Lead responsibilities include at minimum:

- Handle and coordinate all technical issues and able to explain these to the customer

- Able to understand and explain all technical features and functions
- Coordinate and oversee all installation activities
- Test all installations and report any issues to both contractor and State project managers
- Proactively propose/suggest options and alternatives for consideration
- Work with State representatives on all installations
- Approve each installation site has been properly deployed and tested and notify the State when they can commence testing to approve the site

The Trainer's responsibilities include at minimum:

- Schedule and conduct trainings
- Provide documentation of an overview of the training

Single Point of Contact (SPOC) responsibilities include at minimum:

- Be the single point of contact to work through any issues not being handled to meeting the needs of the project.
- Supporting the management of the Contract. Have the authority to make decisions for the company and will be contacted in the event of any issues beyond the normal scope of the project and/or any issue that the MSP feels is not meeting the conditions of the negotiated contract
- Advise the State of performance under the terms and conditions of the Contract.

The State reserves the right to require a change with any current staff if the assigned staff is not, in the opinion of the State, adequately serving the needs of the State. All Key Personnel may be subject to the State's interview and approval process. Any key staff substitution should have a background check and have the prior approval of the State.

The Contractor will provide, and update when changed, an organizational chart indicating lines of authority for personnel involved in performance of this Contract and relationships of this staff to other programs or functions of the firm. This chart should also show lines of authority to the next senior level of management and indicate who within the firm will have prime responsibility and final authority for the work.

B. Supporting Team Roles and Responsibilities

Role	Responsibility	Qualifications
Interface Engineer	• Designs all interfaces according to the Interface Design Document and Database Design Document • Ensures the Test Procedures adequately test the interfaces • Troubleshoots any interface issues • Ensures the interfaces are fully functional after COOP failover	• Bachelor's Degree in Computer Science, a related discipline, or equivalent work experience • Experience in software design and development • Experience with JAVA programming and other languages • Experience with UNIX / Linux and Windows environment • Experience working with relational database management systems, preferably Sybase and Oracle • Experience with application development platforms for building enterprise applications involving workflow automation
Workflow Engineer	• Designs all workflows according to the System Design Document • Ensures the Test Procedures adequately test the workflows • Troubleshoots any workflow issues	• Bachelor's Degree in Computer Science, a related discipline, or equivalent work experience • Experience in software design and development • Experience with JAVA programming and other languages • Experience with UNIX / Linux and Windows environment • Experience working with relational database management systems, preferably Sybase and Oracle • Experience with application development platforms for building enterprise applications involving workflow automation

Role	Responsibility	Qualifications
Integration Engineer	• Leads integration efforts, ensuring all subsystems and interfaced systems function together • Troubleshoots integration issues	• Bachelor's Degree Computer Science, a related discipline, or equivalent work experience • Experience in network and database administration • Knowledge of all phases of product / system development • Experience working with Active Directory, infrastructure, message queues, Python, JAVE scripts, XLS, SOAP, UNIX / Linux and Windows environment • Experience with relational and object oriented databases, preferably Oracle and SQL • Knowledge of hardware installation and hardware configuration • Ability to troubleshoot and fine tune system performance
Frontend Design Engineer	• Ensures the workstation software is configured according to the System Design Document	• Bachelor's Degree in Computer Science, a related discipline or equivalent work experience • Experience in software design and development • Experience with JAVA programming and other languages • Experience with UNIX / Linux and Windows environment • Experience working with relational database management systems, preferably Sybase and Oracle

Role	Responsibility	Qualifications
Reports Engineer	• Ensures the system can produce all MSP required reports	• Bachelor's Degree in Computer Science, a related discipline or equivalent work experience • Experience with SQL queries and database scripting • Experience with reporting software to include Crystal Reports, Jasper Reports or comparable programs
Security Specialist	• Ensures the system meets all Contractor and MSP security requirements	• Bachelor's Degree in Computer Science, Information Systems, a related discipline or equivalent work experience • Five or more years network management systems and architectures, with a focus on security, performance, scalability, and reliability in LAN / WAN design and architecture • Experience in managing and integrating UNIX / Linus in a multi-platform environment • Experience with network related protocols and security • Demonstrated experience with bridging, routing, switching architectures, component and installation

Role	Responsibility	Qualifications
Data Migration Lead	• Leads the effort to configure our data migration software to meet MSP requirements • Monitors the quality of the migrated data and addresses any issues	• Bachelor's Degree in Computer Science, a related field or equivalent work experience • Five years prior experience in migration or related technical data analysis • Demonstrated analytical skills with the ability to collect, organize, analyze and disseminate technical information with detail and accuracy • Technical experience in data models, data mining and segmentation techniques • Knowledge and experience with databases • Oracle experience to include installation, configuration, tuning, and backup / restore required • Experience scripting in a Linux environment and SQL queries

Role	Responsibility	Qualifications
Test Engineer	• Involved in developing the TEMP *[DEL-04]*, Test Plans *[DEL-28]* and Test Procedures *[DEL-21]*, and produces the Test Reports *[DEL-06]* • Involved in conducting the Qualification Testing, FAT, SAT, and / or UAT	• Bachelor's Degree in Computer Science, Engineering or equivalent experience in a related field • Minimum three years of experience in software testing including developing test cases, planning , conducting tests and preparation of test analysis and reports • Experience with scripting and programming concepts such as Python • Experience working with automated and manual testing tools, troubleshooting UNIX / Linux, PC and network hardware • Demonstrated experience with JAVA / error diagnostics in JAVA based programs and database table queries
Product Engineering Lead	• Serves as the conduit for the project team for all Product Development ABIS product needs and issues	• Bachelor's Degree in Computer Science, Engineering or equivalent experience in a related field • Experience in product development and deployment

Role	Responsibility	Qualifications
Regional Customer Support Manager	• Provides the resources to perform the site surveys, ensures the development of the Installation Survey Reports *[DEL-27]* and Installation Plan *[DEL-16]*, and ensures the Customer Support Engineers install and track the System Hardware *[DEL-23]*, Software Licenses *[DEL-24]*, and System Data *[DEL-25]* according to the Configuration Management Plan *[DEL-29]* and the Data and Property Management Plan *[DEL-32]* • Ensures the system meets all operational performance requirements, manages the on-site personnel, and serves as the first-level escalation point for customer support issues • Manages 16 Customer Support Engineers (CSEs) in the Central Region • Allocates CSEs to support the transition phase between implementation and operations • Allocates additional CSEs where required within the region.	• Bachelor's Degree in Technical Field or equivalent work experience • Demonstrated experience in field service and customer support • In depth knowledge of central processing units and associated diagnostics • Problem solving skills including the ability to perform complex analysis of data and / or situational factors. • Strong computer skills with a good knowledge of Windows OD, hardware and software solutions • Demonstrated management skills to include support staff planning, oversight, tasking and escalation

Role	Responsibility	Qualifications
Customer Support Center Manager	• Manages the call center and produces the System Performance Report *[DEL-31]*	• Bachelor's Degree in Technical Field or equivalent work experience • Seven years of experience in field service or customer support responsible for 24 hour operation • Experience in the management of staff responsible for supporting central processing units and execution of associated diagnostics • Demonstrated analytical and problem solving skills. Analysis of complex data and / or situations requiring evaluation of multiple factors • Requires a strong knowledge of Windows OS, hardware and software solutions
Sales Representative	• Serves as a point-of-contact with the customer throughout the life of the contract to ensure client requirements are met and customer satisfaction is achieved and maintained • Participates in strategic planning with customers	• Bachelor's Degree in Business or Related Field or equivalent work experience • Demonstrated experience in translating public security technology into business solutions for public agencies • Minimum of three years managerial experience • Ability to work with customers to identify long term goals and define strategic plans for evolving agency needs

C. Subcontractors

D. On Site Work Requirements

1.Location of Work
The work is to be performed, completed, and managed at multiple locations throughout the State of Michigan as currently identified in Existing Systems Report - Appendix 1.

Additional sites in Michigan may be added or sites may be changed with notice to the vendor. These changes are not to affect the pricing.

The State reserves the right to modify the work location and hours in the best interest of the project.

Contractor shall observe the same standard holidays as State employees. The State does not compensate for holiday pay.

If the State is to host the Solution the Contractor must provide on-site support 8:00 a.m. to 5:00 p.m. EST, Monday through Friday, with work performed as necessary after those hours to meet project deadlines. No overtime will be authorized or paid.

Contractor will perform the following activities at our headquarters in Anaheim, CA

- Project planning and management
- Project Gate Reviews, including:
  - Product Test Readiness Review
  - Pre-Ship Readiness Review
  - System Test Readiness Review
- Development work
- Factory assembly and internal testing
- A Factory Acceptance Test (FAT) with the MSP's participation
- Electronic data migration

Contractor will perform paper card conversion at our subcontractor's facility in Plano, TX, including:

- Management of card transport to and from State facility
- Inventory / barcode cards
- Acquisition of demographic and image data
- Generation of NIST files for loading in production system

Contractor will perform the following activities at MSP's designated facilities.

- System Requirements Review

- System Design Review
- User Acceptance Test Readiness Review
- Operational Readiness Review
- Final Acceptance Review
- System installation (Workstations)
- System Acceptance Test (SAT) with the MSP's participation
- User Acceptance Test (UAT) with the MSP's participation
- User training
- System migration to transition from the legacy system to the new MSP MorphoBIS
- Record extraction to support data migration will be performed in coordination with MSP personnel

During the warranty and maintenance periods, Contractor will support the State's central and remote locations as specified in Statement of Work. We understand that sites may be added or changed and agree that pricing will not be affected.

2. Hours of Operation:

a. AFIS Central Site and Ten-print operations are 24 hours per day, 7 days, including holidays.
b. Remote latent sites are 8:00 a.m. to 5:00 p.m. EST, Monday through Friday, excluding State holidays.

3. Travel:

a. No travel or expenses will be reimbursed. This includes travel costs related to training provided to the State by Contractor.
b. Travel time will not be reimbursed.

4. Additional Security and Background Check Requirements:

Contractor shall afford State the opportunity to interview and investigate the personnel proposed by Contractor prior to granting them security access to State systems and sites, and State reserves the right to reject their access to ABIS equipment, files or site locations whenever Contractor personnel fail to maintain a clean criminal record or pass a background update procedure administered by and satisfactory to State, as further provided elsewhere in the Contract including the System Requirements Specifications [DEL-02].

Contractor shall afford State the opportunity to interview and investigate the personnel proposed by Contractor prior to granting them security access to State systems and sites, and State reserves the right to reject their access to ABIS equipment, files or site locations whenever Contractor personnel fail to maintain a clean criminal record or pass a background update procedure administered by and satisfactory to State, as further provided elsewhere in the Contract including the System Requirements Specifications [DEL-02].

The validity of any previous background check or drug test will be determined solely by the Michigan State Police. Any Background or drug test not found to be current and properly conducted, in the opinion of the MSP, will be re-administered for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card to the State and the FBI and will be subject to MSP criteria for any access to Criminal Justice Information.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

1.202 State Staff, Roles, And Responsibilities

The State project team will consist of Subject Matter Experts (SME's), and a DTMB and Agency project manager:

Subject Matter Experts
The Subject Matter Experts representing the business units involved will support the vision for the business design and how the application shall provide for that vision. They shall be available on an as needed basis.

Name	Agency/Division	Title	Phone/e-mail
Scott Blanchard	MSP	AFIS Manager	(517) 284-3168 BlanchardS1@michigan.gov
Craig Wilkinson	MSP	AFIS Programmer Specialist	(517) 243-4901 WilkinsonC@michigan.gov
Dana DuBois	MSP	Ten-print Manager	(517) 899-2099 DuBoisD2@michigan.gov

State Project Manager- (DTMB and Agency)
DTMB will provide a Project Manager who will be responsible for the State's infrastructure and coordinate with the Contractor in determining the system configuration.
The State's Project Manager will provide the following services:

- Provide State facilities, as needed
- Coordinate the State resources necessary for the project

- Facilitate coordination between various external contractors
- Facilitate communication between different State departments/divisions
- Provide acceptance and sign-off of deliverable/milestone
- Review and sign-off of reports and invoices
- Review project plan, status, and issues.
- Assist in escalating and resolving any issues or deviations from project plan
- Utilize change control procedures
- Conduct regular and ongoing review of the project to confirm that it meets original objectives and requirements
- Document and archive all important project decisions
- Arrange, schedule and facilitate State staff attendance at all project meetings.
- Support the management of the Contract.

Name	**Agency/Division**	**Title**
Scott Blanchard	MSP	AFIS Manager
Gordon Mayes	DTMB	DTMB Manager

DTMB shall provide a Contract Administrator whose duties shall include, but not be limited to, supporting the management of the Contract.

Name	**Agency/Division**	**Title**
Simon Baldwin	MDTMB	Contract Administrator

Contractor Responsibility	**MSP Responsibility**
Project Management Services	
Provide a Project Manager (PjM) to coordinate all design definition, engineering efforts, procurement, factory integration and testing, shipment, installation, site integration, acceptance testing, training, transition, and support activities. The PjM will also: Serve as primary customer contact and develop a close team environment among all personnel to facilitate a continuous transfer of knowledge throughout the contract.	Provide a Project Manager (or Program Manager) to review / approve all deliverables, Final Acceptance, and any Change Orders. Your PM should also: Serve as Contractor's primary point of contact. Coordinate Customer activities, including site preparation, installation support, integration testing support, acceptance testing, and training of your personnel. Act as liaison with your third-party agencies.

Contractor Responsibility	MSP Responsibility
Manage subcontractors. Develop and maintain the Project Management Plan and schedule. Conduct the project's status meetings and provide status reports. Draft and maintain an Issue / Action Log and Risk Spreadsheet. Resolve deviations from the project scope and administer change control.	Work with our personnel to verify the resolution of Action Item list issues. Ensure Contractor personnel have the necessary site access and a safe work environment.
Project Design Documentation	
Draft all Design Documentation.Provide design documentation to the MSP for review, comment, and approval.	Participate in Requirements gathering to support development of Design Documentation. Provide information regarding the current system performance and functionality. Review, provide feedback on and approval of the Project Design Documents. Issue Change Requests for any required changes to the approved documents in accordance with the defined procedures.
Electronic Data Migration	
Please see section on System Migration of this Statement of Work.	Please see section on System Migration of this Statement of Work.
Card Conversion	
Please see section on System Migration of this Statement of Work.	Please see section on System Migration of this Statement of Work.
Purchasing	
Verify that the proposal BOM is still valid and that no items have gone End-of-Life (EOL). Replacement items will be identified, if	

Contractor Responsibility	MSP Responsibility
necessary, and the MSP will be notified of the changes. Procure the hardware and third-party software listed on the BOM. Inventory the material. Stage the equipment for factory testing.	
Engineering Integration	
Configure the Contractor COTS software according to the requirements in the approved Design Documents: Develop, test, and implement workflows. Develop, test, and implement the interfaces (on Contractor software side) required for the system operation as defined in the Interface Design Documents (IDDs). Provide Simulators / Test Files for Contractor software to enable the MSP to test the external systems interfaces prior to the on-site integration. Simulators will reflect functionality, and scripts will be used to simulate performance of the actual system. Configure and test the user interfaces, access rights, scanning and printout formats, and reports for Contractor software according to the SDD *[DEL-14]*. Configure the data storage, backup, security, and user management for the items that are under Contractor responsibility. Load the software and converted / migrated data on the staged equipment and perform integration testing of basic functionality to verify the system is ready for testing. Conduct a Qualification Test Readiness Review (QTRR).	Develop, test, and implement any required interfaces from the MSP systems to the new Contractor system as required by the IDDs. Provide Test Files / Simulators for the external systems to enable Contractor to perform testing prior to the on-site integration. Configure the network (LAN / WAN) and security according to the SDD *[DEL-14]*.
Factory Testing	

Contractor Responsibility	MSP Responsibility
Draft a Test and Evalution Master Plan, Test Plan, and Test Procedures for the MSP's review and approval. The Test Procedures validate the approved requirements. Perform testing according to the approved Test Plan. Note that interfaces are simulated for all factory testing. Note any issues and their severity in the Contractor JIRA Ticket database, and track the resolution. Conduct the Product Test Readiness Review (PTRR). Conduct a Factory Acceptance Test (FAT) according to the approved FAT Test Plan. Track any issues found during the FAT on the Issue / Action Log and provide a plan for resolution.	Review, provide feedback on, and approve the Test Plan. Participate in the PTRR. Provide authorization to proceed with the FAT. Attend the FAT and participate in the testing. Provide test data according to the FAT Test Plan. For each test scenario, either provide approval or note discrepancies.
Site Preparation	
Perform site surveys and provide Installation Survey Reports. Provide site preparation documentation (Installation Plans and Installation Drawings) identifying the power, network, AC, space, cabling, access, security, and equipment layout requirements for system implementation.	Approve the scheduling of the hardware / COTS / Contractor software delivery. Identify the locations for each item procured. Provide an address, contact name, and contact phone number for each site. Provide access to the sites for site surveys by Contractor if necessary, and assist in the surveys. Provide the required layout information on the sites, as well as any known constraints. Review the site preparation documentation and confirm that there are no compliance issues. Prepare the sites and the interconnection of the sites according to the site preparation documentation. The MSP is responsible for the local area and wide area networks. Performance will be

Contractor Responsibility	MSP Responsibility
	affected by network bandwidth. Contractor requires a minimum 1 GB LAN for a Central site connection, and at least 10Mb dedicated network connection for each remote Review Station. The MSP is responsible for network and power reliability and availability. Failure in these areas cannot be counted against Contractor's reliability and availability of contractual requirements. Provide a formal notice for Contractor indicating that the site preparation has been completed, validated, and the interconnection is operational before equipment is shipped to the sites. If the network is not functioning according to the specifications when Contractor arrives for installation, requests for correction should be addressed within one day. Delays will impact the schedule and may result in charges for the additional labor, hotel, and per diem expenses for the duration of the extension for the employees on site. Provide a temporary storage area for the delivered hardware, if required.
Shipping and Delivery	
Provide a schedule for shipping and delivery to each site. Conduct the Pre-Ship Review. Securely crate or palletize all deliverables. Provide shipping manifests that identify all items, including serial numbers. Arrange for the secure shipping of all hardware, and third-party and Contractor software to the designated target sites.	Approve the schedule for shipment and delivery of the hardware and software for each site. Participate in the Pre-Ship Review. Provide ship authorization. Receive all material and immediately notify Contractor of any visible damage to shipping containers. Provide temporary storage for the delivered hardware, if required.

Contractor Responsibility	MSP Responsibility
Installation and On-Site Integration Testing	
Propose the site-by-side installation schedule in advance of delivery. Unpack, inventory, and install all equipment. Power up the equipment and verify connectivity between components. Troubleshoot any installation issues. Run on-site Engineering Site Tests with the external systems. Identify any open issues prior to Acceptance Testing. Conduct the System Test Readiness Review,	Confirm the installation schedule in advance of delivery. Provide access to the sites for Contractor and Contractor sub-contractors as required. Provide the support for site and security issues. Ensure timely IT support availability for addressing network issues. Arrange for access to test beds for interfaced systems (for example, regional AFIS, FBI, etc.). Provide access to the site 8 a.m. to 8 p.m., Monday through Saturday, with escort, if required. Participate in the System Test Readiness Review. Provide authorization to proceed with SAT.
Site Acceptance Test (SAT)	
Organize the SAT and run the tests according to the approved Test Plan. Track any issues found during the SAT in the Issue / Action Log and provide a plan for resolution. Fix the Issue / Action Log issues, re-run the failed tests, and issue a report for a SAT re-test. Conduct an Operational Readiness Review.	Participate in the SAT, signing off on passed tests and identifying any failed requirements. Validate the fixes during re-testing and sign-off on the SAT. *Note: Expected results for accuracy and / or performance are described in the technical proposal. Conformance and potential deviations on specific tests will be reviewed with respect to expected results, data quality, and other potential factors, in reference with FBI standards and Industry practices.* Participate in the Operational Readiness Review. Provide approval to proceed with User Acceptance Testing.

