EXHIBIT B

Statement of Work

The purpose of the Statement of Work is to define the standard work performed on a project by both the Monterey County Sheriff's Office (MCSO) and IDEMIA. The goal is to ensure that roles, responsibilities, and deliverables are clearly defined so that the project is delivered on time, on budget, and with the highest customer satisfaction.

1 IDEMIA and Customer Responsibility Matrix

Table 1 defines IDEMIA and Monterey County Sheriff's Office responsibilities for project activities and deliverables.

Table 1: Activities and Deliverables

IDEMIA Responsibility	MCSO 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 PM 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. – Manage subcontractors (if applicable) – Develop and maintain the Project Management Plan and schedule – Conduct the project's status meetings and provide status reports. – Create and maintain an Action Item Log. – Resolve deviations from the project scope and administer change control.	• Provide a Project Manager (or Program Manager) to review / approve all deliverables, final acceptance, and any change orders. • Your PM should also: – Serve as IDEMIA'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. – Work with our personnel to verify the resolution of Action Item Log issues. – Ensure the IDEMIA personnel have the necessary site access and a safe work environment.
Project Design Services	
• Draft all Design Documentation in the List of Deliverables (Table 7) and provide to the MCSO for review, comment, and approval.	• Participate in Requirements gathering to support development of Design Documentation. • Provide information regarding current system performance and functionality. • Review, provide feedback on, and approve the Project Design Documents by the scheduled

IDEMIA Responsibility	MCSO Responsibility
	deadline and in accordance with this Statement of Work. • Issue Change Requests for any post contract changes required changes to the approved and agreed documents in accordance with the procedure described in Table 10 of this Statement of Work.
Electronic Data Migration	
• Please see Section 1.3 of this Statement of Work.	• Please see Section 1.3 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 necessary, and the MCSO will be notified of the changes. • Procure the hardware and third-party software listed on the BOM. • Inventory the material. • Stage the equipment as needed for factory testing.	• Obtain the Customer-provided hardware, if any, ensuring it meets the requirements specified in the approved Design Documentation. • If required, ship Customer-provided hardware to IDEMIA for factory staging.
Engineering Integration	
• Configure the commercial-off-the-shelf (COTS) software according to the requirements in the approved Design Documents: – Develop, test, and implement all the workflows. – Develop, test, and implement the interfaces on IDEMIA software side required for the system operation, as defined in the Interface Control Documents (ICDs). – Provide simulators / test files for the IDEMIA software side to allow the Customer to test the external system interfaces prior to the on-site integration. Simulators will reflect functionality and 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 IDEMIA software according to the Requirements Definition Document (RDD). – Configure the data storage, backup, security, and user management for the	• Develop, test, and implement any required interfaces from the Customer systems to the new IDEMIA system as required by the ICD(s). • Provide test files / simulators for the external systems to allow IDEMIA to perform testing prior to the on-site integration. • Configure network (LAN / WAN) and security on customer premises according to the RDD, including all necessary Network Area Translation on the customer network. • Provides IDEMIA with blocks of private IP addresses that we can use for workstations and customer-facing servers (IPs of workstations and customer-facing servers must be private IPs, allocated by the customer to IDEMIA, IDEMIA will not buy or lease any public IP). • Provide 3 blocks of 24 IP addresses (for production, disaster recovery. and test systems)

IDEMIA Responsibility	MCSO Responsibility
items that are under IDEMIA responsibility. • Load the software and converted / migrated data on the staged equipment and perform integration testing of basic functionality testing to verify the system is ready for further testing. • Conduct a Qualification Test Readiness Review (QTRR).	
Factory Testing	
• Draft a Test Plan and Test Procedures for your review and approval. The Test Procedures are designed to validate the approved requirements. • Perform Qualification testing per the approved Test Plan. Note that interfaces are simulated for all factory testing. • Note any issues and their severity in the IDEMIA JIRA Ticket database and track the resolution. • Conduct a Factory Acceptance Test (FAT) per the approved Test Plan. • Track any issues found during the FAT on a punch list and provide a plan for resolution.	• Review, provide feedback on and approve the Test Plan and Test Procedures. • Attend the FAT and participate in the testing. • For each test scenario, either provide approval or note discrepancies.
Site Preparation	
• Perform site surveys as needed. • With regards to equipment installed on customer's premises: Provide site preparation documentation identifying the power, network, air conditioning, space, cabling, access, security, and equipment layout requirements for system implementation.	• Approve the scheduling of the hardware / COTS / IDEMIA software delivery. • Identify the locations for each item procured. Provide a physical address, contact name, and contact phone number for each site. • Provide access to the sites for site surveys by IDEMIA 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 MCSO is responsible for the local area and wide area networks and the connectivity to the Microsoft Azure data center. Performance will be affected by network bandwidth. • IDEMIA requires a minimum 100Mbps Central Site connection to WAN recommended. • 10Mbps is recommended for remote sites connection to Central Site for best performance (all