Contractor Responsibility	MSP Responsibility
Training Documentation	
Deliver the user manuals for Contractor Trak applications. Deliver the administrator manual(s) for the system. Deliver all other contracted training materials.	Make unlimited electronic copies for internal use, as needed.
Training	
Draft the Training Plan and training schedule based upon your specific organizational and contractual requirements. Provide all training according to the approved Training Plan. Provide attendance sheets and training certificates. Provide, collect, and review feedback forms. Provide contact information for follow-up questions.	Review, comment on, and approve the Training Plan and training schedule. Ensure availability of the trainees and confirm they meet any prerequisite requirements. Provide a meeting room and projection equipment for the classroom training. Provide feedback on the training courses.
User Acceptance Test (UAT)	
Organize the UAT and run the tests according to the approved Test Plan. Track any issues found during the UAT in the Issue / Action Log and provide a plan for resolution. Fix the Issue / Action Log issues, re-run the failed tests, and issue a report for a SAT re-test.	Determine which cases will be run on the ABIS. Coordinate communications with the managers of any interfaced livescans to arrange for dual submission (if necessary). Participate in the UAT, signing off on passed tests and identifying any failed requirements. Validate the fixes during re-testing and sign-off on the UAT. *Note: Expected results for accuracy and / or performance are described in the technical proposal. Conformance and potential deviations*

Contractor Responsibility	MSP Responsibility
	on specific tests will be reviewed with respect to expected results, data quality, and other potential factors, in reference with FBI standards and Industry practices.
Cutover	
Provide a full Transition Plan and schedule. Place the system in production status. Closely monitor the system performance to ensure transactions are being processed properly. Provide issue reports to the MSP Project Manager. Complete a final residual migration / conversion and load records. Conduct a Final Acceptance Review. Submit a request for Final Acceptance.	Provide the staffing necessary to support cutover. Notify remote sites of any downtime scheduled and how to report problems. Coordinate communications with the managers of any interfaced systems to support the transition from test mode to live mode. Assist in obtaining records for the residual conversion. Participate in the Final Acceptance Review. Provide Final Acceptance.
Travel	
Organize Contractor personnel travel. Pay for Contractor personnel travel expenses.	Organize any Customer personnel travel. Pay for Customer personnel travel expenses.

(d) 1.300 Project Plan

1.301 Project Plan Management

Preliminary Project Plan
Contractor will provide a Preliminary Project Plan with the proposal for evaluation purposes, including necessary time frames and deliverables for the various stages of the project and the responsibilities and obligations of both the Contractor and the State.

1. In particular, the Preliminary Project Plan will include a MS Project plan or equivalent (check the SUITE/PMM standard):
    1. All Work described in this SOW and attachments, including:
        a. All deliverables, including those referenced in the pricing schedule,
        b. All tasks, subtasks, deliverables, and other work,

c. Associated dependencies, if any, among tasks, subtasks, deliverables, and other work,
d. Resources assigned to each task, subtask, deliverable, and other work,
e. Start date and date of completion for each task, subtask, deliverable, and other work,
f. Proposed State review period for each deliverable,
g. Proposed milestones, and
h. Other information reasonably required by State;

2. Identification of all Contractor key personnel and Contractor key staff;
3. A deficiency management plan, documenting the approach to deficiency management, including methodology, recommended tool(s), and escalation process;
4. Approach to project communications;
5. A risk management plan, documenting the approach to risk analysis (e.g., the evaluation of risks and risk interactions to assess the range of possible project outcomes), risk mitigation (e.g., the identification of ways to minimize or eliminate project risks), risk tracking/control (e.g., a method to ensure that all steps of the risk management process are being followed and, risks are being mitigated effectively) and clearly establishing a process for problem escalation, to be updated, as needed, throughout the term of the Contract;
6. Initial identification of risks that may impact the timely delivery of the Solution;
7. Project staffing and resource management plan; and
8. Configuration and change management plan. Changes, in this context, refer to changing the functionality of, or adding additional functionality (e.g., changes to the project scope) to, any Solution component. The approach shall ensure that the impact and rationale for each change are analyzed and coordinated prior to being approved.

2. The Preliminary Project Plan shall include the following deliverable/milestones for which payment shall be made.
   a. Payment to the Contractor will be made upon the completion and acceptance of the deliverable or milestone, not to exceed contractual costs. A milestone is defined as complete when all of the deliverables within the milestone have been completed.

Note: A Final Project Plan will be required as stated in Article 1, Section 1.301 Project Control below.

Orientation Meeting
Upon 15 calendar days after receipt of the Purchase Order, the Contractor will be required to attend an orientation meeting to discuss the content and procedures of the Contract. The Contractor will be required to facilitate this Meeting with support from the State. The meeting will be held in Lansing, Michigan, at a date and time mutually acceptable to the State and the Contractor. The State shall bear no cost for the time and travel of the Contractor for attendance at the meeting.

Performance Review Meetings

All Project Meetings and Technical reviews will be conducted at a State facility located in Lansing MI, at the Vendor's facility, or by teleconference at a date and time mutually agreed upon. The State shall bear no cost for the time and travel of the Contractor for attendance at any meeting required under this SOW at the State's location.

Contractor shall furnish all agendas, presentation materials, and minutes for all meetings required under this SOW regardless of location.

Contractor's Project Manager shall prepare and present to State's Project Manager written status reports documenting project progress, plans, and outstanding issues, in accordance with the Reports Section 1.302.

State and Contractor shall meet at least weekly in person, by telephone or through the provision of e-mail updates exchanged between their respective Program Managers unless the parties otherwise mutually agree in writing via their respective Program Managers. Contractor must attend, in person, at least quarterly. Attendees at the meetings will include State and its staff and Contractor and subcontractors personnel, as determined by State and Contractor management. The objectives of the weekly meetings are (i) to confirm that the program is not encountering technical problems that would cause the program to fail to maintain the agreed-upon service levels, (ii) to provide immediate feedback to the parties to permit any issues to be resolved on a timely basis, (iii) to provide a contemporaneous record showing that the parties have acted to ensure that the program is progressing in accordance with prior agreements, and (iv) to ensure that parties are proactively identifying and addressing issues that could adversely affect service levels.

Contractor shall participate in an on-site System Test and Operational Readiness Review meeting at a State facility 30 days prior to the scheduled date for declaring State's Initial Operational Capability (IOC). The purpose of the meeting is to introduce key State and Contractor operations and operations support personnel, discuss plans, examine the status of any risks or issues, and address any other issues that State and/or Contractor may wish to discuss.

Contractor shall conduct management and technical reviews and provide management and technical reports throughout the System Operation and Support phase of the Contract. Contractor shall log all transaction and system activity necessary to evaluate Contract performance, facilitate trend analysis, and support system and other transactional analysis [System Performance Report DEL-31]. Contractor shall supply appropriate quality assurance and audits to ensure that logs are complete and accurate.

Contractor shall conduct semi-annual Operational Program Management Reviews (OPMRs). Attendees at the OPMRs will include State and its staff and Contractor and subcontractors staff, as necessary. The first OPMR shall be held within 60 days after the IOC. Each OPMR shall address:

- Performance against SLAs.
- Financial and schedule status.
- Planned activities.
- Action item status.
- Problem report status.
- Configuration management and quality assurance reporting.
- Issues and risks.
- Other service level shortfalls and plans for corrective action.

The OPMRs shall also address selected technical and programmatic topics as directed by State.

When the OPMR is held at a State's location, Contractor shall make available the key personnel necessary to carry out an efficient and effective agenda and shall provide presentation materials and supporting data.

Project Control

Contractor's Project Manager shall provide full project management and control of project activities.

State shall work closely with Contractor during the preparation of the Final Project Management Plan. The Final Project Management Plan may be modified only if such modification has been approved in advance in writing by State's Project Manager. The Project Management Plan shall be the basis for the Project Schedule, which shall be updated upon finalization of the Project Management Plan. Failure to provide deliverable/milestone by the identified date may be subject to liquidated damages (See Section 1.502 Final Acceptance).

Contractor shall develop an Integrated Master Schedule (IMS) [DEL-03]) and keep it current throughout the System Implementation phase of the Contract. The IMS shall be resource-loaded and shall include, at a minimum, all activities required under this SOW, including all management and technical reviews. The IMS shall identify activities by applicable Site (primary site, Continuity of Operations [COOP] site, and remote sites). The IMS shall identify any schedule margin/reserve. The IMS shall provide sufficient detail to demonstrate confidence that the schedule is complete and realistic. The IMS shall identify due dates associated with any State-furnished items (e.g., information, data, facilities access) and due dates associated with all Contractor deliverable items.

I. The Contractor will carry out this project under the direction and control of MDTMB and MSP.

II. Upon 30 calendar days after receipt of the Purchase Order the Contractor will submit to the State project manager(s) for final approval of the project plan. This project plan must be in agreement with all activities required under this SOW, developed in State-specified version of Microsoft Suite Product (currently 2010), and at a minimum, must include the following:

1. All Work described in this SOW and attachments, including:
    a. All deliverables, including those referenced in the pricing schedule,
    b. All tasks, subtasks, deliverables, and other work,
    c. Associated dependencies, if any, among tasks, subtasks, deliverables, and other work,
    d. Resources assigned to each task, subtask, deliverable, and other work,
    e. Start date and date of completion for each task, subtask, deliverable, and other work,
    f. Proposed State review period for each deliverable,
    g. Proposed milestones, and
    h. Other information reasonably required by State;
2. Identification of all Contractor key personnel and Contractor key staff;
3. A deficiency management plan, documenting the approach to deficiency management, including methodology, recommended tool(s), and escalation process;
4. Approach to project communications;
5. A risk management plan, documenting the approach to risk analysis (e.g., the evaluation of risks and risk interactions to assess the range of possible project outcomes), risk mitigation (e.g., the identification of ways to minimize or eliminate project risks), risk tracking/control (e.g., a method to ensure that all steps of the risk management process are being followed and, risks are being mitigated effectively) and clearly establishing a process for problem escalation, to be updated, as needed, throughout the term of the Contract;
6. Initial identification of risks that may impact the timely delivery of the Solution;
7. Project staffing and resource management plan; and
8. Configuration and change management plan. Changes, in this context, refer to changing the functionality of, or adding additional functionality (e.g., changes to the project scope) to, any Solution component. The approach shall ensure that the impact and rationale for each change are analyzed and coordinated prior to being approved.

III. The Contractor will manage the project in accordance with the State Unified Information Technology Environment (SUITE) methodology, which includes standards for project management, systems engineering, and associated forms and templates which is available at http://www.michigan.gov/suite

a. Contractor will use an automated tool for planning, monitoring, and tracking the Contract's progress and the level of effort of any Contractor personnel spent performing Services under the Contract. The tool shall have the capability to produce, but not limited to:
   - Staffing tables with names of personnel assigned to Contract tasks;
   - Project plans showing tasks, subtasks, deliverables, and the resources required and allocated to each (including detailed plans for all Services to be performed within the next 7 calendar days, updated monthly);
   - Updates must include actual time spent on each task and a revised estimate to complete; and
   - Graphs showing critical events, dependencies and decision points during the course of the Contract.

b. Any tool(s) used by Contractor for such purposes must produce information of a type and in a manner and format that will support reporting in compliance with the State standards.

IV. Within 120 days of Contract execution, the Contractor must provide the Disaster Recovery Plan to the State for their review.

The Contractor will provide the following deliverables in advance of the stated delivery dates.

Document No.	Deliverable/Plan Title	Delivery Dates
DEL-01	Project Management Plan	Update within 30 days after the effective date of the Contract.
DEL-02	System Requirements Specifications	At System Requirements Review.
DEL-03	Integrated Master Schedule	Update at Project Management Reviews.
DEL-04	Test and Evaluation Master Plan	Update within 30 days after the effective date of the Contract.
DEL-05	Migration Plan	At System Design Review.
DEL-06	Test Report – several sets, each corresponding to the outcomes of Factory Acceptance Test, System Acceptance Test and User Acceptance Test	For each increment, at Pre-Ship Review and Operational Readiness Review.
DEL-07	Agenda	5 business days prior to a meeting.
DEL-08	Presentation Materials	Draft – 5 business days prior to a meeting, with updates – at the meeting and final – as part of DEL-09.
DEL-09	Minutes	Draft – 2 business days after the meeting, with final – 5 business days after receipt of State comments.

Document No.	Deliverable/Plan Title	Delivery Dates
DEL-10	Security Plan	Update within 30 days after the effective date of the Contract.
DEL-11	User Manuals	At each training session and for online reference.
DEL-12	Database Design Document	Draft – 5 business Days prior to System Design Review, with updates – at the review, and Final as part of DEL-09.
DEL-13	Interface Design Document	Draft – 5 Business days prior to System Design Review, with updates – at the review, and final – as part of DEL-09.
DEL-14	System Design Document	Draft – 10 business days prior to System Design Review, with updates – at the review, and final – as part of DEL-09.
DEL-15	Bill of Materials	At System Design Review with updates – at Pre-Ship Review.
DEL-16	Installation Plan	For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review.
DEL-17	Training Plan	At System Design Review with updates – at Pre-Ship Review.
DEL-18	Installation Drawings	At System Design Review with updates – at Pre-Ship Review.
DEL-19	Training Materials	For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review.
DEL-20	Technical Report	As specified in Management and Technical Reporting and Technology Refresh and Enhancements Reviews or as required or requested by State.
DEL-21	Test Procedures	Draft – 30 working days prior to Product Test and Readiness Review and System Test and Readiness Review, with updates – at the review, and final – as part of DEL-09.
DEL-22	COOP Plan	At System Design Review with revision – at Pre-Ship Review.
DEL-23	System Hardware	Prior to Operational Readiness Review.
DEL-24	Software Licenses	Prior to Operational Readiness Review.
DEL-25	System Data	Prior to Operational Readiness Review.
DEL-26	Version Description Document	At Pre-Ship Review with updates – at Operational Readiness Review and Final Acceptance Review.
DEL-27	Installation Survey Report	At completion of each site survey.
DEL-28	Test Plan	At System Design Review with revision – at Test Readiness Review.
DEL-29	Configuration Management Plan	Within 30 days after the effective date of the Contract.

Document No.	Deliverable/Plan Title	Delivery Dates
DEL-30	Requirements Verification and Traceability Matrix	Draft – 5 business days prior to System Design Review, with updates – at the review, and final – as part of DEL-09.
DEL-31	System Performance Report	Periodic logs of all transaction and system activity necessary to evaluate Contract performance and to facilitate trend analysis, support system and other transactional analysis.
DEL-32	Data and Property Management Plan	Contractor shall develop, document and implement comprehensive procedures for the management of data, documentation and State property (equipment, hardware or software that belongs to State).

1.302 Reports

Contractor's Project Manager shall present to State's Project Manager written status reports documenting project progress, plans, and outstanding issues. Contractor's Project Manager shall meet with or conduct a status update conference with State's Project Manager on a weekly basis, or as otherwise agreed to by State and Contractor, to review project status reports and any related matters. All variances shall be presented to State for approval at the status meetings.

Reporting formats must be submitted to the State's Project Manager for approval 30 calendar days after receipt of the Purchase Order. Once both parties have agreed to the format of the report, it shall become the standard to follow for the duration of the contract.

Contractor prepared status reports, shall include, but are not limited to:

- *Project planning and direction;*
- *Weekly Project status;*
- *Monthly written Project Plan update reports; Updated project plan, requirement specifications, software/hardware modifications, etc.;*
- *Evaluation of results and status reporting;*
- *Contractor staffing and personnel matters, including management of Contractor technical staff;*
- *Summary of activity during the report period;*
- *Accomplishments during the report period;*
- *Deliverable status;*
- *Schedule status;*
- *Action Item status;*
- *Issues;*
- *Change Control; and*
- *Repair status*

- *System Performance Report*
- *Maintenance Activity*
- *Hosting Activity*
- *Disaster Recovery*

(e) 1.400 Project Management

Contractor shall provide full project management, planning, monitoring, supervision, tracking and control of all project activities during the term of the resultant Contract. Contractor shall employ project management industry standards and practices in the performance of all Work.

Contractor shall provide ongoing project administration, which shall include, but is not limited to, the following:

- Agenda;
- Presentation Materials;
- Minutes;
- Weekly status update conferences;
- Attendance at meetings with State Executives and Management as needed; and
- Updates to the Project Management Plan and the Project Schedule.

1.401 Issue Management

An issue is an identified event that if not addressed may affect schedule, scope, quality, or budget.

The Contractor shall maintain an issue log for issues relating to the provision of services under this Contract. The issue management log must be communicated to the State's Project Manager on an agreed upon schedule, with email notifications and updates. The issue log must be updated and must contain the following minimum elements:

- Description of issue
- Issue identification date
- Responsibility for resolving issue.
- Priority for issue resolution (to be mutually agreed upon by the State and the Contractor)
- Resources assigned responsibility for resolution
- Resolution date
- Resolution description

Issues shall be escalated for resolution from level 1 through level 3, as defined below:

Level 1 – Business leads
Level 2 – Project Managers

Level 3 – Project Sponsors

Example of an Issue / Action Log

This format is also used for tracking Test Report issues.

Item #	Esc, Level	Title - Description	Comments / Resolution	Status	Priority High / Med / Low	Owner	Report Date	Target Date	Complete Date
1	1	Printing – Name field is not properly aligned	Code complete – test on site	Open	Med	Contractor Technical Lead	21-Apr-17	31-Apr-17	

In accordance with State Guidelines, issues will be escalated from Level 1 through Level 3, as defined below:

Level 1: Business Leads

Level 2: Project Managers

Level 3: Project Sponsors

In addition to capturing general implementation issues, the Issue / Action Log will be used to consolidate issues discovered during the FAT, SAT, and UAT, and track their resolution.

1.402 Risk Management

A risk is an unknown circumstance or event that, if it occurs, may have a positive or negative impact on the project.

The Contractor is responsible for establishing a risk management plan and process, including the identification and recording of risk items, prioritization of risks, definition of mitigation strategies, monitoring of risk items, and periodic risk assessment reviews with the State.

A risk management plan format shall be submitted to the State for approval within 30 calendar days after receipt of the Purchase Order. The risk management plan will be developed during the initial planning phase of the project, and be in accordance with the State's PMM methodology. Once both parties have agreed to the format of the plan, it shall become the standard to follow for the duration of the contract. The plan must be updated bi-weekly, or as agreed upon.

The Contractor shall provide the tool to track risks. The Contractor will work with the State and allow input into the prioritization of risks.
The Contractor is responsible for identification of risks for each phase of the project. Mitigating and/or eliminating assigned risks will be the responsibility of the Contractor. The State will assume the same responsibility for risks assigned to them.

Risk Management Approach

Risk Identification
The first phase of project risk management consists of identifying all possible risks likely to impact the success of the project. A risk is defined as the probability of an undesirable event occurring with a potential negative impact to the project performance, cost, and / or schedule.
Risks can be broken down into the following categories:

- Technical
- Product
- Implementation
- Supportability

Risk Areas and Mitigation

Risk Area	Contractor's Approach
Technical	The most accurate lights-out matching as proven in NIST benchmarks and by the use of our algorithms in the FBI's NGI system.
Product	Proven, mature products, built on a COTS hardware platform.
Implementation	We know how to implement complex systems. We have installed more state-wide AFIS solutions than any other vendor. As the provider of the FBI NGI fingerprint, palm print, and latent matching solution, we offer the most interoperability with the NGI system.
Supportability	Our standards-based solution uses service-oriented architecture (SOA), which simplifies upgrades and expansions. Most software updates can be pushed out to the workstations from the Central site. Our development organization is headquartered in Anaheim, not Asia, so we are easily accessible for any troubleshooting help. Our Customer Support organization is highly rated by our customers. We received a 99% overall satisfaction rating in a 2015 Customer Satisfaction survey.

Risk Assessment

The second phase of project risk management consists of risk analysis and assessment. Having identified the possible risks, the next phase is to analyze them. Risk analysis involves the identification of risks and determining both the probability (quantification) and seriousness (consequences) of the possible outcomes. These two factors are multiplied together to obtain an overall risk criticality, as shown in Table 10.

The Risk Analysis Section of the Spreadsheet

Risk Effects	Cost of Risk Occurring	Initial Risk Assessment			
		Probability	Seriousness	Criticality	Control
Multiple review cycles resulting in schedule slip as approval of Design Documents is critical path, or possible rework, if issues are found during the FAT.	TBD	2	2	4	

Risk Mitigation

The third phase of project risk management consists of risk mitigation planning. A risk mitigation plan is established for each managed risk. The focus of the mitigation plan is to reduce the level of each risk by increasing the number of choices available and / or reducing the probability of occurrence, as shown in **Error! Reference source not found.**.

Risk Mitigation Tracking

Risk mitigation planning and tracking helps ensure the best possible outcome.

Mitigation Strategy	Mitigation Plan	Cost to Mitigate the Risk	Risk Owner

Protect (reduce effect)	Involve key users in the design process and early testing to get their buy-in	MSP to determine	MSP PM / Contractor PM

The choices of Risk Mitigation Strategy include:

Accept: adopted when mitigation taken would be more harmful than the effects of the risk.

Avoid: consists of not performing the activity presenting the risk.

Transfer: consists of having the activity presenting the risk performed by another participant who accepts responsibility for the risk.

Prevent: consists of actions on causes that aim to reduce the probability of the risk.

Protect: consists of actions on the potential effects that aim to reduce the seriousness of the risk.

The Mitigation Plan defines action steps to be taken. Any associated costs are identified and added to the spreadsheet. The Risk Owner is identified.

(f) Risk Review

The fourth phase of project risk management consists of risk review and control. Contractor's Project Manager, with the involvement of the MSP, will continually monitor and manage the risk issues identified at contract initiation and any additional risks identified during project implementation.

Risk Assessment Tracking

The Risk Assessment is updated after a mitigation strategy has been implemented.

Mitigation Dates			Updated Risk Assessment				Comments
Planned Closure Date	New Closure Date	Actual Closure Date	Probability	Seriousness	Criticality	Control	
TBD					-		

On a regular basis (for example, weekly or biweekly, as required), the Management Team will monitor and evaluate the risk list shown in the table above. The team will review progress towards closure, risk measurements, and updated analyses. When resolved, the team may upgrade or remove risks from the list.

1.403 Change Management

Project Change Management

The Contractor will employ the change control methodologies to justify changes and to ensure those changes will not adversely affect performance or availability.

Change management is defined as the process to communicate, assess, monitor, and control all changes to system resources and processes. The State also employs change management in its administration of the Contract.

The Contractor must employ change management procedures to handle such things as “out-of-scope” requests or changing business needs of the State while the migration is underway.

Referenced or applicable documents cited within the resultant Contract, including this SOW, shall be considered compliance documents for the purpose of the Contract. State recognizes that some of the compliance documents and their associated data items listed below may change. Throughout the term of the Contract, Contractor or State may propose compliance with newer documents and their associated data items that replace or supersede those identified in this list. To substitute newer documents and their associated data items, Contractor shall perform all of the following, in the order as listed:

1. Identify existing standards and data items to be replaced;
2. Identify new documents and associated data items proposed for use;
3. Provide a rationale for using the new items including cost, schedule, performance, and supportability impact; and
4. Obtain State approval.

Contract Change Management

If a proposed contract change is approved by the Agency, the Contract Administrator will submit a request for change to the Department of Technology, Management and Budget, Procurement Buyer, who will make recommendations to the Director of DTMB-Procurement regarding ultimate approval/disapproval of change request. If the DTMB Procurement Director agrees with the proposed modification, and all required approvals are obtained (including State Administrative Board), the DTMB-Procurement Buyer will issue an addendum to the Contract, via a Contract Change Notice. **Contractors who provide products or services prior to the issuance of a Contract Change Notice by the DTMB-Procurement, risk non-payment for the out-of-scope/pricing products and/or services.**

(g) 1.500 Acceptance

1.501 Criteria

The following criteria will be used by the State to determine Acceptance of the services and/or deliverables provided under this SOW.

The system shall be deemed accepted by the State and final payment will be paid by the State when the standard of performance is met as defined below.

Acceptance – The State is responsible for final acceptance of the software using an integrated Performance and Reliability Evaluation (PARE) as described below. The PARE process applies specifically to the CAS applications.

1. Determination of System Readiness Application
    - i. Prior to the PARE, a committee of four (4) persons will be identified to evaluate the performance on a daily basis. The committee will consist of one Contractor representative, two MSP representatives, and one DTMB representative.
    - ii. The PARE will begin when the Contractor certifies in writing that the solution is ready for use by the State.
    - iii. A functional benchmark demonstration will be run for the PARE Committee to confirm that the solution is operating and integrating per contract. This run must be completed to the satisfaction of the PARE Committee.
2. Standard of Performance
    - i. The performance period (consisting of ninety (90) consecutive calendar days) shall commence when the system is fully operational and system is ready for full production use. The date and time of the start of the PARE will be agreed upon by the Contractor and the State.
        1. During the successful performance period, all rerun time resulting from State equipment failure shall be excluded from the performance period hours. Equipment failure down-time shall be measured by those intervals during the performance period between the time that the Contractor is notified of equipment failure and the time that the equipment is returned to the State in operating condition. Any solution failure within the ninety (90) consecutive calendar days PARE, for a cause other than those identified above, will cause a re-start of the PARE.
        2. During the successful performance period, a minimum of two thousand one hundred sixty (2,160) hours of operational use time on each component will be required as a basis for computation of the average effectiveness level.
            - a. The average effectiveness level is a percentage figure determined by dividing the total operational use time by the total operational use time plus associated down-time.
            - b. If each component operates at an average level of effectiveness of 99.8 percent or more for a period of ninety (90) consecutive calendar days from the commencement date of the performance period, it shall be deemed to have met the State's standard of performance.
            - c. The State shall notify the Contractor in writing of the successful completion of the performance period.
            - d. The software shall operate in substantial conformance with the Contractor's published specifications applicable to such equipment on the date of this Contract.

e. If successful completion of the PARE is not attained within one-hundred and eighty (180) consecutive calendar days from the original start date of the PARE, the State shall have the option of terminating the Contract, or continuing the performance tests. The State's option to terminate the contract shall remain in effect until such time as a successful completion of the performance period is attained. The Contractor shall be liable for all outbound preparation and shipping costs for contracted items returned under this clause.
f. The PARE will be complete when the equipment has met the required effectiveness level of the prescribed time period.

3. Acceptance testing identified above must be sufficiently detailed to demonstrate the system's compliance with key criteria of the contract. At a minimum, the acceptance testing will confirm the following:
   i. Functional – the capabilities of the system with respect to the functions and features described in the technical portion of the contract.
   ii. Performance – the ability of the application to perform the workload throughput requirements. All problems should be completed satisfactorily within the allotted time frame.

Document Deliverables

1. Documents are dated and in electronic format, compatible with State of Michigan software.
2. Requirements documents are reviewed and updated throughout the development process to assure requirements are delivered in the final product.
3. Draft documents are not accepted as final deliverables.
4. The documents will be reviewed and accepted in accordance with the requirements of the Contract and Appendices.
5. DTMB and MSP will review documents within a mutually agreed upon timeframe.
   a. Approvals will be written and signed by DTMB and MSP Project Manager.
   b. Issues will be documented and submitted to the Contractor.
   c. After issues are resolved or waived, the Contractor will resubmit documents for approval within 30 days of receipt.

Software Deliverables - Software includes, but is not limited to, software product, development tools, support tools, data migration software, integration software, and installation software.

1. Beta software is not accepted as final deliverable.
2. The software will be reviewed and accepted in accordance with the requirements of the contract.
3. DTMB and MSP will review software within a mutually agreed upon timeframe for acceptance of functionality, usability, installation, performance, security, standards compliance, backup/recovery, and operation.
   a. Approvals will be written and signed by DTMB and MSP Project Manager.
   b. Unacceptable issues will be documented and submitted to the Contractor.
   c. After issues are resolved or waived, the Contractor will resubmit software for approval within 30 days of receipt.

4. Software is installed and configured, with assistance from DTMB and MSP, in an appropriate environment (e.g. development, conversion, QA testing, UAT testing, production, and training).
5. Contingency plans, de- installation procedures, and software are provided by the Contractor and approved by DTMB and MSP Project Manager.
6. Acceptance of the software will depend on the successful completion of User Acceptance Testing (UAT) and successful completion of the PARE.
7. Testing will demonstrate the system's compliance with the requirements of the contract. At a minimum, the testing will confirm the following:
    a. Functional - the capabilities of the system with respect to the functions and features described in the contract.
    b. Performance - the ability of the system to perform the workload throughput requirements. All problems should be completed satisfactorily within the allotted time frame.
8. DTMB and MSP will review test software, data, and results within a mutually agreed upon timeframe.
    a. Approvals will be written and signed by DTMB and MSP Project Manager.
    b. Unacceptable issues will be documented and submitted to the Contractor.
    c. After issues are resolved or waived, the Contractor will resubmit test software, data and results for approval within 30 days of receipt.

9. Software source code, where applicable, is reviewed by DTMB and MSP within a mutually agreed upon timeframe for readability, structure, and configuration management.
    a. Approvals will be written and signed by DTMB Project Manager.
    b. Unacceptable issues will be documented and submitted to the Contractor.
    c. After issues are resolved or waived, the Contractor will resubmit source code for approval.

1.502 Final Acceptance

Upon the successful completion of UAT through COOP Plan, State will conduct a Final Acceptance Review (FAR) to determine whether Contractor has satisfied the terms and conditions of this SOW and to accept the system into operations.

Final acceptance is expressly conditioned upon completion of all deliverables, completion of all tasks in the project plan as approved, completion of all applicable inspection and/or testing procedures, delivery of services, and the certification by the State that the Contractor has met the defined requirements. Final acceptance of any component or enhancement will be formally executed in writing by the State of Michigan and the Contractor after all issues identified during User Acceptance Testing have been resolved, tested, and accepted.

Failure to provide late or improper deliverable/milestone by the identified date within the Final Project Management Plan may be subject to liquidated damages. Therefore, late or improper deliverable/milestone, the State is entitled to collect liquidated damages in the amount of $50,000.00 and an additional $1,600.00 per day for each day Contractor fails to remedy the late or improper completion of the Work, up to a maximum of thirty (30 days).

(h) 1.600 Compensation and Payment

1.601 Compensation And Payment

Method of Payment
See Pricing (Schedule D) attached for details. The Costs Table(s) attached are to be used as the format for submitting pricing information.

The project will be paid based on successful completion of milestones.

Service Credits may be exchanged for training conferences, services, equipment, or deducted from State's payment due to Contractor.

Invoicing
Contractor will submit properly itemized invoices to

DTMB – Financial Services
Accounts Payable
P.O. Box 30026
Lansing, MI 48909
or
DTMB-Accounts-Payable@michigan.gov

. Invoices must provide and itemize, as applicable:

- Contract number;
- Purchase Order number
- Contractor name, address, phone number, and Federal Tax Identification Number;
- Description of any commodities/hardware, including quantity ordered;
- Date(s) of delivery and/or date(s) of installation and set up;

- Price for each item, or Contractor’s list price for each item and applicable discounts;
- Maintenance charges;
- Net invoice price for each item;
- Shipping costs;
- Other applicable charges;
- Total invoice price; and
- Payment terms, including any available prompt payment discount.

The State may pay operation and support charges on a monthly basis. Payment of maintenance service/support of less than one (1) month’s duration shall be prorated at 1/30th of the basic monthly operation and support charges for each calendar day.

Incorrect or incomplete invoices will be returned to Contractor for correction and reissue.

SCHEDULE A, ATTACHMENT 1 – REQUIREMENTS

All requirements listed in the table below will be provided without customization with the exception of.

Req. No.	Requirement
Ten-print Input	
Ten-Print Input 1	For paper forms (cards) submitted, the ABIS ***shall*** provide the user with the capability to scan the image portions of fingerprint and palm print cards at 500 or 1,000 (configurable) pixels per inch (ppi) using FBI-certified Appendix F scanner systems and assign a unique transaction control number (TCN), pursuant to the EBTS.
Ten-Print Input 2	For paper forms (cards) submitted, the ABIS ***shall*** support the scanning of the entire front and back of the cards at 500 (configurable) ppi as Type 20 records and link the image(s) with the friction ridge image entry in accordance with ID Input 1.
Ten-Print Input 3	For paper forms (cards) submitted, the ABIS ***shall*** provide the user with the capability of entering card field text, pursuant to the EBTS, and linking the text fields (Types 1 and 2) with the appropriate scanned images in accordance with ID Input 1 and 2.
Ten-Print Input 4	For paper forms (cards) submitted, after scanning and text entry are complete [ID Input 1 through ID Input 3], the ABIS ***shall*** automatically create a complete EBTS transaction with the record types 1, 2, 14, and 15, as appropriate, using an appropriate type of transaction (TOT) from the MSP AFIS Transactions Supported table.
Ten-Print Input 5	The ABIS ***shall*** be able to ingest EBTS transactions as listed in the MSP AFIS Transactions Supported table and parse them for compliance with the EBTS to include checking for duplicate TCNs.
Ten-Print Input 6	The ABIS ***shall*** be able to perform quality check (QC) (i.e., fingerprint quality via NIST Fingerprint Image Quality [NFIQ], sequence, and presence of spurious fingers) the friction ridge images of ingested and created EBTS transactions against adjustable quality thresholds (NFIQ threshold and non-recoverable sequence errors).

Req. No.	Requirement
Ten-Print Input 7	The ABIS ***shall*** forward the transactions that fail the automated QCs [Ten-print Input 6] to appropriate examiner work queues for examiner-assisted QCs.
Ten-Print Input 8	The ABIS ***shall*** permit examiners to selectively pick a transaction from the QC queue and present the selected transaction's images within 4 seconds of the selection. Further, the ABIS ***shall*** permit the examiner to select a feature whereby the system automatically provides the examiner the next job to be edited.
Ten-Print Input 9	The ABIS ***shall*** provide support to examiners in performing QC activities (adjust sequence, correct or establish the pattern, center images, to include rejecting a transaction) and in responding to the live scan station when finished.
Ten-Print Input 10	The ABIS ***shall*** allow the ten-print examiner to swap type-4 images, roll for roll, slap for slap, thumb slap for roll, and roll for thumb slap. Then the solution will save these changes to the ABIS and archive, and then send to the FBI. Updating the NIST based on these changes to be stored and forwarded.
Ten-Print Input 11	The ABIS ***shall*** allow for cutting and pasting from four finger slap to roll and thumb slap to roll, and store to AFIS.
Ten-Print Input 12	The ABIS ***shall*** permit the examiner to select the presentation of transactions based on configurable and selectable criteria such as, but not limited to, TOT, live scan ID, etc.
Ten-Print Input 13	The ABIS ***shall*** log the NFIQ score for each rolled finger in a retrievable format to include finger number and all Type 1 field data, independent of the transaction passing or failing the automated QC [Ten-print Input 7].
Ten-Print Input 14	The ABIS ***should*** be able to respond to the noncompliant or unacceptable image quality transactions via an EBTS ten-print transaction error (ERRT), said functionality to be phased in based on end-user devices.
Ten-Print Input 15	The ABIS ***shall*** be able to forward the acceptable transactions to the local criminal records repository to solicit any name-based candidates via the MSP specifications.
Ten-Print Input 16	The ABIS ***shall*** be able to ingest EBTS responses from the criminal records repository.
Ten-Print Input 17	The ABIS ***shall*** update the original ingested transaction with information from the criminal records repository response.

Req. No.	Requirement
Ten-Print Input 18	The ABIS ***shall*** update the log entry for each transaction with the results of each EBTS ingested.
Ten-Print Input 19	The ABIS ***shall*** store in a temporary file a copy of each EBTS forwarded for processing.
Ten-Print Input 20	The ABIS ***shall*** be able to ingest EBTS transactions received from the various live scan devices and external systems (cross-jurisdictional searches).
Ten-Print Input 21	The ABIS ***shall*** parse ingested EBTS transactions from external systems, checking for compliance with the EBTS to include checking job queues and archive for duplicate TCNs.
Ten-Print Input 22	The ABIS ***shall*** be able to respond to the noncompliant transactions via an EBTS ERRT, said functionality to be phased in based on end-user devices.
Ten-Print Input 23	The ABIS ***shall*** record a copy of each ingested transaction in the ANSI/NIST Archive based on the retentions field.
Ten-Print Input 24	Ability to have a cards scanning window open while having job queue window open to see live scan transactions coming in/edit/verify.
Ten-Print Input 25	An additional column in the queue that displays the initial time the job came in the queue versus the last update date and time to see first priority transactions.
Ten-Print Input 26	Must be able to rotate boxes and change the size of boxes in automated and manual submissions, especially with palms.
Ten-print Processing	
Ten-Print Proc 1	The ABIS ***shall*** "feature extract" all friction ridge images and create appropriate internal ten-print to ten-print (TP-TP) searches of the matchers, and cascade (TP-LT), and known palm to latent (KP-LT) internal searches based on the record types (4, 14, and 15) in the transaction for all transactions.

Req. No.	Requirement
Ten-Print Proc 2	The ABIS ***shall*** automatically execute all searches created in Ten-print Input 1.
Ten-Print Proc 3	If the TP-TP matcher score for a name-based searched candidate is above a settable threshold (#1), then the ABIS ***shall*** automatically declare a match.
Ten-Print Proc 4	If the TP-TP matcher score for a technical search candidate is above a settable threshold (#2), then the ABIS ***shall*** automatically declare a match.
Ten-Print Proc 5	If the matcher score for all candidates is below a settable threshold (#3), then the ABIS ***shall*** automatically declare a no-match.
Ten-Print Proc 6	If there is no automatic decision (match or no-match) and there are candidates with scores between Thresholds #2 and #3, then the ABIS ***shall*** create and move a verification package (original images and candidate images and information) to the appropriate examiner work queues for examiner-assisted verification for a settable number of candidates (up to 200, default 10), to include any candidate in score order.
Ten-Print Proc 7	The ABIS ***shall*** permit examiners to selectively pick a transaction from the Verification queue and present the selected transaction's images for at least the search prints and the first candidates within 4 seconds of the selection.
Ten-Print Proc 8	The ABIS ***shall*** permit the examiner to select a feature whereby the system automatically provides the examiner the next job to be verified
Ten-Print Proc 9	The ABIS ***shall*** permit the examiner to select transactions to be presented based on configurable and selectable criteria such as, but not limited to, TOT, live scan ID, etc.
Ten-Print Proc 10	The ABIS ***shall*** provide support for examiners to verify candidates for searches selected from the queue and to selectively manipulate the original image and the candidate image separately or in synchrony (e.g., zoom, magnify, and rotate; and adjust contrast, brightness, and sharpness) as well as use hyperlinked fields in the candidate entries to go to the master identity cross-reference file or to a specific archived transaction.

Req. No.	Requirement
Ten-Print Proc 11	The ABIS ***shall*** permit the examiners to print any search or candidate fingerprint set with Type 1, Type 2, Type 4s, Type 10s, and type 15s data.
Ten-Print Proc 12	In the case of an automatic or manual no-hit decision for which the retention code, field 2.005, is set to Y, the ABIS ***shall*** establish a new State Identification Number (SID).
Ten-Print Proc 13	The ABIS ***shall*** be able to ingest EBTS response transactions (submission results-electronic [SRE] and ERRT) from the FBI, US VISIT and any other external systems where a search was requested.
Ten-Print Proc 14	The ABIS ***shall*** use the response information from the external systems to update the master identity files and the transaction log.
Ten-Print Proc 15	The ABIS ***shall*** establish and maintain a master identity for each subject enrolled – to include links to all successfully processed transactions' TCNs and associated SIDs.
Ten-Print Proc 16	The ABIS ***shall*** automatically log all search transaction results to include the original Type 1 fields, Type 2 fields, time received, time at end of processing, and the results.
Ten-Print Proc 17	The ABIS ***shall*** allow for secondary verify, configurable by system administrator. The configuration must include off, on, and fingerprint quality parameters. Human verifies will go to a secondary operator, whereas all system verifications go to operator verification.
Ten-Print Proc 18	The ABIS ***shall*** provide the option for a verification to be marked as unable to be determined, then send the record to a second person for verification.
Ten-Print Proc 19	The ABIS ***shall*** allow for drop-down pick list for SID and TCN delete reason, purge of active job, and edit reject. Pick lists must be modifiable by administrator and logged.
Ten-Print Proc 20	Ability to abort and rerun a transaction.
Ten-Print Proc 21	The ABIS shall provide administrative parmeters to adjust what level of edits are returned to the ten-print operators. The parameters must include, fingerprint quality, number of scars pattern calls, out of sequence, minutia count,…
Ten-Print Proc 22	The ABIS must be accurate enough with pattern calls, core and axis setting so good prints do not need to be edited, without causing negative impact on ABIS accuracy. At least 50% of the transactions should not need operator editing intervention.
Ten-print Output	

Req. No.	Requirement
Ten-Print Output 1	The ABIS ***shall*** automatically prepare and return an SRE response containing the original TCN and Incident ID for all transactions in which the subject was successfully searched – showing the results (for hit and no-hit), said functionality to be phased in based on end-user devices.
Ten-Print Output 2	The ABIS ***shall*** automatically add response transactions (SRE and ERRT) to the ANSI/NIST Archive.
Ten-Print Output 3	ABIS ***shall*** allow the printing of EBTS records to the print server from the job queue for all jobs. This must include system rejected, examiner reject, and system abort jobs.
Ten-Print Output 4	Ability to card print fingerprints and palms from AFIS job queue and archive, including Type 1, Type 2, Type 4s, and Type 15s. Allow operator to select the state or FBI, criminal or applicant must be determined by TOT by system. System shall default to state format so operator doesn't have to select each time.)
Ten-Print Output 5	System must have the ability to print the composite print card.
NFF Compliance	
NFF 1	The ABIS and vendor ***shall*** provide all functionality to support participation in the NFF.
NFF 2	The ABIS ***shall*** be able to ingest EBTS transactions from the criminal records repository and parse them for compliance with the EBTS to include checking for duplicate TCNs.
NFF 3	The ABIS ***shall*** be able to forward the acceptable transactions to the appropriate and necessary destinations.
NFF 4	The ABIS ***shall*** record in a log the results of each EBTS ingested.
NFF 5	The ABIS ***shall*** store in a temporary file a copy of each EBTS forwarded to any other destination, by destination.
NFF 6	The ABIS ***shall*** be able to ingest EBTS transactions received from the various live scan or input devices or external systems.
NFF 7	The ABIS ***shall*** record a copy of each ingested transaction in the ANSI/NIST Archive.

Req. No.	Requirement
NFF 8	The ABIS ***shall*** process the EBTS transactions [Image Upgrade In 7] and forward image upgrade transactions to the FBI system.
NFF 9	The ABIS ***shall*** be able to ingest responses from the FBI**.**
NFF 10	The ABIS ***shall*** use the response information from the FBI system to update the transaction log.
NFF 11	The ABIS ***shall*** automatically forward any internal or external system response transactions (FISR and ERRI) to the submitting criminal records repository.
NFF 12	The ABIS ***shall*** automatically add response transactions (FISR and ERRI) to the ANSI/NIST Archive.
T/LI Input	
TLI Input 1	The ABIS ***shall*** be able to ingest EBTS transactions as responses from searches made in response to ten-print identification service input.
TLI Input 2	The ABIS ***shall*** be able to ingest EBTS transactions from the FBI/NGI.
TLI Input 3	The ABIS ***shall*** record in a log the results of each EBTS ingested.
TLI Input 4	The ABIS ***shall*** store in a temporary file a copy of each EBTS forwarded to the ABIS.
TLI Input 5	The ABIS ***shall*** be able to ingest EBTS transactions received from the various latent stations.
TLI Input 6	The ABIS ***shall*** record a copy of each ingested transaction in the ANSI/NIST Archive in the EBTS-compliant form in which it was received.
TLI Input 7	The ABIS ***shall*** generate and send the resultant candidate list (both the MSP and FBI) to the originating terminal.
T/LI Processing	
TLI Proc 1	The ABIS ***shall*** add all transactions that are received from the FBI to the ANSI/NIST Archive.
TLI Proc 2	The ABIS ***shall*** forward all transactions that are received from the FBI to the appropriate latent station.
TLI Proc 3	The ABIS ***shall*** create a latent entry in the appropriate verification work queue for each transaction that is received.

Req. No.	Requirement
TLI Proc 4	The ABIS ***shall*** support examiners in selectively picking a transaction from the Verification queue.
TLI Proc 5	The ABIS ***shall*** support the examiners in the verification of candidates for searches selected from the queue by providing the associated friction ridge images (reverse-search print and original latent image) within 3 seconds of the verification transaction selection.
TLI Proc 6	The ABIS ***shall*** support the examiners in verifying candidates for searches selected from the queue and selectively manipulating the original image and the candidate image separately or in synchrony (e.g., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, mirror [horizontal or vertical], sharpen/unsharpen, mark points of similarity, apply false color encoding based on image density, and generate histograms).
TLI Proc 7	The ABIS ***shall*** permit the examiners to print (1) any search latent at 1:1 or 5:1 size for latent images with case number and image number as well as time and date printed, or (2) any candidate fingerprint/palmprint set with Type 1 and Type 2 data for ten-print and palmprint cards.
TLI Proc 8	The ABIS ***shall*** support the forensic examiner selectively declaring a match, returning the transaction to the work queue, or forwarding the transaction to another examiner for confirmation or advice.
TLI Proc 9	The ABIS ***shall*** automatically log all reverse friction ridge search transactions and the steps taken, the examiners involved, and the search results.
TLI Proc 10	The ABIS ***shall*** support the preparation of court presentations when a match is found in any TLI search.
TLI Proc 11	The ABIS ***shall*** automatically log all TLI search transactions and the examiners' results in the system log and ABIS.
T/LI Output	
TLI Output 1	The ABIS ***shall*** automatically prepare a latent report for all TLI searches.
TLI Output 2	The ABIS ***shall*** support the examiner in selecting to (1) mark the case as closed, or (2) simply save and close the latent file.
TLI Output 3	The ABIS ***shall*** maintain a searchable log of all TLI searches submitted to the ABIS by external systems and to the latent stations from the ABIS.

Req. No.	Requirement
TLI Output 4	TLI verifications **shall** be routed to the AFIS Site that registered the unsolved latent.
LI Input	
LI Input 1	The ABIS ***shall*** support the examiners in creation of a new case in the appropriate latent entry to include entering data in the case information fields as well as the following image fields per image: • Case number – lab number must be auto filled and be validated against a valid lab table. Case year must be validated as numeric. • Owning agency – pick list from originating agency (ORI) table. No free text (ORI or department name). • Date of search – automatic. • Create operator – automatic based on sign on. • Terminal search came from – automatic. • Crime code – Pick list limited to valid codes. • Memo – Free text to note case details, detectives, etc. • 10 additional free text fields.
LI Input 2	The ABIS ***shall*** support the ingesting of digital images with latent fingerprints or palm prints captured at various scales as Type 13 images into a specific case using a pull-down menu of cases associated with the examiner's agency.
LI Input 3	The ABIS ***shall*** support the scanning of latent friction ridge material into Type 13 images at 1:1 scale, 500 or 1000 ppi, 8-bit gray scale, along with a ruler for calculating/verifying scale and resolution into a specific case using a pull-down menu of cases associated with the examiner's agency.
LI Input 4	The ABIS ***shall*** support the imaging with a high resolution digital camera of latent friction ridge material as Type 13 images at 1:1 scale, 500 or 1000 ppi, 8-bit gray scale, along with a ruler for calculating/verifying scale and resolution into a specific case using a pull-down menu of cases associated with the examiner's agency.
LI Input 5	The ABIS ***shall*** support the ingesting of latent case textual information linked to a latent image as Type 2 fields from a text file or the keyboard into a specific case using a pull-down menu of cases associated with the examiner's agency.
LI Input 6	The ABIS ***shall*** support the scanning of inked fingerprints with a flatbed scanner into either a Type 4 or 13 image (selectable) from deceased persons at 500 ppi, 8-bit gray scale into a specific case using a pull-down menu of cases associated.

Req. No.	Requirement
LI Input 7	The ABIS ***shall*** support the examiner in selectively creating an LFFS package for each latent image in a case, with the appropriate Type 1, Type 2, Type 13, and Type 20 records, and store it in the ABIS as an LFFS.
LI Input 8	The ABIS ***shall*** update the latent entry logs with the results of each step in the forensic services input process.
LI Processing	
LI Proc 1	The ABIS ***shall*** automatically queue the latent transaction within the ABIS.
LI Proc 2	The ABIS ***shall*** permit a forensic examiner to select a transaction for preprocessing from the work queue.
LI Proc 3	The ABIS ***shall*** support the preprocessing of Type 13 latent images to include image processing (e.g., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, apply a Fast Fourier Transform [FFT], mirror [horizontal or vertical], sharpen/unsharpen, mark features, apply false color encoding based on image density, generate histograms, and select a region of interest) and save the results to ABIS.
LI Proc 4	The ABIS ***shall*** selectively export from the latent entry the Type 13 images for preprocessing on another system.
LI Proc 5	The ABIS ***shall*** import to the latent entry Type 13 images that were preprocessed on other systems.
LI Proc 6	The ABIS ***shall*** support examiner in selectively saving and closing the case or submitting it for extraction.
LI Proc 7	The ABIS ***shall*** support the auto-extraction of features from latent entry transactions using the Extended Feature Set (EFS) as defined in the ANSI/NIST ITL-1 2011 Standard and save the results to ABIS.
LI Proc 8	The ABIS ***shall*** support the manual review and editing of features by an examiner and save the results to ABIS.
LI Proc 9	The ABIS ***shall*** support the creation/editing of search parameters such as selective geographic location, crime type(s), or a specific subject (e.g., a suspect in the case), pattern type, hand, or finger position, to include a candidate list (length up to 250 candidates) using pull-down menus.

Req. No.	Requirement
LI Proc 10	The ABIS ***shall*** support the submittal of LI searches selectively against any combination of known fingerprints, palmprints, and unsolved latents on the ABIS for instances in which the known fingerprints include all enrolled exemplars – both rolled and plain impressions.
LI Proc 11	The ABIS ***shall*** automatically search the submitted LI searches.
LI Proc 12	The ABIS ***shall*** build candidate lists of possible matches to forward searches and queue them for forensic examiners to select for verification. Candidate Type 2 information ***shall*** include sex, race, date of birth (DOB), and complete pattern type list.
LI Proc 13	If the latent case was a remote, lights-out search, the ABIS ***shall*** automatically forward the candidate list to the submitting examiner with the images of the top candidates (a selectable number up to 255 or a default, configurable value).
LI Proc 14	The ABIS ***shall*** support examiners in selectively picking a transaction from the Verification queue.
LI Proc 15	The ABIS ***shall*** support the examiners in the verification of candidates for searches selected from the queue by providing the associated friction ridge images, features (search print and first candidate), and a list of Type 2 and record-processing history within 4 seconds of the selection.
LI Proc 16	The ABIS ***shall*** support the examiners in the verification of candidates for searches selected from the queue and allow them to selectively manipulate the original image and the candidate image separately or in synchrony (e.g., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, apply FFT, mirror [horizontal or vertical], sharpen/unsharpen, mark points of similarity, apply false color encoding based on image density, generate histograms, turn on and turn off all minutiae, and display matching minutiae).
LI Proc 17	The ABIS ***shall*** support the option for forensic examiner in selectively declaring a tentative match, returning the transaction to the queue, forwarding the transaction to another examiner for confirmation or advice, or editing and resubmitting the search to include manually editing the feature set.
LI Proc 18	The ABIS ***shall*** support the option for a second forensic examiner selectively choosing a confirmation-verification package and using the tools declaring a match, non-match, or elimination; or editing and resubmitting the search to include manually editing the feature set.

Req. No.	Requirement
LI Proc 19	The ABIS ***shall*** automatically log all forward friction ridge search transactions and the steps taken, the examiners involved, and the search results in the ABIS.
LI Proc 20	The ABIS ***shall*** support the preparation of court presentations when a match is found in any forensic friction ridge search.
LI Proc 21	The ABIS ***shall*** automatically log all LI search transactions and the examiners' results in the system log and ABIS.
LI Output	
LI Output 1	The ABIS ***shall*** automatically prepare a latent entry report for all forensic searches that lead to an identification.
LI Output 2	The ABIS ***shall*** support the examiner in selecting to (1) add new unsolved latents to the unsolved latent file with a link to the appropriate latent entry records, (2) delete the record, or (3) simply save and close the ABIS file.
LI Output 3	The ABIS ***shall*** support the selective forwarding of LFFS transactions to the FBI, first using a latent penetration query (LPNQ) transaction, if appropriate, or to other systems (e.g., cross-jurisdictional partners) using the EFS or ULW to generate a more appropriate Type 9 record.
LI Output 4	The ABIS ***shall*** support the ingesting of any response to an LPNQ transaction (a latent penetration query response [LPNR] TOT) automatically forwarding it to the appropriate latent entry case.
LI Output 5	The ABIS ***shall*** support the ingesting of any response to an LFFS transaction (search results-latent [SRL] or latent transaction error [ERRL] TOTs) automatically forwarding it to the appropriate latent entry case.
LI Output 6	The ABIS ***shall*** maintain a searchable log of all forensic transactions submitted (along with the responses) to the ABIS and to external systems in the system log and ABIS.
LI Output 7	The ABIS ***shall*** support the selective forwarding of FBI and other external responses (SRL TOTs) to latent transactions to the appropriate Verification queue.
LI Output 8	The ABIS ***shall*** automatically log all LI search transactions and the examiners' results in the system log and ABIS.

Req. No.	Requirement
Latent access to the FBI AFIS ULW Functionality	
ULW 1	The ABIS ***shall*** provide seamless ULW functionality between the ABIS and the FBI.
ULW 2	All features related to the FBI's ULW access should be included. Latent search, verification, image retrieval, latent registration, latent delete, image retrieval (latent and ten-print)
ABIS 1	The ABIS ***shall*** support latent examiners and system administrators in the creation of latent cases, independent of actually loading any images, to include entering and saving information in the following data fields: • Case number must be validated as numeric. • Case number – lab number must be auto filled and be validated against a valid lab table. • Case year must be validated as numeric. • Owning agency – pick list from originating agency (ORI) table. No free text (ORI or department name). • Date of search – automatic. • Create operator – automatic based on sign on. • Terminal search came from – automatic. • Crime code – Pick list limited to valid codes. • Memo – Free text to note case details, detectives, etc. 10 additional free text fields.
ABIS 2	The ABIS ***shall*** support system administrators in populating and updating a table of statutes of limitations on state crime codes. This will allow for batch purging of latent cases. The system should also allow for the system administrator to select by crime code and age of transactions to be deleted. This would allow for specific crime code and age batch purge or all crime codes by statute of limitations table. System must relay to administrator "are you sure…" and schedule the purge then or next business day.

Req. No.	Requirement
ABIS 3	The ABIS ***shall*** permit and support latent examiners and system administrators in selective maintenance of the latent entry files, unsolved latent file, and matcher files to include correcting incorrectly entered information, moving images between cases, merging cases, and updating the table of statutes of limitations based on state crime codes.
ABIS 4	The ABIS ***shall*** automatically track all latents submitted to external agencies for retention.
ABIS 5	The ABIS ***shall*** automatically track for reporting purposes all latents submitted by external agencies.
ABIS 6	The ABIS ***shall*** automatically identify situations in which searches against different latents from the same case have identical candidates anywhere in the top 100 positions and alert the examiner(s) assigned to the case with a message in his/her work queue. MorphoBIS sends an e-mail message to the agency when different latents from the same case have identical candidates anywhere in the top 100 positions.
ABIS 7	The ABIS ***shall*** offer latent examiners and system administrators the ability to remove latent images from the ABIS and/or an external unsolved latent file(s). With MorphoBIS, authorized users can remove latent images from the ABIS or request removal of a latent image from an external unsolved latent file(s).
ABIS 8	If latent examiners and system administrators elect to remove a latent image from any external system's unsolved latent file, the ABIS ***shall*** automatically generate the appropriate TOT.
ABIS 9	The ABIS ***shall*** automatically alert the system administrator via a message in an administrative queue when a case reaches the following windows: 90, 60, and 30 days from the expiration of the statute of limitations for any and all cases.
ABIS 10	The ABIS ***shall*** support the latent examiners and system administrators in selectively opening and dealing with administrative message in their work queue and in relaunching or closing cases for which the statute of limitations expired notice has been sent to them.
ABIS 11	The ABIS ***shall*** automatically delete unsolved cases from the latent entry when the statute of limitations expires if the Auto-Delete flag was set to "Y" in ABIS when the case was opened or at any later point.
ABIS 12	If the ABIS automatically closes a latent case that has any images in an external system's unsolved latent file, the ABIS ***shall*** automatically generate the appropriate TOT.

Req. No.	Requirement
ABIS 13	The ABIS ***shall*** send LI management transactions to the FBI's NGI system.
ABIS 14	The ABIS ***shall*** be able to ingest external system responses from the FBI (ULAR, ULDR, LSMR, and administrative transaction error [ERRA] TOTs).
ABIS 15	The ABIS ***shall*** use the response information from the FBI to update the transaction log.
ABIS 16	The ABIS ***shall*** automatically forward any external system response transactions to the appropriate latent entry file.
ABIS 17	The ABIS ***shall*** automatically log all latent management transactions and activities to include date, time, person performing the activity, activity type, status (successful or problem encountered), and any changes to the ABIS or external system matcher files of unsolved latents.
ABIS 18	The ABIS ***shall*** record a copy of each ingested transaction in the ANSI/NIST Archive in the EBTS-compliant form in which it was received.
RMID Input	
RMID Input 1	The ABIS ***shall*** be able to ingest TPIS transactions and parse them for compliance with the EBTS to include checking for duplicate TCNs.
RMID Input 2	The ABIS ***shall*** process the acceptable TPIS transactions with the priority set to 1 (the highest priority value) by an administrator which is also configurable.
RMID Input 3	The ABIS ***shall*** record in a log the results of each TPIS transaction ingested.
RMID Input 4	The ABIS ***shall*** store in a temporary file a copy of each TPIS forwarded for processing.
RMID Input 5	The ABIS ***shall*** be able to ingest TPIS transactions received.
RMID Input 6	The ABIS ***shall*** record a copy of each ingested TPIS transaction in the ANSI/NIST Archive in the fully EBTS-compliant form in which it was received.
RMID Input 7	RMID jobs must appear in the ten-print job queue so operators can see them, allowing for manual search and verify if requested.
RMID Input 8	System shall accept any number of fingers.
RMID Processing	

Req. No.	Requirement
RMID Proc 1	The ABIS ***shall*** feature extract the fingerprint images and create an appropriate internal search of the matchers (TP-TP).
RMID Proc 2	The ABIS ***shall*** automatically prepare and return an ERRT response containing the original TCN and Incident ID for all transactions that were not process able, phased in over time.
RMID Proc 3	The ABIS ***shall*** automatically execute all TP-TP searches using the features extracted.
RMID Proc 4	The ABIS ***shall*** forward transactions to the FBI's NGI if a search was requested.
RMID Proc 5	The ABIS ***shall*** ingest the FBI responses (SRT, ten-print rap sheet response [TPRR], and ERRT).
RMID Proc 6	The ABIS ***shall*** automatically log all TPIS search transaction results (local and FBI) to include the Type 1 fields, time received, time logged at end of processing, and the results.
RMID Proc 7	The system shall be able to use any combinations of fingers.
RMID Proc 8	System shall accept NIST fields to determine if transaction should be sent to the FBI RISC.
RMID Output	
RMID Output 1	If there are any candidates available, then the ABIS ***shall*** automatically return a response TOT with the five highest (configurable) scoring candidates and associated mug shots, if available.
RMID Output 2	If there are no candidates available, then the ABIS ***shall*** automatically return a response TOT with that information.
RMID Output 3	The ABIS ***shall*** automatically forward FBI responses (SRT, TPRR, and ERRT) to the originating device.
RMID Output 4	The ABIS ***shall*** automatically add response transactions (SRT, TPRR, and ERRT) to the ANSI/NIST Archive.
General System Functionality	
GEN 1	The ABIS ***shall*** support transaction logging that starts as soon as the system receives the transaction, including live scan, hard card, and mobile ID transactions.

Req. No.	Requirement
GEN 2	The ABIS ***shall*** support a suppression flag. Administrative staff and specific users, definable in the User Authentication File (UAF) can set the flag base on SID or TCN as being suppressed. A record in this state cannot return information for mobile ID. Retainable live scan searches would use this SID; non-retainable searches would not find this SID. The ABIS would be able to provide these types of SIDs as candidates to latent searches.
GEN 3	The ABIS ***shall*** provide a logical delete on the minutia and archive databases by SID and TCN. Records can be set to this status by UAF authorized staff and batch processing. A record in this state cannot return information for mobile ID. Retainable live scan searches would use this SID; non-retainable searches would not find this SID. The ABIS would be able to provide these types of SIDs as candidates to latent searches.
GEN 4	The ABIS ***shall*** provide a utility to physically delete TCNs and SIDs that have been in the logical delete status for a configurable number of days, configurable by the MSP.
GEN 5	The ABIS ***shall*** provide a utility to allow MSP users with authority in the UAF to send a transaction from Archive to the FBI and allow changes to TOT and other data before sending.
GEN 6	The ABIS ***shall*** provide a utility to allow MSP users with authority in the UAF to send or resend a transaction from the job queue to the FBI and allow changes to TOT and other data before sending.
GEN 7	The ABIS ***shall*** provide a utility to pull TCNs from Archive and resubmit as a live scan job. The system must allow the same TCN to be used or initiate with new unique TCN, and allow changes to TOT and data before sending. Also the system must set flags to not return messages to field.
GEN 8	The ABIS Archive ***shall*** store EBTS files as received and a version as modified. After EBTS files are received and sent to the Criminal History System (CHS), some fields are modified and created by CHS. The Archive must also allow displaying and printing of the original EBTS and the modified version.
GEN 9	The ABIS ***shall*** have one utility with formatted screens to define ABIS terminals, live scan devices, live scan groups (agency that has more than one device), live scan region, mobile ID device, system administrators, site supervisors, latent examiners, ten-print examiners, and the access levels and functions allowed for the device, site, and user.

Req. No.	Requirement
GEN 10	The vendor ***shall*** meet with the MSP to determine what fields are required for each database and screen.
GEN 11	The ABIS ***shall*** allow each user to define the arrangement of fields, columns, and buttons and save the arrangement by user. This would allow the user to see the screens as they arranged them the last time they signed on.
GEN 12	In the case of batch Sync AFIS and Archive with CCH, the ABIS ***shall*** create SID and TCN files to be compared to CCH to determine whether SID and/or TCN need to be deleted from AFIS and/or Archive.
GEN 13	The ABIS ***shall*** allow for batch delete from AFIS and archive to include real delete and logical delete.
GEN 14	The ABIS ***shall*** allow for TCN and SID batch suppression.
GEN 15	The ABIS ***shall*** allow for batch latent delete.
GEN 16	The ABIS ***shall*** provide that in the case of logical deletes and suppressed records they cannot be returned to RMID searches.
Gen 17	The ABIS shall provide event status for each step/phase of a ten-print, latent, and Mobile ID transaction on the job queue and event log. Each status must be adjustable to terms easily understood by staff. Examples are Search Exec, Name Search, Send FBI, and Done.
ABIS Storage Capacity Requirements	
Stor Req 1	For the base contract, the ABIS ***shall*** have the capacity to store in the ANSI/NIST Archive at the beginning of any year, at least the number of EBTS transactions listed per year in the Transaction Counts and Throughput table for that year.
Stor Req 2	For the base contract, the ABIS ***shall*** have the annual capacity to store in the matchers the templates for enrolled fingerprints.
Stor Req 3	For the base contract, the ABIS ***shall*** have the annual capacity at the beginning of the year to store in the matchers the templates for enrolled unsolved fingerprints and palm prints at the levels shown in the Transaction Counts and Throughput table.

Req. No.	Requirement
Stor Req 4	For the base contract, the ABIS ***shall*** have the capacity to store a backup copy on portable digital media of all ANSI/NIST transactions that are in the ANSI/NIST Archive and the biometric feature sets (also known as templates) in the matchers, in any given year, as a backup for the Archive and matchers.
Stor Req 5	The ABIS ***shall*** have the capacity and ability to create and store ABIS level logs for all activities listed in the Functional Requirements for a period commensurate with the FBI CJIS Security Policy, version 5.3, plus 3 additional years.
Throughput Requirements	
ThruPut Req 1	The ABIS ***shall*** be able to ingest, process, and respond in the **peak** period to at least the daily average of transaction counts noted in the Transaction Counts and Throughput table while maintaining the response times noted in the Response Times Per Transaction Type table while latent and mobile ID transactions are being ingested, processed, and responded to. [This requirement is independent of any time for examiners to perform QC on the input stream or to review candidate lists/perform verification.]
ThruPut Req 2	The ABIS ***shall*** be able to ingest, process, and respond in the **peak** period to at least the daily average of transaction counts noted in the Transaction Counts and Throughput table while maintaining the response times noted in the Response Times Per Transaction Type table, while identification and rapid/mobile ID transactions are being ingested, processed, and responded to. [This requirement is independent of any time for examiners to perform QC on the input stream or to review candidate lists/perform verification.]

Req. No.	Requirement
ThruPut Req 3	The ABIS ***shall*** be able to ingest, process, and respond in the **peak** period to at least the daily average of transaction counts noted in the Transaction Counts and Throughput table while maintaining the response times noted in the Response Times Per Transaction Type table, while identification and latent transactions are being ingested, processed, and responded to. The proposed system is sized to meet or improve upon the required performance matrix, including both peak throughput and response time, as identified in the referenced the Statement of Work. Sizing the system for five or six years out helps ensure improved performance. Contractor understands that "peak period" is "The hour of time on any given day in which the greatest number of transactions are received by AFIS for processing."
ThruPut Req 4	If in any day the ABIS is presented with more transactions in a **peak** hour than the design capacity, then the ABIS ***shall*** queue the additional work and process it as soon as capacity is available, with that processing to be based on the priority of the transactions.
Response Time Requirements	
Response Req 1	The ABIS ***shall*** provide responses for 95% of submitted transactions in accordance with the response times noted in the Response Times Per Transaction Type table. Response time is to be measured from the end of ingest through the final response, to the return of a response from the ABIS to the submitting device with no error TOTs in the mix.
Response Req 2	The ABIS ***shall*** use transaction priority in assigning transactions to queues and in processing them when higher than peak transaction rates are encountered – processing higher-priority transactions ahead of lower-priority transactions in the same Transaction Class Type.
Accuracy Requirements	
Accuracy Req 1	The ABIS ***shall*** provide accuracy for submitted transactions in accordance with the values in the Accuracy Rates by Transaction Type table while conforming to the response times noted in the Response Times Per Transaction Type table. The accuracy will be measured using vendor best practices.

Req. No.	Requirement
Safety Requirements	
Safety Req 1	All hardware configuration items delivered as part of the ABIS ***shall*** conform to the appropriate U.S. Underwriters Laboratory standards for electronic devices and be so certified.
Safety Req 2	All required grounding ***shall*** conform to the manufacturer's specifications and recommendations.
Information Security Requirements	
InfoSec Req 1	The ABIS design ***shall*** conform to the CJIS Security Policy v5.0 or later.
InfoSec Req 2	Antivirus software ***shall*** be loaded on all processors that run operating systems for which commercial antivirus packages are available.
InfoSec Req 3	The antivirus software ***shall*** automatically virus scan all files on portable data storage devices (i.e., CDs, DVDs, USB devices with memory, and floppy disk media) presented to a system and report alerts and other problems, including performing auto-updates of the anti-virus software.
InfoSec Req 4	The antivirus software ***shall*** automatically log all virus alerts and action taken.
InfoSec Req 5	The ABIS ***shall*** support the updating of antivirus software databases of virus information without compromising the security of the system.
InfoSec Req 6	The ABIS ***shall*** support encryption of data at rest on any hard drive or other storage device used in the ABIS environment, as well as any data in-flight in the system.
InfoSec Req 7	The ABIS ***shall*** provide for robust and configurable system user management and authentication (including the use of user roles, groups, etc.), which should also be capable of operating in conjunction with current agency user management products.
Environmental Requirements	
Envrn Req 1	Each workstation ***shall*** have a UPS that can support the workstation for up to 20 continuous minutes in the event of a loss of building power.

Req. No.	Requirement
Envrn Req 2	Each workstation UPS ***shall*** provide the user with a signal for cases in which the UPS has been the only source of power to the device for 10 continuous minutes.
Envrn Req 3	The verification stations ***shall*** be able to operate in an office environment, without any requirement for supplemental air conditioning or noise suppression: • 68° to 72° temperature with a relative humidity between 40% and 60%. • Noise below 70 dBA measured at the workstation suite.
Hardware Requirements for Workstations and Printers	
Hdwe Req 1	Each ten-print workstation ***shall*** have: • A microprocessor with at least 3.4 GHz clock speed and at least four cores. • Built-in graphics or a graphics board with at least 1 - 2 GB of onboard memory. • 12 GB of internal RAM. • Two 24-inch to 27-inch monitors with at least 1920×1200 resolution and digital visual interface. • 1 Gb network interface card. • At least one 500 GB or greater hard disk drive. • Hard disk or solid state drive. • Keyboard and mouse. • FBI EBTS Appendix F-certified flatbed scanner. • The most recent version of the operating system that was used to certify the scanner. • A full suite of the vendor ten-print software and the ability to use the vendor latent software. • One black and white printer for each ten-print workstation. • One network color printer per ten-print site.

Req. No.	Requirement
Hdwe Req 2	Each latent workstation ***shall*** have: • A microprocessor with at least 3.4 GHz clock speed and at least four cores. • Built-in graphics or a graphics board with at least 12 GB of onboard memory. • 12 GB of internal RAM. • Two 24-inch or larger flat panel displays with at least 1920×1200 resolution and digital visual interface. • 1 Gb network interface card. • At least one 500 GB or greater hard disk drive. • Keyboard and mouse. • FBI EBTS Appendix F-certified flatbed scanner. • The most recent version of the operating system that was used to certify the scanner. • Adobe Photoshop Elements™ Version 9 or later. • A full suite of the vendor latent software and the ability to use the vendor ten-print software. • One set of camera equipment. • One color printer for each site.
Hdwe Req 3	Each card printer ***shall*** have: • At least two drawers/trays to support fingerprint and palmprint card stock simultaneously without having to physically change trays. • FBI Appendix F certification. • Connectivity to a workstation or server running the most recent version of the operating system that was used to certify the printer. • Simultaneous two-sided print capability. • 1 Gb network interface card. • At least 256 MB of memory.
Hdwe Req 4	The ABIS ***shall*** allow for remote/Web site administration from current MSP terminals.
ABIS Availability Requirement	

Req. No.	Requirement
SAR Req 1	During the life of this contract, to include any optional extensions, the ABIS ***shall*** provide at least 99.8% availability of all ABIS services unless a catastrophic event occurs – measured monthly, to include as unavailable time (1) any scheduled outages for preventive maintenance and (2) planned upgrades during which ABIS users do not have access to and the use of ABIS services. For purposes of this requirement "catastrophic event" is defined as a natural or man-made disaster that destroys both the primary and the disaster recovery ABIS sites or renders both unusable due to fire, water damage, earthquake, radioactive leak, large-scale power outage, declared medical pandemic, or a large-scale communications infrastructure outage (telephones and Internet access). Large-scale means at least impacting the city where the site is located. Contractor understands MSP requirements for Business Continuity and Disaster Recovery. The Disaster Recovery configuration consists of two distinct systems (Primary and DR) working together to ensure operational continuity over a wide range of circumstances. The systems support the 99.8% uptime requirement. The proposed configuration provides high-availability across multiple levels: site, transactional, workflow, matcher subsystem, database, and site level. At the site level, a Quorum server is employed to monitor the status of each site. The Quorum server is the arbitrator for site processing and can institute a failover should either site experience a failure or network connectivity loss. The failover from dual to single site processing is executed without impacting the operation of the system. At the transactional level, the DES functions as a transaction manager for components within this complex closed system. MorphoBIS supports multiple DES for high scalability in a load-balanced architecture as well as supporting operational network connectivity loss. At the workflow level, Contractor will use JBOSS clustering across the two Workflow Application Services (WAS) units on each system (Primary and COOP). This allows the system to treat the separate units as a logically single unit; if one system goes down the system will continue to function as usual. The matchers dynamically reconfigure the matching threads if hardware issues are incurred. In addition to utilizing the resource pool, the matchers themselves are designed in a multi-threaded architecture.
Interface Requirements	

Req. No.	Requirement
Interface Req 1	The ABIS shall provide, test, and implement each and all of the interfaces listed in the Interface Requirements table during implementation of the new system environment.
Test Transaction Input Requirements	
Test Input	
Test Input 1	The ABIS provider ***shall*** provide a test ABIS environment, including an archive for the purposes of testing.
Test Input 2	The ABIS ***shall*** be able to ingest test EBTS transactions from the criminal record repository and parse them for compliance with the ABIS EBTS, to include checking for duplicate TCNs.
Test Input 3	The ABIS ***shall*** be able to respond to the noncompliant test transactions via an EBTS ERRT to the criminal record repository or other submitter.
Test Input 4	The ABIS ***shall*** be able to forward the acceptable test transactions to the originator.
Test Input 5	The ABIS ***shall*** record in a log the results of each test EBTS ingested.
Test Processing	
Test Proc 1	The ABIS ***shall*** ingest the test EBTS transactions received from the devices and process them.
Test Proc 2	The ABIS ***shall*** update the transaction log with the processing results.
Test Output	
Test Output 1	The ABIS ***shall*** automatically generate and forward the appropriate system response transaction to the submitting criminal record repository.
Test Output 2	If the test transaction is marked to be forwarded to the FBI, the ABIS ***shall*** automatically forward it as designated during the system design.
Test Output 3	The ABIS ***shall*** ingest all responses received from the FBI and forward them to the appropriate device.
Test Output 4	The ABIS ***shall*** update the transaction log with the processing results.

Req. No.	Requirement
<u>System Administrator Requirements</u>	
Admin Function 1	The ABIS ***shall*** permit the system administrators to selectively set up and manage at least 10 classes of users (e.g., latent supervisor) with configurable permissions per class.
Admin Function 2	The ABIS ***shall*** support the system administrator in assigning workflows and, within workflows specific TOTs, to default priority queues – with up to nine priorities to conform to the ANSI/NIST Standard for Field 1.006: *"The values shall range from "1" to "9", with "1" denoting the highest priority. The default value shall be defined by the agency receiving the transaction."*
Admin Function 3	The ABIS ***shall*** support the system administrator in maintaining and changing Thresholds 1, 2, 3, and 4 as appropriate.
Admin Function 4	The ABIS ***shall*** support the system administrator in maintaining and changing QC thresholds for ten-prints and separately for palmprints.
Admin Function 5	The ABIS ***shall*** support the system administrator in maintaining and changing default candidate lengths for verification, separately for ten-prints, LIs, and TLIs.
Admin Function 6	The ABIS ***shall*** support the system administrator in maintaining and changing a selectable second-level verification in accordance with International Standards Organization (ISO) standards.
Admin Function 7	The ABIS ***shall*** support the system administrator in selectively reviewing and printing the ABIS logs – reviewing and printing must be organized by any or all of the following selectable options: time, date, user, transaction type, file-accessed name, device logged into, problem reports, TCN, and transaction results.
Admin Function 8	The ABIS ***shall*** enable the system administrator to selectively back up IT, biographic, ANSI/NIST Archive, and forensic files at all system levels from workstations to the ABIS.
Admin Function 9	The ABIS ***shall*** support the system administrator in selectively restoring IT, biographic, ANSI/NIST Archive, and forensic files.
Admin Function 10	The ABIS ***shall*** allow the system administrator to selectively ingest any supported transactions, individually or in bulk, and process them as appropriate to the TOT.

Req. No.	Requirement
Admin Function 11	The ABIS ***shall*** permit the system administrator to selectively cancel programs that are not responding and restart any program or computer.
Admin Function 12	The ABIS ***shall*** support the forensic system administrator in selectively exporting "known" files in bulk or individually.
Admin Function 13	The ABIS ***shall*** support the system administrator in selectively exporting "unknown" (latent) files in bulk or individually.
Admin Function 14	The ABIS ***shall*** support the systems administrator in preparing selective reports for, at a minimum, selectable time periods and classes of services and on use patterns of the ABIS and aggregating those reports so they can be edited, merged with other reports, and printed.
Admin Function 15	The ABIS ***shall*** support automated logging and system administrator selective reporting on the following information: • Use by time, person, functionality, etc. • Viruses encountered – at the device level. • All events associated with unsuccessful login attempts, at the device level.
Admin Function 16	The ABIS ***shall*** support automated logging and system administrator selective reporting on the following information: • Disk memory used, free, and as-built totals by system and component: o ANSI/NIST Archive. o Temporary files. o The ABIS. • Matcher memory used, free, and totals by system, by component, and by modality (e.g., reverse palm search matchers).
Admin Function 17	The ABIS ***shall*** support automated logging and system administrator selective reporting on the following information: • A record of abnormal shutdown of any computer, along with any available diagnostics. • Number and percentage of transactions by class that failed/passed parser and image QCs.

Req. No.	Requirement
Admin Function 18	The ABIS ***shall*** support automated logging and system administrator selective reporting on the following information: • NFIQ scores by finger, TOT, ORI, and/or time. • Number of transactions. • Searches by class. • Hit rate by class. • Hit rate by TOT. • Error rate in processing transactions. • Current size of each repository to include available space, selectively for one or more system elements, or the entire ABIS.
Admin Function 19	The ABIS ***shall*** provide for a central monitoring system that monitors all functions of ABIS and provides warnings and alerts using visual and audio features and e-mails.
Admin Function 20	The ABIS ***shall*** provide for fingerprint-enabled sign-on for users.
Admin Function 21	The ABIS ***shall*** support the selective production of reports from all workflows and administrative functions to a specified color or gray-scale printer, to a file using comma-separated format for future use to include editing and merging with other such files and saving reports as an Adobe Portable Data Format (PDF) file. The ABIS ***shall*** minimally provide a baseline set of management reports.
Admin Function 22	The ABIS ***shall*** offer ABIS management the ability to easily track, monitor, and produce reports on the types of ten-print, latent, and administrative activities.
Admin Function 23	The ABIS ***shall*** permit administrators to design their own report formats from pull-down menus.
Admin Function 24	The ABIS ***shall*** permit administrators to synchronize system time across all ABIS elements that have or use time clocks (e.g., servers, workstations, and logs).
Admin Function 25	The ABIS ***shall*** permit administrators to select auto-synchronization of system time across all ABIS elements that have or use time clocks (e.g., servers, workstations, and logs) on a selectable frequency (between 6 hours and 24 hours).
Admin Function 26	All tables created for edits or used selection for the operator, such as crme codes, race, sex, ORI, lab code live scan ID, mobile identification ID, must be easily updated by the MSP administrator functions.

SCHEDULE B – SERVICE LEVEL AGREEMENT

1. **Definitions.** For purposes of this Exhibit, the following terms have the meanings set forth below. All initial capitalized terms in this Exhibit that are not defined in this **Section 1** shall have the respective meanings given to them in the Contract

"**Actual Uptime**" means the total minutes in the Service Period that the Hosted Services are Available.

"**Authorized Users**" means all Persons authorized by the State to access and use the Services through the State's account under the Contract, subject to the maximum number of users specified in the Contract.

"**Availability**" has the meaning set forth in **Section 4(a)**.

"**Availability Requirement**" has the meaning set forth in **Section 4(a)**.

"**Available**" has the meaning set forth in **Section 4(a)**.

"**Business Day**" means a day other than a Saturday, Sunday or State Holiday.

"Contractor Security Officer" has the meaning set forth in **Section 3.1**.

"**Contractor Service Manager**" has the meaning set forth in **Section 3.1**.

"**Contractor Systems**" has the meaning set forth in **Section 6.3**.

"**Corrective Action Plan**" has the meaning set forth in **Section 5.6**.

"**Critical Service Error**" has the meaning set forth in **Section 5.4(a)**.

"**DR Plan**" has the meaning set forth in **Section 7.3(a)**.

"**Exceptions**" has the meaning set forth in **Section 4.2**.

"**Force Majeure Event**" has the meaning set forth in **Section 8.1**.

"**High Service Error**" has the meaning set forth in **Section 5.4(a)**.

“**Hosted Services**” has the meaning set forth in **Section 2.1(a)**.

“**Minor Service Error**” has the meaning set forth in **Section 5.4(a)**.

“**Resolve**” has the meaning set forth in **Section 5.4(b)**.

“**Scheduled Downtime**” has the meaning set forth in **Section 4.3**.

“**Scheduled Uptime**” means the total minutes in the Service Period.

“**Service Availability Credits**” has the meaning set forth in **Section 4.5(a)**.

“**Service Error**” means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Exhibit.

“**Service Level Credits**” has the meaning set forth in **Section 5.5**.

“**Service Level Failure**” means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

“**Service Period**” has the meaning set forth in **Section 4(a)**.

“**Service Software**” means any and all software applications and any third-party or other software, and all new versions, updates, revisions, improvements and modifications of the foregoing, that Contractor provides remote access to and use of as part of the Services.

“**Service Support Level Requirements**” has the meaning set forth in **Section 5.4**.

“**Services**” has the meaning set forth in **Section 2.1**.

“**Software Support Services**” has the meaning set forth in **Section 5**.

“**State**” means the State of Michigan.

“**State Service Manager**” has the meaning set forth in **Section 3.2**.

"**State Systems**" means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

"**Support Request**" has the meaning set forth in **Section 5.4(a)**.

"**Support Service Level Requirements**" has the meaning set forth in **Section 5.4**.

"**Term**" has the meaning set forth in the Contract.

"**Workstations**" has the meaning set forth in the Statement of Work.

2. **Services.**

2.1 Services. Throughout the Term, Contractor will, in accordance with all terms and conditions set forth in the Contract and this Exhibit, provide to the State and its Authorized Users the following services ("**Services**"):

(a) the hosting, management and operation of the Service Software in the Microsoft Azure Government cloud, support and maintenance of the on premise Workstations, and other services for remote electronic access and use by the State and its Authorized Users ("**Hosted Services**");

(b) the Software Support Services set forth in **Section 5** of this Exhibit;

(c) the necessary security set forth in **Section 6** of this Exhibit; and

(d) the disaster recovery and backup services set forth in **Section 7** of this Exhibit.

3. **Personnel**

3.1 Contractor Personnel for the Hosted Services. Contractor will appoint: (i) a Contractor employee to serve as a primary contact with respect to the Services who will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support Requests and the Software Support Services (the "**Contractor Service Manager**"); and (ii) a Contractor employee to respond to the State's inquiries regarding the security of the Contractor Systems who has sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto ("**Contractor Security Officer**").

3.2 State Service Manager for the Hosted Services. The State will appoint and, in its reasonable discretion, replace, a State employee to serve as the primary contact with respect to the Services who will have the authority to act on behalf of the State in matters pertaining to the Software Support Services, including the submission and processing of Support Requests (the "**State Service Manager**").

4. **Service Availability and Service Availability Credits.**

(a) Availability Requirement. Contractor will make the Hosted Services Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a "**Service Period**"), at least 99.8% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the "**Availability Requirement**"). "**Available**" means the Hosted Services are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Contract. "**Availability**" has a correlative meaning. The Hosted Services are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services, in whole or in part. The Availability Requirement will be calculated for the Service Period as follows: (Actual Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services are not Available Due to an Exception) x 100 = Availability.

4.2 Exceptions. No period of Hosted Service degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following ("**Exceptions**"):

(a) failures of the State's or its Authorized Users' internet connectivity;

(b) Scheduled Downtime as set forth in **Section 4.3**.

(c) Due to an event not the fault of the Contractor or otherwise beyond the control of the Contractor, other than acts of Microsoft Azure.

4.3 Scheduled Downtime. Contractor must notify the State at least twenty-four (24) hours in advance of all scheduled outages of the Hosted Services in whole or in part ("**Scheduled Downtime**"). All such scheduled outages must: (a) last no longer than ninety (90) minutes per month; (b) be scheduled for a date and time to be determined by the Program Manager; provided that Contractor may request the

State to approve extensions of Scheduled Downtime above ninety (90) minutes, and such approval by the State may not be unreasonably withheld or delayed.

4.4 Service Availability Reports. Within thirty (30) days after the end of each Service Period, Contractor will provide to the State a report describing the Availability and other performance of the Hosted Services during that calendar month as compared to the Availability Requirement. The report must be in electronic or such other form as the State may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform the State of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement are fully met.

4.5 Remedies for Service Availability Failures.

(a) If the actual Availability of the Hosted Services is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to the State the following credits on the fees payable for Hosted Services provided during the Service Period ("**Service Availability Credits**"):

Availability	**Credit of Fees**
≥99.8%	None
<99.8% but ≥99.5%	15%
<99.5% but ≥98.0%	35%
<98.0%	50%

(b) Any Service Availability Credits due under this **Section 4.5** will be applied in accordance with payment terms of the Contract.

(c) If the actual Availability of the Hosted Services is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to the State, the State may terminate the Contract on thirty (30) days written notice to Contractor and failure to cure with no liability, obligation or penalty to the State by reason of such termination.

5. **Support and Maintenance Services**. Contractor will provide Hosted Service maintenance and support services (collectively, "**Software Support Services**") in accordance with the provisions of this

Section 5. The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

5.1 Support Service Responsibilities. Contractor will:

(a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;

(b) provide unlimited telephone and online support 24 hours a day, 7 days a week, including State holidays for the ABIS software and hardware and ten-print site equipment; 8:00 am to 5:00 pm EST Monday – Friday for remote latent sites;

(c) provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and

(d) respond to and Resolve Support Requests as specified in this **Section 5**.

5.2 Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

(a) proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service security;

(b) if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

(c) if Contractor receives knowledge that the Hosted Service or any Hosted Service function or component is not Available (including by written notice from the State pursuant to the procedures set forth herein):

(i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;

(ii) if Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 5.4**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) notifying the State that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

5.3 Service Maintenance. Contractor will continuously maintain the Hosted Services to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to the State and its Authorized Users:

(a) all updates, bug fixes, enhancements, new releases, new versions and other improvements to the Hosted Services, including the Service Software, that Contractor provides at no additional charge to its other similarly situated customers; and

(b) all such services and repairs as are required to maintain the Hosted Services or are ancillary, necessary or otherwise related to the State's or its Authorized Users' access to or use of the Hosted Services, so that the Hosted Services operate properly in accordance with the Contract and this Exhibit.

5.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 5.4** ("**Support Service Level Requirements**"), and the Contract.

(a) Support Requests. The State will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a "**Support Request**"). The State Service Manager will notify Contractor of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	**Description:**

	Any Service Error Comprising or Causing any of the Following Events or Effects
Critical Service Error	• Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by the State; or • Widespread access interruptions. • system or component failures that prevent subjects from being enrolled, images from being searched, or responses from being delivered. (This includes all central site and ten-print site equipment supplied by Contractor associated with the system, including other required peripherals that prevent users from accomplishing their work.)
High Service Error	• Primary component failure that materially impairs its performance; or

	• Data entry or access is materially impaired on a limited basis.
Minor Service Error	• Hosted Service is operating with minor issues that can be addressed with a work around. • Request for assistance, information, or services that are routine in nature.

(b) Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. "**Resolve**" (including "**Resolved**", "**Resolution**" and correlative capitalized terms) means that, as to any Service Error, Contractor has provided the State the corresponding Service Error correction and the State has confirmed such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error:

Support Request Classification	**Service Level Metric** **(Required Response Time)**	**Service Level Metric** **(Required Resolution Time)**	**Service Level Credits** **(For Failure to Respond to any Support Request Within the Corresponding Response Time)**	**Service Level Credits** **(For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)**

Critical Service Error	Thirty (30) minutes	Two (2) hours	Ten percent (10%) of the Fees for the month in which the initial Service Level Failure begins and ten percent (10%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Ten percent (10%) of the Fees for the month in which the initial Service Level Failure begins and ten percent (10%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
High Service Error	One (1) hour	Four (4) hours	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for the first additional hour or portion

			corresponding Service Error is not responded to within the required response time.	thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
Minor Service Error	Three (3) hours	Eight (8) hours	N/A	Four percent (4%) of the Fees for the month in which the initial Service Level Failure begins and four percent 4%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment

(c) Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Service Manager and Contractor's management or engineering personnel, as appropriate.

5.5 Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements for Critical Service Errors will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 5.4(b)** ("**Service Level Credits**") in accordance with payment terms set forth in the Contract. The maximum amount of service level credit for any one month shall not exceed fifty percent (50%) of any monthly fee.

5.6 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

6. **Security**.

6.1 Protection of the State's Confidential Information. Throughout the Term and at all times in connection with its actual or required performance of the Services hereunder, Contractor will:

(a) maintain an annual SSAE 16 SOC 2 Type 2 audit of the hosted facilities, IT infrastructure security controls, and processes;

(b) ensure that the Service Software is securely hosted, supported, administered, and accessed in a data center that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com);

(c) maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State's Confidential Information that comply with the requirements of the State's data security policies as set forth in the Contract, and, to the extent such practices and standards are consistent with and not less protective than the foregoing requirements, are at least equal to applicable best industry practices and standards as recommended by the National Institute of Standards and Technology (NIST);

(d) provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of the State's Confidential Information and the nature of such Confidential Information, consistent with best industry practice and standards.

(e) take all reasonable measures to:

(i) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Systems or the information found therein;

(ii) prevent (A) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (B) the State's Confidential Information from being commingled with or contaminated by the data of other customers or their users of the Services; and (C) unauthorized access to any of the State's Confidential Information;

(f) continuously monitor its systems for potential areas where security could be breached.

6.2 Unauthorized Access. Contractor may not access, and shall not permit any access to, State Systems, in whole or in part, whether through Contractor's Systems or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State Systems must be solely in accordance with the Contract and this Exhibit, and in no case exceed the scope of the State's authorization pursuant to this **Section 6.2**. All State-authorized connectivity or attempted connectivity to State Systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

6.3 Contractor Systems. Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems) and networks used by or for Contractor in connection with the Services ("**Contractor Systems**") and shall prevent unauthorized access to State Systems through the Contractor Systems.

6.4 Security Audits. During the Term, Contractor will:

(a) maintain complete and accurate records relating to its data protection practices, IT security controls, and the security logs of any of the State's Confidential Information, including any backup, disaster recovery or other policies, practices or procedures relating to the State's Confidential Information and any other information relevant to its compliance with this **Section 6**;

(b) upon the State's request, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least five (5) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to, perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Contractor Systems and their housing facilities and operating environments; and

(c) if requested by the State, provide a copy of Contractor's SSAE 16 SOC 2 Type 2 audit report to the State within thirty (30) days after Contractor's receipt of such report. Any such audit reports will be recognized as Contractor's Confidential Information.

6.5 Nonexclusive Remedy for Security Breach. Any failure of the Services to meet the requirements of this Exhibit with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract upon fifteen (15) days written notice to Contractor and failure to cure, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

7. **Redundancy, Data Backup and Disaster Recovery**. Contractor must, in accordance with the provisions of this **Section 7**, maintain or cause to be maintained disaster avoidance procedures designed to safeguard State Data and the State's other Confidential Information, Contractor's processing capability and the availability of the Hosted Services, in each case throughout the Term and at all times in connection with its actual or required performance of the Services. The force majeure provisions of **Section 8.1** do not limit Contractor's obligations under this **Section 7**.

7.1 Redundant Hosting and Connectivity. Contractor will simultaneously operate a mirror system at a location in the continental United States that is geographically remote from the primary system on which the Service Software and Hosted Services are hosted. Except for its location, the mirror system must: (a) be identical in all respects to the primary system; (b) have hardware and software, network connectivity, power supplies, backup generators and other similar equipment and services that operate independently of the primary system; (c) have fully current backups of all State Data stored on the primary system; and (d) have the ability to provide the Hosted Services in accordance with the Contract during the performance of routine and remedial maintenance or any outage or failure of the primary system. Contractor will operate, monitor and maintain such mirror system so that it may be activated within five (5) hours of any failure of the Hosted Services to be Available.

7.2 Data Backup. Contractor will conduct, or cause to be conducted, daily back-ups of State Data and perform, or cause to be performed, other periodic back-ups of State Data on at least a weekly basis. On written notice from the State, Contractor will provide the State with a copy of the backed up State Data in such format as the State reasonably requests. The State will reimburse Contractor for all media costs and shipping charges reasonably incurred in fulfilling the State's requests for copies of backed up State Data.

7.3 Disaster Recovery/Business Continuity. Throughout the Term and at all times in connection with its actual or required performance of the Services hereunder, Contractor will:

(a) maintain a Business Continuity and Disaster Recovery Plan for the Hosted Services (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Upon request, Contractor must provide the State with a copy of its current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance; and

(b) provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under the Contract, in its sole discretion, immediately terminate the Contract for cause.

8. **Force Majeure**.

8.1 Force Majeure Events. Subject to **Section 8.3**, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

8.2 State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more, and the State will reimburse the contractor for work performed prior to such termination. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

8.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Exhibit:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions or malfunctions of Contractor Systems or any of Contractor's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Contractor Systems; or

(ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.

SCHEDULE C - END-USER LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY: This End-User License Agreement ("**EULA**") is a legal agreement between the State of Michigan the ("**Licensee**") and MorphoTrak, LLC ("**MorphoTrak**" or "**Licensor**") for Licensor's proprietary system software set forth in the Hosted Software Contract between Licensor and Licensee (the '**Hosted Contract**") that includes any and all associated media provided and otherwise made available to Licensee and the printed, online or electronic documentation ("**Documentation**") created by Licensor (collectively the "**Software**"). As of the effective date of the Hosted Contract, Licensee agrees to be bound by the terms of this EULA.

The Software is also protected by United States Copyright Laws and international Copyright treaties, as well as other U.S. and international laws. The Software is licensed and not sold to Licensee.

1. GRANT OF LICENSE. In consideration of Licensor's receipt of payment in full for all applicable license fees for the Software and all additional fees under the Hosted Contract, as well as Licensee's compliance at all times with the license terms and conditions in this EULA, Licensor hereby grants to Licensee a nonexclusive license only for the duration of the Hosted Contract to:

A. access and use the hosted and installed Software for Licensee's own internal operational use in furtherance of the program and limited to the workstations described in the Hosted Contract;

B. use the Documentation solely in furtherance of Licensee's use of the Software; and

C. make one (1) archival copy of the Software for disaster recovery purposes.

2. LICENSE LIMITATIONS AND RESTRICTIONS. Licensee's use of the Software is limited to Licensee's own internal operational use and is conditioned upon Licensor being paid all license fees and all other fees under the Hosted Contract. While the Software is designed to be configurable in certain functions in accordance with Licensor's functional specifications, Licensee shall not directly or indirectly modify or prepare derivative works based on the Software. Licensee shall not directly or indirectly reverse engineer, decompile, or disassemble the Software. Licensee shall not sublicense, rent, lease or otherwise make the Software available for beneficial use by any third party without Licensor's prior express written consent. The license granted in Section 1, herein, is personal to Licensee. However, Licensee may transfer any of its rights under this EULA only in accordance with the terms of the Hosted Contract.

3. OWNERSHIP OF INTELLECTUAL PROPERTY RIGHTS. All right, title and interest in and to the Software, and any all copies, modifications and derivative works based thereon, including all rights in Copyright and all other intellectual property rights, shall be owned solely by Licensor.

Any third party software components that are contained in the Software are licensed to Licensee under the terms and conditions of the third parties' software license agreements and other documentation that may be contained in the Documentation or other parts of the Software.

4. DISCLAIMER OF WARRANTIES. EXCEPT FOR THE EXPRESS WARRANTIES PROVIDED IN THIS EULA AND THE HOSTED CONTRACT AND TO WHICH LICENSOR MAY SEPARATELY AGREE IN WRITING WITH LICENSEE, LICENSOR HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. WARRANTY CLAIM / LICENSEE'S REMEDIES. If Licensor confirms that any copy of the Software delivered by Licensor to Licensee does not perform as warranted in the Hosted Contract, then Licensor will use reasonable commercial efforts to correct, repair or replace the Software and deliver a corrected version to Licensee at no additional cost to Licensee.

6. LIMITATION OF LIABILITY. THE LIABILITY BETWEEN LICENSOR AND LICENSEE WILL BE AS SET FORTH IN THE HOSTED CONTRACT.

7. TERMINATION. This License Agreement will terminate when the Hosted Contract terminates.

8. U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is commercial computer software that is provided to Licensee with RESTRICTED RIGHTS. Use, duplication or disclosure to the United States Government is subject to the restrictions as set forth in Federal Acquisition Regulation 12.212 for civilian agencies and Defense Federal Acquisition Regulation 227.7202 for military agencies.

9. SOFTWARE CHANGE ORDERS / UPDATES. This will be governed by the terms of the Hosted Contract.

10. SOFTWARE SUPPORT SERVICES. This will be governed by the terms of the Hosted Contract.

11. GOVERNING LAW. This EULA is governed by the laws of the State of Michigan, without regard to its conflict of laws provisions and excluding application of the Uniform Computer Information Transactions Act (UCITA).

12. ENTIRE AGREEMENT. The entire understanding between Licensor and Licensee concerning the licensing of the Software is contained in this EULA and the Hosted Contract. This EULA supersedes all prior and contemporaneous communications and agreements with respect to such subject matter. There are no representations, warranties, terms, conditions, undertakings or collateral agreements, express, implied or statutory, between the parties other than as expressly set forth in this EULA and the Hosted Contract. This EULA cannot be changed, modified, amended or terminated except by an instrument in writing executed by both Licensor and Licensee.

SCHEDULE D – PRICING

"Vendor Owned, Vendor Hosted" Milestone Payment Schedule Years 1-5

Month	Implementation Milestones				Cloud Service		Total Monthly Payment (Imp + Cloud)		Annual Total
0	Contract Signed								
1	Project Planning	10%	$250,000		$104,167		$354,167		
2	System Design Review	10%	$250,000		$104,167		$354,167		
3					$104,167		$104,167		
4					$104,167		$104,167		
5					$104,167		$104,167		
6	Development Complete	10%	$250,000		$104,167		$354,167		
7					$104,167		$104,167		
8					$104,167		$104,167		
9	Factory Acceptance	10%	$250,000		$104,167		$354,167		
10					$104,167		$104,167		
11					$104,167		$104,167		
12	Training	10%	$250,000		$104,167		$354,167		$2,500,000
13					$104,167		$104,167		
14	UAT	20%	$500,000		$104,167		$604,167		
15	Go Live	20%	$500,000		$104,167		$604,167		

16				$104,167	$104,167	
17				$104,167	$104,167	
18	PARE (90 days) Complete	10%	$250,000	$104,167	$354,167	
19				$104,167	$104,167	
20				$104,167	$104,167	
21				$104,167	$104,167	
22				$104,167	$104,167	
23				$104,167	$104,167	
24				$104,167	$104,167	$2,500,000
25				$84,008	$84,008	
26				$84,008	$84,008	
27				$84,008	$84,008	
28				$84,008	$84,008	
29				$84,008	$84,008	
30				$84,008	$84,008	
31				$84,008	$84,008	
32				$84,008	$84,008	
33				$84,008	$84,008	
34				$84,008	$84,008	
35				$84,008	$84,008	
36				$84,008	$84,008	$1,008,093
37				$86,108	$86,108	
38				$86,108	$86,108	
39				$86,108	$86,108	

40				$86,108	$86,108	
41				$86,108	$86,108	
42				$86,108	$86,108	
43				$86,108	$86,108	
44				$86,108	$86,108	
45				$86,108	$86,108	
46				$86,108	$86,108	
47				$86,108	$86,108	
48				$86,108	$86,108	$1,033,294
49				$88,260	$88,260	
50				$88,260	$88,260	
51				$88,260	$88,260	
52				$88,260	$88,260	
53				$88,260	$88,260	
54				$88,260	$88,260	
55				$88,260	$88,260	
56				$88,260	$88,260	
57				$88,260	$88,260	
58				$88,260	$88,260	
59				$88,260	$88,260	
60				$88,260	$88,260	$1,059,120
			$2,500,000	**$5,600,507**	**$8,100,507**	**$8,100,507**

Options

Year	Implementation Milestones				Cloud Service (Monthly)		Total Monthly Payment (Imp + Cloud)		Annual Total
Year 6					$90,284		$90,284		$1,083,408
Year 7					$92,584		$92,584		$1,111,008
Year 8					$94,941		$94,941		$1,139,292
Year 9					$97,357		$97,357		$1,168,284
Year 10					$99,833		$99,833		$1,197,996
Year 11					$102,372		$102,372		$1,228,464
Year 12					$104,974		$104,974		$1,259,688
Year 13					$107,640		$107,640		$1,291,680
Year 14					$110,374		$110,374		$1,324,488
Year 15					$113,176		$113,176		$1,358,112
	Total Options								**$12,162,420**
	Base + Options								**$20,262,927**

NOTES:

- System Implementation costs and System Refresh costs for the Vendor Owned State Hosted & Vendor Owned Vendor Hosted models are included in the annual payments.
- Disaster recovery is included in within the annual fees provided.

SCHEDULE E - DISASTER RECOVERY PLAN

SCHEDULE F - TERMS FOR ON-SITE WORKSTATIONS

1. **Definitions**. All initial capitalized terms in this Schedule that are not defined herein shall have the respective meanings given to them in the Contract.

2. **Workstations**. Contractor must provide fully functioning ABIS workstations and workstation peripherals, which will consist of the following (collectively, the "**Workstations**"), excluding desk furniture and chairs:

    a. ABIS Ten-print Terminal
        i. Desktop(11)
        ii. Laptop (2) for remote work
        iii. Flatbed scanners (11)
        iv. High Speed Duplex Scanner (2) Equivalent or better than Epson Expression 10000 XL
        v. Black and White Printers (11)
        vi. Color Network Printer (1)

    b. ABIS Latent Terminal
        i. Desktop (18)
        ii. Latent Flatbed Scanner (18)
        iii. Latent Camera (18)
        iv. Color Printer (17)

    c. Card Print
        i. Desktop, if necessary (1)
        ii. Printer (1)

3. **Delivery**. Contractor must deliver the Workstations to the locations designated by the State by the delivery date specified in the Statement of Work. Five days prior to the actual delivery date, Contractor must give written notice to the State specifying the precise delivery date and time. Contractor must pay all costs associated with replacing any item damaged in transit to the final destination. Contractor acknowledges that no item will be considered delivered on the delivery date if it is damaged or otherwise not ready for the State to begin its acceptance procedures. Contractor must, at a minimum, package the Workstations according to industry standards and include a packing slip with each shipment. Contractor must also arrange for any rigging and drayage necessary to deliver the Workstations. All costs associated with packaging, shipping, transportation, delivery and insurance are included in the implementation costs set forth in the Contract.

4. **Installation, Integration and Configuration**.

    a. Contractor must unpack, assemble, install, integrate, interconnect, and configure all the Workstations at the locations specified in the Statement of Work. Where necessary to complete installation, Contractor must provide all required moving and installation resources, including but not limited to personnel, packing material, and floor protection panels. After completing installation, Contractor must provide the State with written notification that the Workstations are ready for use.

b. Contractor must supply all materials required to complete the assembly, installation, integration, interconnection, and configuration of the Workstations at the locations specified in the Statement of Work so that they are ready for use and acceptance, including providing and setting up all required connections to the power supply and any other necessary cables and any other accessories or supplies.
c. Contractor must leave all work areas clean once installation is complete, which includes removing and disposing of all packing materials.
d. All costs associated with the installation services described in this **Section** are included in the implementation costs set forth in the Contract.

5. **Documentation**. Contractor must provide to the State all end-user documentation for the Workstations. The documentation, at a minimum, must include all the documentation available to consumers from the manufacturer of the Workstations about the technical specifications of the Workstations, installation requirements, and operating instructions, as well as details about the software programs with which the Workstations function.

6. **Acceptance**.

   a. The Workstations are subject to acceptance by the State. As part of its acceptance process, the State may test any function of the Workstations to determine whether they meet the requirements set forth in the Statement of Work. If the Workstations do not meet the requirements set forth in the Statement of Work, the State may reject the Workstations or require that they be corrected at Contractor's sole cost and expense before accepting them.
   b. Acceptance by the State does not relieve Contractor of its responsibility for defects in the Workstations or other failures to meet the requirements of the Statement of Work or of its support and maintenance obligations.
   c. The procedure for acceptance will be as follows:
      i. Contractor must notify the State in writing once the Workstations are ready for use, in accordance with **Section 4.a** above;
      ii. the State will have ten (10) Business Days to perform its acceptance procedures (the "**Acceptance Period**"); and
      iii. if the State provides notice of any deficiency during the Acceptance Period, Contractor must address the deficiency at no cost to the State as soon as possible and notify the State in writing once the work is complete, at which time the State will be entitled to re-inspect the Workstations and the Acceptance Period will start again.

7. **Warranty for Workstations**.

   a. Even if the State has accepted the Workstations, Contractor warrants that, throughout the Term, the Workstations will conform in all ways with the requirements set forth in the Statement of Work.
   b. This warranty does not apply to a specific item of the Workstations if the only reason that item fails to conform to the requirements of the Statement of Work is because:
      i. a person other than the Contractor, a subcontractor, or a person approved by either of them modifies the Workstations or attaches equipment to the

Workstations that was not designed or approved for use with the Workstations by the Contractor or the manufacturer of the Workstations; or

ii. the State uses consumable supplies or materials in or on the Workstations that are supplied by a person other than the Contractor, if those consumables or materials do not conform to the Workstation manufacturer's instructions to consumers.

c. Contractor must provide maintenance and support services for the Workstations throughout the Term in accordance with **Schedule B** to the Contract, the Service Level Agreement. All charges and costs associated with providing the maintenance and support during the Term are included in the Contract rates.

8. **Risk of Loss**. Contractor agrees to bear the risk of loss of or damage to the Workstations while they are being transported or installed and during the entire time the Workstations are in the State's possession, except losses or damages caused by the negligence of the State or someone acting on the State's behalf.

9. **De-installation and Removal of Workstations**.

   a. Contractor must de-install and remove the Workstations promptly after expiration or termination of the Contract. Contractor must provide all necessary removal resources, and must arrange for any necessary transportation, rigging and drayage in connection with the removal of the Workstations from the State's premises. All costs associated with the de-installation, removal and transportation to Contractor's premises are included in the implementation costs set forth in Contract.
   b. If Contractor does not de-install and remove the Workstations within thirty (30) days of the expiration or termination of the Contract, the State may arrange for the de-installation and removal of the Workstations, at the Contractor's cost. The State may deduct this amount from any amount owing by the State to the Contractor from time to time, under the Contract or otherwise.

Michigan State Police

Automated Biometric Identification System Requirements Project

EXISTING SYSTEMS REPORT – APPENDIX 1

May 15, 2015

Document Control Page

Document Status: Final
Document Date: May 15, 2015

Document Purpose

This report presents an overview of the existing Michigan State Police (MSP) Automated Fingerprint Identification System (AFIS) environment. This information will ultimately be included in the pending AFIS Request for Proposals (RFP) as background information for prospective bidders.

Version	Date	Description/Changes
0.1	4/15/15	Working draft for project team review.
0.2	4/28/15	Discussion draft reflecting updates from April 15, 2015, review sessions.
1.0	5/15/15	Finalized document reflecting all updates from May 13, 2015, review session.

TABLE OF CONTENTS

Page

Glossary

I. Introduction

The Michigan State Police (MSP) have engaged MTG Management Consultants, LLC, to assist with developing the requirements and other crucial content for a Request for Proposals (RFP) for the acquisition of a future Automated Biometric Identification System (ABIS). This deliverable outlines the key aspects of the currently deployed Automated Fingerprint Identification System (AFIS) at MSP. This information will ultimately be included in the pending ABIS RFP as background information for prospective bidders.

A. Background

MSP is interested in assessing its current biometric processing environment, planning for its desired future processing model, and conducting a complete and comprehensive acquisition of that future ABIS environment solution from a qualified vendor. In addition, MSP is interested in taking a "best practices" approach to the development of the RFP and associated documentation for the procurement of this solution.

B. Objective and Purpose

This document outlines the basic elements of MSP's current AFIS environment as a means to ensure that vendors proposing a replacement ABIS will have the requisite background and understanding of current operations. Aspects of the current operational environment will be critical to the understanding of proposing vendors in that it will provide them with the dimensions necessary to prepare an effective proposal.

C. Scope

The remainder of this document outlines the current MSP AFIS environment and is organized as follows:

- *Section II – General AFIS Topology.* An overview of the biometric systems, equipment, and interfaces currently in use.
- *Section III – Metrics, Records, and Transactions.* An enumeration of the general processing measurements associated with the current environment.
- *Section IV – Standards.* A description of the applicable standards currently applied.
- *Section V – Workflows*. A description of the general workflows associated with the current environment.

II. General AFIS Topology

This section provides an overview of the current MSP AFIS operating environment, including a look at each aspect of topology, hardware, input devices, and system interfaces and exchanges.

A. Introduction

In 2007, MSP executed a contract with NEC Corporation of America, Inc. (NEC) to implement the then-current version of AFIS, named AFIS21. AFIS21 went live in 2008 and continues as the current MSP biometric platform today.

B. Overview

The figure below depicts the topology of the current AFIS environment at MSP. This diagram serves as the primary reference point on which subsequently presented information is based.

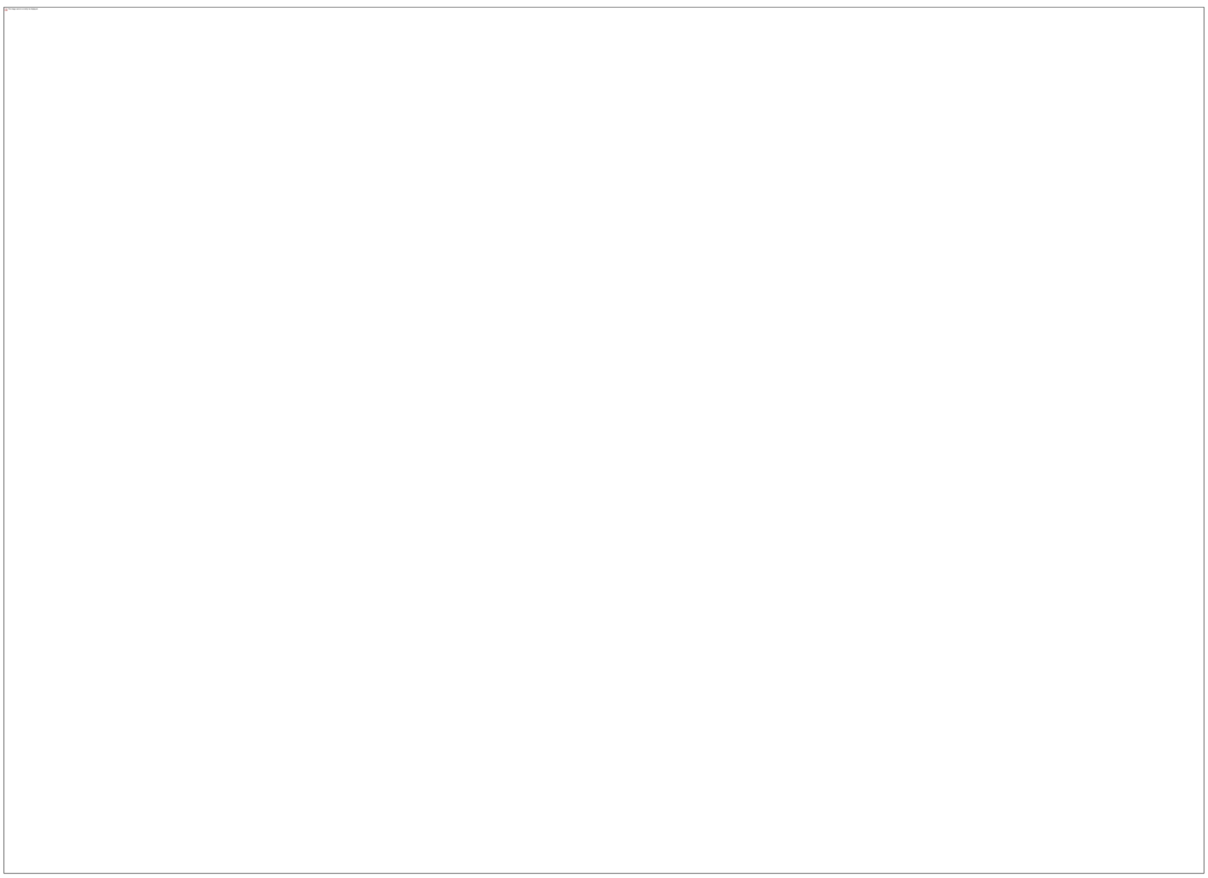


Figure 1: Current MSP AFIS Topology

- *MSP Data Center* – The items below are physically located at MSP's headquarters in Lansing, Michigan.
  - » *AFIS* – The current NEC AFIS system is composed of a series of servers, databases, and subsystems that perform the basic biometric identification matching and related administrative services. AFIS comprises several components including an image process controller, matchers, interface service, and administrative and reporting services.
  - » *Global Transaction Controller (GTC)* – GTC acts as the front-end processor for prioritizing and regulating transactions into AFIS.
  - » *Landing Server* – This component serves as a connection point for coordinating the receipt of transactions from live scan and mobile identification (MID) devices.
  - » *AFIS Archive* – The archive stores originally submitted images from live scan workstations and manual card entry for ease of retrieval and display.
  - » *MID Server* – This server provides a connection point for the BlackBerry-based MID infrastructure. Less than ten-finger transactions are forwarded to the landing server for AFIS processing.
  - » *Statewide Network of Agency Photos (SNAP)* – AFIS has an interface with SNAP by which every ten-print Electronic Biometric Transmission Specification (EBTS) file that AFIS receives from the field via live scan is forwarded to the SNAP server. No evaluation is made as to the contents having a mugshot or tattoo image. SNAP is required to evaluate the file and make appropriate use of the file. The one thing AFIS does before sending the file to SNAP is to strip out the type 15 (palms) before the file is placed in a location where SNAP can have access to it. In addition:
    - – SNAP servers will receive the files that are prepared by AFIS and transfer them via Secure File Transfer Protocol (SFTP). It will then delete the files off the directory structure on the AFIS server. AFIS needs to have the directory structure set to allow for large volumes of EBTS to be placed with a method prepared to store files if the interface is down for a time period.
    - – For MID, AFIS interfaces with SNAP to pull photos for mobile ID search candidates. Each mobile transaction could return up to six candidates. AFIS performs a SQL search on SNAP for each state identification SID number in the candidate list to query if a mug photo exists. The AFIS server will prepare and send back the response to the MID device.

    - Finally, SNAP also forwards the entire National Institute of Standards and Technology (NIST) package to the Courts and Law Enforcement Management System (CLEMIS) without the palm (NIST type 15) images. SNAP was purchased from and is maintained by DataWorks Plus.

  - *Workstations* – MSP maintains some latent and ten-print workstations at MSP headquarters.
- *CLEMIS* – Oakland County, Michigan, has a cooperative criminal justice and public safety systems environment that includes a stand-alone AFIS from 3M Cogent. From an architectural standpoint, the CLEMIS AFIS connects to MSP through the landing server using the same protocols as a live scan device.
- *Computerized Criminal History (CCH)* – AFIS interfaces with MSP's CCH system located at the MSP Criminal Justice Information Center (CJIC) also in the City of Lansing, Michigan. The CCH is a customized product from Science Applications International Corporation (SAIC), based on its ALIAS platform.
- *Statewide Terminals* – AFIS ingests images from regulated devices, or terminals, for matching and official registration of images. The following devices currently connect to AFIS:
  - *Live Scan Terminals* – These devices largely collect ten-print images and related NIST types depending on device capabilities. There are approximately 600 devices deployed statewide in various law enforcement-related facilities.
  - *Latent Terminals* – Latent terminals generally consist of software designed to capture and enhance photographic or scanned images from objects and/or their impressions using various forensic techniques. There are approximately 20 latent terminals statewide.
- *MID Deployments* – There are effectively three types of MID deployments associated with MSP's AFIS:
  - *Local MIDs* – These are MIDs managed by the particular local law enforcement agency. These devices conform to MSP security standards for purposes of transmitting and processing Ten-Print Fingerprint Image Search (TPIS) and Rapid Fingerprint Identification Search (RPIS) transactions.
  - *MSP MIDs* – MSP has an agreement with the Department of Information Technology to manage the delivery of BlackBerry-based MID transactions. As a note, this infrastructure is currently slated for replacement.
  - *Blackberry Replacement* – MSP has planned for MDC and Android deployment to replace Blackberry solution.

- *Department of Homeland Security (DHS)* – The MSP AFIS connects with the DHS US-Visit database for searching with DHS watch files.
- *Federal Bureau of Investigation (FBI)* – The MSP AFIS connects with FBI's Next Generation Identification (NGI) Integrated Automated Fingerprint Identification System (IAFIS) for searching images on watch lists and from jurisdictions outside Michigan.

C. AFIS Interfaces

The key interface/exchange elements shown in the topology figure above are described in the table below, along with an indication as to whether interface specifications are available.

Ref.	Interface/Exchange	Interface Specifications Available?	Reference Document
External Systems			
1	DHS US-Visit	Yes	FBI EBTS
2	FBI NGI	Yes	FBI EBTS
3	CLEMIS	Yes	Michigan EBTS (June 25, 2014)
Internal Systems			
4	CCH	Yes	Technical System Design Document
5	SNAP	Yes	DataWorks Plus Document
6	Live Scan Terminals	Yes	Michigan EBTS
7	Latent Terminals	Yes	Michigan EBTS
8	MID	Yes	MSP MID Submission to MSP and FBI Repository for Individuals of Special Concern (RISC)
9	Landing Server	No	NEC Proprietary

As indicated above, some interface specifications are proprietary and largely not available for reference without special circumstances.

D. AFIS Equipment

The subsections that follow provide a view of the various operational hardware, ten-print and latent terminal, and live scan device components utilized in the current AFIS environment.

1. AFIS Hardware Inventory

The table below provides a detailed listing of the core AFIS hardware components for the current system located at MSP headquarters in Lansing. This hardware occupies approximately six racks in MSP's data center.

Ref.	Description	Hardware	Quantity
1	NEC Repository Manager and System Controller	Dell PowerEdge 6850	1
2	NEC Matching Subsystem NEC Fingerprint Matching Processors	Dell PowerEdge 6850 NEC Proprietary	4 8
3	Transaction Controller	Dell PowerEdge 2950	2
4	Database Servers	Dell PowerEdge 2950	2
5	Image Processing Controllers	Dell PowerEdge 1950	4
6	NIST Archive	Dell PowerEdge 2950	2
7	Web Server	Dell PowerEdge 1950	2
8	Reports Server	Dell PowerEdge 1425	1

2. AFIS Workstations

AFIS workstation equipment is currently located at varying unique sites throughout the state. The table below provides a breakdown, by device, of the number and locations for these components.

Ref.	Workstation Type	Total Number	Location(s)
1	Ten-Print	11	Lansing (MSP Headquarters)
2	Latent	20	20 Locations Statewide
3	Print Server	1	Lansing (MSP Headquarters)

As a note, any on-site vendor presence in the future environment must include the use of its own workstations, which must be supplied in addition to MSP's workstation needs.

3. Live-Scan Deployment

Approximately 600 live scan devices are currently submitting transactions to the MSP AFIS:

- MSP maintains a contract with IDNetworks for 20 live scans at various MSP posts throughout the state. MSP is presently replacing these 20 via competitive procurement.
- Other vendors currently approved to sell and connect devices to the MSP AFIS are:
  - » MorphoTrust USA (using 3800 and 4800 series devices).
  - » ID Networks, Inc. (using Morpho 4800 and CrossMatch 500p devices).
  - » CrossMatch (using the 500p devices).
  - » DataWorks Plus (using CrossMatch 500p devices).

The above-listed devices are owned and operated by various business partners, including police departments, sheriff's offices, correctional agencies, civil background checking agencies, training facilities, probation and parole facilities, courts, and others (e.g., airports, school districts).

4. Applicant Live Scan

The state of Michigan has a contract with IdentoGO (MorphoTrust) to be within 50 miles of any applicant within 2 days. This contract is in place mostly for applicant licensing for other Michigan departments that pay for their applicants to be checked but any applicant can use this service. Applicants can be processed by law enforcement and other applicant vendors as well.

5. Latent Case Management

MSP forensic labs use a laboratory information management system (LIMS) from Forensic Advantage Systems to manage their forensic workload. In addition, labs use a recently acquired product from Foray, LLC, for latent case management. MSP labs prepare their latent fingerprints using Foray and track their efforts in LIMS. Technicians generally export images manually (in tagged image file format [TIFF]) from Foray using the AFIS Connect feature when they are ready to launch an AFIS search.

E. Reports

The current MSP AFIS produces many useful reports across the following dimensions:

- *System Level* – Showing the status of various aspects of the system and subsystems.
- *Live Scan/MID Transaction Level* – Showing the processing status and results for individual live scan and MID submissions.

- *Latent Transaction Level* – Showing the status and results of latent search transactions.
- *Statistical Level* – Showing various statistical aspects of system metrics and identification-related transactions.

The current reports are housed on a separate report server to serve the operational and historical needs of AFIS management. Specific examples of these reports will be included in a Reports Library (Exhibit 4).

F. Current Projects

There are five known project efforts that will impact the scope of MSP's AFIS replacement project:

- *Headquarters Move* – MSP is currently planning to move its main offices in downtown Lansing to another location in the Lansing area. The move is currently planned between September 2015 and December 2016. Details of where the replacement system will be installed and housed are subject to the move and may include options to house at other locations.
- *BlackBerry-Based MID Replacement* – The BlackBerry-based MID infrastructure currently managed by the Department of Information Technology will be de-commissioned prior to AFIS replacement. These devices will be replaced using a similar architecture as those presented as local MIDs in the discussions above, and the replacement will completed by September 2015.
- *Live Scan Replacement* – Approximately 20 live scan devices statewide will be replaced with more current devices. This is expected to occur in early 2016, and will affect live scan deployments in the locations statewide.
- *National Fingerprint File (NFF)* – MSP's CCH division is actively seeking to become NFF-compliant. As part of the current AFIS environment, provisions are being made to accommodate NFF requirements.
- *NGI Rap Back* – MSP retains applicant transactions and already has a state-oriented system for providing Rap Back functionality. Going forward, MSP will adopt the NGI Rap Back standard and is actively examining policies and procedures.
- Metrics, Records, and Transactions

This section includes general statistical information regarding current MSP AFIS processing, capacity, response time, and transaction types and records processed.

» Database Sizing and Growth

The table below summarizes the MSP AFIS sizing and growth as of January 2015.

Ref.	Record Type	01/2015 Number	Historical Annual Growth Rate
1	Ten-Print – Card	4,010,992	7%
2	Ten-Print – Palm	736,614	35%
3	Ten-Print – Slap	2,264,798	20%
4	Latent – Card	59,040	n/a
5	Latent – Case	40,416	n/a
6	Latent – Palm	3,577	n/a
7	Archive – Transaction Control Numbers (TCNs)	6,786,346	12%
8	Archive – SIDs	3,288,952	7%
9	Archive – SIDs Deleted	20,497	n/a

For instances in which annual growth measures are listed as not applicable (n/a), no information was available or it is not tracked.

» Throughput Capabilities

The table below provides a summary currently contracted AFIS transactional throughput capabilities. These are presented as contractual performance limits, not actual processing metrics:

Ref.	MSP Record Type	Peak Hour	Per Day	Per Year
1	Ten-Print Submissions	500	5,500	2,000,000
2	Ten-Print Cold Searches	275	2,200	n/a
3	Ten-Print-to-Latent Inquiries	500	5,500	n/a
4	Palm Submissions	n/a	1,000	n/a
5	Latent Inquiries	n/a	100	n/a
6	Latent Palm Inquiries	n/a	50	n/a
7	Mobile Identification Inquiries	n/a	1,500	n/a

G. NIST Record Types Supported

The current MSP AFIS solution provides the ability to ingest, match, and archive a portion of the 20 record types currently identified by NIST.[1] As part of any acquisition approach, MSP will procure a solution having equal or enhanced transactional capabilities. The table below identifies the current NIST record types in use at MSP.

NIST Type	Description	Ingest	Match	Archive
1	Record header information.	X		X
2	Demographic, charge, and user-defined information.	X		X
3	Gray scale fingerprint images (low resolution).			
4	Live Scan/CardScan ten-print images (500 dpi).	X	X	X
5	Low-resolution fingerprint binary image data.			
6	High-resolution fingerprint binary image data.			
7	User-defined (scanned documents) images.			
8	Digitized signatures.			
9	Fingerprint minutiae data.			
10	Mugshots and photos (scars, marks, and tattoos [SMTs]).	X	X	X
11	*Reserved.*			
12	*Reserved.*			
13	Latent fingerprint images.	X	X	
14	Individual (including flat/slap) fingerprint images.			
15	Palm prints.	X	X	X
16	User-defined images.			
17	Iris images.			
18	*Reserved.*			
19	*Reserved.*			

1 ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar, Mark, and Tattoo (SMT) Information, Section 7.

NIST Type	Description	Ingest	Match	Archive
20	Source representation data.			
21	Associated context (audio/visual/other) data.			
98	Security information.			
99	Common Biometric Exchange File Format (CBEFF) data.			

Legend

X = As of April 2015, this is supported in the current MSP AFIS environment.

H. Identification TOTs Supported

Below are the specific identification types of transaction (TOTs) currently supported and processed in the identification environment (as defined in the Michigan EBTS).

TOT	Transaction Name
CAR	Criminal Ten-Print Submission
MAP	Miscellaneous Applicant Civil
TPIS	Ten-Print Fingerprint Image Search (MID)
DEK	Known Deceased
DEU	Unknown Deceased
MPR	Missing Persons
AMN	Amnesia Victim
CNA	Criminal Ten-Print Submission (no answer necessary)
NFUF	Non-Federal Applicant User Fee
RPIS	Rapid Fingerprint Identification Search
RPISR	Rapid Fingerprint Identification Search Response
CONV	Palm Conversion, Manual Entry
ARCH	Add Images to Archive

Other TOTs are supported through MSP's compliance with the FBI EBTS (version 9.4).

III. Standards

This section presents an overview of the national, state, and local standards and policies applicable to MSP's AFIS environment, as well as an assessment of the compliance status of the current environment. Finally, the section at any network/communication and technology standards applicable in Michigan.

A. Applicable Data and Transaction Standards

Current standards and models applicable in the existing AFIS environment are:

- Michigan Electronic Biometric Transmission Specification (EBTS), June 25, 2014.
- American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, 2011.
- Electronic Biometric Transmission Specification (EBTS), IAFIS-DOC-01078-9.4.
- IAFIS-IC-0110 (V3), 1993. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.
- IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.
- IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.
- NIST Best Practice Recommendation for the Capture of Mugshots. Version 2.0. September 23, 1997.
- FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.0, CJIS Security Policy, Version 5.0, dated February 9, 2011.

B. Compliance Status

The table below outlines the compliance status for the current AFIS operating environment in the terms of standards and policies.

Ref.	Standard/Policy	Compliance Status
1	CJIS Security Policy	✓
2	ANSI-NIST ITL 1-2011	✓
3	FBI EBTS, Version 9.4	✓

Ref.	Standard/Policy	Compliance Status
4	Latent Interoperability Transmission Specification (LITS) 2012	✓
5	IAFIS-IC-0110 (V3), 1993 WSQ Standard	✓
6	IS 10918-1, 1994 JPEG Standard	✓
7	IS 15444-1, 2001 JPEG 2000 Standard	✓
8	NIST Best Practice Recommendation for the Capture of Mugshots v2.0	✓
9	Michigan EBTS	✓

Legend

✓ = Operational compliance.

It should also be noted that the standards and policies above are current as of this publication. It is anticipated that these documents will continue to be updated to reflect emerging requirements, and this documentation will be modified as necessary to remain current.

C. Communication / Network Standards

MSP communicates with other systems through one or a combination of these three communication methods:

- TCP direct socket-based communication.
- Secure FTP-based communication using NIST standards (for Live scan).
- SMTP-based communications (for FBI).

D. Technology Standards

MSP adheres to applicable technology standards and policies from the Michigan Department of Technology, Management and Budget (DTMB). These standards are located at the following Web site: http://michigan.gov/dtmb/0,5552,7-150-56355---,00.html

IV. Workflows

The current MSP AFIS is modeled according to several workflows. A detailed explanation of these are contained in the MSP AFIS Implementation Plan Document from NEC, dated May 22, 2008, and is outlined here with permission. For functional reference, system workflows are organized as follows:

A. Automated Workflow Management Facility

The Automated Workflow Management Facility (AMF) works as the automated transaction workflow manager and is responsible for managing the following basic workflows:

- Live Scan Workflow.
- Match Process.
- Hit Process.
- No Hit Process.
- Substitution.
- Consolidation.
- NIST CardScan (Palmprint).
- Ten-Print Delete From CCH.
- Ten-Print Update From CCH.

B. Manual Ten-Print, Palmprint, and Slap Workflow

The Manual Workflow Management Facility (MMF) works as the manual transaction workflow manager and is responsible for managing the following basic workflows:

- TR & T/LI (Combination function Ten-Print Finger Registration and Ten-print to Latent Inquiry).
- TR-P & T/LI-P (Combination function Ten-Print Palm Registration and Ten-Print to Latent Palm Inquiry).
- T/LI T/LI#2 (Ten-Print to Latent Inquiry or Ten-Print to Latent Inquiry #2 [input from AFIS database]).
- T/LI-P (Ten-Print to Latent Palm Inquiry or Ten-Print to Latent Palm Inquiry #2 [input from AFIS database]).
- TR (Ten-Print Registration Finger).

- TR-P (Ten-Print Registration Palm).
- TR-S (Ten-Print Registration Slap).
- RS/RSS (Roll print Substitution [initial function] or Roll print Substitution subsequent [from the Job queue]).
- RS-P/RSS-P (Roll print Substitution Palm [initial function] or Roll print Substitution subsequent palm [from the Job queue]).
- RS-S/RSS-S (Roll print Substitution Slap [initial function] or Roll print Substitution subsequent Slap [from the Job queue]).
- TD (Ten-Print Delete).
- TD-P (Ten-Print Delete Palm).
- TD-S (Ten-Print Delete Slap).
- TI & TR & T/LI (Combination function: Ten-Print Inquiry, Ten-Print Registration and Ten-Print-to-Latent Inquiry - Full Record Fingers, Slaps and Palms).
- TI (Ten-Print Inquiry).
- TI#2 (Ten-Print Inquiry #2 [input from AFIS database]).
- TU (Ten-Print Update).

C. Latent Manual Functions

In addition, the MMF works as the manual transaction workflow manager responsible for managing the following basic latent workflows:

- LI & LR & L/LI (Combination function: Latent Inquiry, Latent Registration and Latent to Latent Inquiry).
- LI-P & LR-P (Combination function: Latent Inquiry Palm and Latent Registration Palm).
- LI (Latent Inquiry).
- LI-P (Latent Inquiry Palm).
- LI#2 (Latent Inquiry #2 [search Image comes from database]).
- LI-P#2 (Latent Inquiry Palm #2 [search Image comes from database]).
- L/LI (Latent to Latent Inquiry).
- L/LI#2 (Latent to Latent Inquiry [search Image comes from database]).
- L/LI-P (Latent to Latent Inquiry Palm).
- LR (Latent Registration).
- LR-P (Latent Registration Palm).

Glossary

This table presents a glossary of the acronyms used in this report.

Acronym	Definition
ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
AMF	Automated Workflow Management Facility
AMN	Amnesia Victim
ANSI	American National Standards Institute
ARCH	Add Images to Archive
CAR	Criminal Ten-Print Submission
CBEFF	Common Biometric Exchange File Format
CCH	Computerized Criminal History
CJIC	Criminal Justice Information Center
CJIS	Criminal Justice Information Services
CLEMIS	Courts and Law Enforcement Management System
CNA	Criminal Ten-Print Submission (No Answer Necessary)
CONV	Palm Conversion, Manual Entry
DEK	Known Deceased
DEU	Unknown Deceased
DHS	Department of Homeland Security
DTMB	Department of Technology, Management and Budget
EBTS	Electronic Biometric Transmission Specification
FBI	Federal Bureau of Investigation
GTC	Global Transaction Controller
IAFIS	Integrated Automated Fingerprint Identification System
JPEG	Joint Photographic Experts Group
LI	Latent Inquiry

Acronym	Definition
LI#2	Latent Inquiry #2
LIMS	Laboratory Information Management System
LI-P	Latent Inquiry Palm
LI-P#2	Latent Inquiry Palm #2
LITS	Latent Interoperability Transmission Specification
L/LI	Latent-to-Latent Inquiry
L/LI#2	Latent-to-Latent Inquiry #2
L/L-P	Latent-to-Latent Inquiry Palm
LR	Latent Registration
LR-P	Latent Registration Palm
MAP	Miscellaneous Applicant Civil
MID	Mobile Identification
MMF	Manual Workflow Management Facility
MPR	Missing Persons
MSP	Michigan State Police
NEC	NEC Corporation of America, Inc.
NFF	National Fingerprint File
NFUF	Non-Federal Applicant User Fee
NGI	Next Generation Identification
NIST	National Institute of Standards and Technology
RFP	Request for Proposals
RISC	Repository for Individuals of Special Concern
RPIS	Rapid Fingerprint Identification Search
RPISR	Rapid Fingerprint Identification Search Response
RS	Roll Print Substitution
RS-P	Roll Print Substitution Palm
RS-S	Roll Print Substitution Slap
RSS	Roll Print Substitution Subsequent
RSS-P	Roll Print Substitution Subsequent Palm
RSS-S	Roll Print Substitution Subsequent Slap
SAIC	Science Applications International Corporation
SFTP	Secure File Transfer Protocol
SMT	Scar, Mark, and Tattoo
SNAP	Statewide Network of Agency Photos
TCN	Transaction Control Number
TD	Ten-Print Delete
TD-P	Ten-Print Delete Palm

Acronym	Definition
TD-S	Ten-Print Delete Slap
TI	Ten-Print Inquiry
TI#2	Ten-Print Inquiry #2
TIFF	Tagged Image File Format
T/LI	Ten-Print-to-Latent Inquiry
T/LI#2	Ten-Print-to-Latent Inquiry #2
T/LI-P	Ten-Print-to-Latent Palm Inquiry
T/LI-P#2	Ten-Print-to-Latent Palm Inquiry #2
TOT	Type of Transaction
TPIS	Ten-Print Fingerprint Image Search
TR	Ten-Print Registration Finger
TR-P	Ten-Print Registration Palm
TR-S	Ten-Print Registration Slap
TU	Ten-Print Update