IDEMIA Responsibility	MCSO Responsibility
	remote communications are channeled through the central site connection point to the Cloud). • If MCSO elects to use Azure ExpressRoute to connect to IDEMIA Cloud, MCSO will own the ExpressRoute subscription which will terminate in MCSO's tenant from which appropriate traffic will be routed to IDEMIA Cloud. • The MCSO is responsible for network connectivity with Azure and power reliability and availability of workstations and equipment deployed on customer's premises. Failure in these areas cannot be counted against IDEMIA's reliability and availability of contractual requirements. • Provide a formal notice for IDEMIA indicating that the site preparation has been completed and validated, and the interconnection is operational before equipment is shipped to the sites. • If the network is not functioning per the specifications when IDEMIA arrives for installation, the MCSO should address requests for correction within one day. Delays will impact the schedule and may result in additional charges for labor, lodging, and per diem for the employees on site for the duration of the extension. • Provide a temporary storage area for the delivered hardware if required.
Shipping and Delivery	
• Provide a schedule for shipping and delivery to each site. • 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 IDEMIA software to the designated target sites.	• Approve the schedule for shipment and delivery of the hardware and software for each site. • Provide assistance as required to ensure shipments clear Customs, if applicable. • Pay import taxes and duties, if applicable. • Provide ship authorization. • Receive all material and immediately notify IDEMIA of any visible damage to shipping containers. • Provide temporary storage for the delivered hardware if required.
Deliverables: Hardware, Software, and Services	
• The MBIS and its software reside in the cloud. Where IDEMIA is requested to deliver workstation hardware and software, we will provide the following, to be owned and maintained by IDEMIA. – Latent Expert workstations – Tenprint Card Capture workstations – Reviewer workstations • IDEMIA Professional Services, including:	• Should MCSO wish to purchase and maintain its own hardware, IDEMIA will define minimum specifications in the Requirements Definition Document for the following: – Latent Expert workstations – Tenprint Card Capture workstations – Reviewer workstations

IDEMIA Responsibility	MCSO Responsibility
– Technical Requirements – Data migration services – Program / Project Management – Systems Engineering – System Integration – Installation and Test – Factory and Site Acceptance Test (FAT / SAT) – Training	
Installation and On-Site Integration Testing	
• Propose the site-by-site installation schedule in advance of delivery. • Unpack, inventory and install all IDEMIA-provided workstation 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.	• Confirm the installation schedule in advance of delivery. • Provide access to the sites for IDEMIA and IDEMIA 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, FBI, CCH, etc.). • Provide access to the site during standard business hours for all on-site implementation work. IDEMIA may request site access outside of standard business hours as needed to maintain the schedule, but it will be the MCSO's decision whether or not to approve the request. • In the event that MCSO provides the workstation hardware, the systems will be loaded with the Operating System and antivirus software, placed in their operating locations, provided with power and networking ready for IDEMIA configuration. • Provide authorization to proceed with the 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.	• Participate in the SAT, sign off on passed tests, and identify 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.
Training Documentation	
• Deliver the user manuals for IDEMIA applications.	• The MCSO may make unlimited electronic copies for internal use.

IDEMIA Responsibility	MCSO Responsibility
• Deliver the administrator manual(s) for the system. • Deliver all other contracted training materials.	
Training	
• Draft a training schedule based upon the MCSO's organizational and contractual requirements. • Provide operator workstation training and system administrator training per the approved schedule. • Provide attendance sheets and training certificates. • Provide, collect, and review feedback forms. • Trainers provide contact information for follow up questions.	• Review, comment on, and approve the 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. • Trainees are encouraged to provide feedback on the training courses.
Cutover	
• Provide a Transition Plan and schedule. • Work with the MCSO staff to place the system in production status. • Monitor system performance for a minimum of three days to ensure transactions are being processed properly. • Report issues to the Customer Support Center for Support tracking. • Complete a final residual migration 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 scheduled downtime, and provide a procedure for reporting 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 migration. • Participate in the Final Acceptance Review. • Provide Final Acceptance.
Travel	
• Organize IDEMIA personnel travel. • Pay for IDEMIA personnel travel expenses.	• Organize any MCSO personnel travel. • Pay for MCSO personnel travel expenses.

2 Training Course Summary

Table 2 defines the training sessions that will give MCSO personnel the skills they need to be successful using their new MBIS.

Table 2: Training Overview

Type of Training / Class Duration / # of Attendees	Locations	Number of Sessions	Course Overview
MBIS System Administrator • 3 Days • 5 Trainees Max.	Central Site	1	This course teaches the skills needed to use and deliver training on the Workstation Operations. The course covers: • LINUX and Windows operating systems • User management, including adding, removing users, and changing user roles • System management and monitoring • Database maintenance and management • System monitoring and troubleshooting • Report generation • Statistical reporting, which includes accuracy and productivity • Workstation and peripheral operations • System performance tools
Tenprint Operator Card Capture • 2 Days • Up to 10 trainees total, with 2 per workstation	Central Site	1	This course teaches the skills needed to use and deliver training on the Workstation Operations. The course covers: • Best-practice recommendations • Tenprint / Palm Print entry • Identification – Tenprint • Fingerprint focal points • Deleting and editing minutiae • Enhancing fingerprint images • Quality control • Searches –Tenprint and Palm Print • Handling exceptions and errors • "Lights out" processing • Processing Manual Cards
Latent Operator Latent Expert • 3 Days • Up to 10 trainees total, with 2 per workstation	Central Site	1	This course teaches the skills needed to use and deliver training on the Workstation Operations. The course covers: • Best-practice recommendations • Latent-Print entry • Fingerprint focal points • Deleting and editing minutiae • Minutiae encoding and placement • Enhancing fingerprint images • Latent searches • Searches of the Unsolved Latent File (ULF) • Handling exceptions and errors
Optional **MBIS Archive Service**	Central Site	1	This course teaches the skills needed to use the MBIS Archive Service Application. The course covers:

Type of Training / Class Duration / # of Attendees	Locations	Number of Sessions	Course Overview
This training is covered in the CC and LE classes • 1 hour • Up to 10 trainees with 2 per workstation			• Searching for Records • Understanding NIST format • Printing Finger / Palm Cards • Deleting Records
Optional **Mobile Device - MorphoIDent** • 2 hours • 10 Trainees Max	Central Site	1	This course teaches the skills needed to use and deliver training on the mobile devices. The course covers: • Best-practice recommendations • Connecting / Pairing the device • Fingerprint capture • Viewing results • Browsing and deleting cases
Optional **Mobile Device - RapID™ X1** • 2 hours • 10 Trainees Max	Central Site	1	This course teaches the skills needed to use and deliver training on the mobile devices. The course covers: • Best-practice recommendations • Connecting / Pairing the device • Fingerprint capture • Viewing results • Browsing and deleting cases

3 System Operations, Monitoring, & Administration Tasks

Table 3 defines IDEMIA and MCSO responsibilities for system operations, monitoring, and administration tasks.

Table 3: System Operations, Monitoring, and Administration Tasks

IDEMIA Responsibility	MCSO Responsibility
System Operations Report	
• Capacity and Throughput reporting	• Run system operations reports.
LAN / WAN Administration and Supervision	
• N / A	• Provide all LAN / WAN administration, supervision, and support.
User Management	

IDEMIA Responsibility	MCSO Responsibility
N / A	• MCSO System administrators will be responsible for user management including: – Creating users. – Establishing and modifying user access rights. – Enabling and disabling user accounts. – Deactivating users.
Help Desk	
• Provide Call Center support per your service agreement, including a 1-800 number and e-mail access. • Record and track all service calls in our database. • Dispatch local Customer Support Engineers as may be required, according to service level agreement	• N / A
Delivery of Consumables	
N / A	• Customer is responsible for any consumables to maintain operations of local workstations (for example, ink cartridges, paper, etc.)
System Monitoring	
• IDEMIA will be responsible for monitoring, which includes: – 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. – Notifications when an abnormal event is detected with regards to responsibilities outlined above.	• MCSO System Administrator will be responsible for monitoring: – In-process transactions – Notifications when an abnormal event is detected with regards to in-process transactions
System and Transaction Management	
• IDEMIA will manage key components of the system, including: – Starting and stopping all services, interfaces, and databases of the system	• MCSO 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; to include taking the appropriate action.	• N / A

IDEMIA Responsibility	MCSO Responsibility
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, Texas, if the main system is hosted in Virginia).	• N / A

4 System Maintenance Tasks

Table 4 defines IDEMIA and MCSO responsibilities for system maintenance tasks.

Table 4: System Support and Maintenance Tasks

IDEMIA Responsibility	MCSO Responsibility
Hardware Preventive Maintenance	
• Perform all necessary preventive hardware maintenance for hardware and software provided by IDEMIA.	• Perform all necessary preventive hardware maintenance, for hardware and software (OS) provided by MCSO.
Software Preventive Maintenance	
• Perform log analysis and software updates, and load any software updates and upgrades required to ensure software is current and performing per specification.	• N / A
Anti-Virus	
• Run Windows anti-virus software on workstations prior to shipping, and the back end system. • Assist MCSO IT personnel with implementation of anti-virus update schema.	• Manage Workstation virus protection after the system is installed, including definition downloads, virus checking, and reporting.
Performance Analysis and Tuning	
• Conduct monthly reviews of system capacity, usage, performance indicators, and event logs to identify potential problems. • Routinely evaluate performance indicators, and modify system parameters and configurations to maintain optimum performance. Implement approved changes.	• Review and approve configuration changes.
Remedial Maintenance Support	
• Repair, replace, or upgrade hardware as necessary to ensure that failed or degraded	• N / A

IDEMIA Responsibility	MCSO Responsibility
hardware is performing per specification within the conditions of the maintenance contract. • Perform log analysis and technical investigations as necessary to diagnose system events. • Produce software updates and fixes within the conditions of the maintenance contract. This may include source code analysis and patch creation. • Test and install software updates and fixes in the production environment within the conditions of the maintenance contract.	
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	
• Perform record analysis as necessary to address issues such as missed identifications or other record processing anomalies.	• Notify IDEMIA of any known anomalies, such as missed identifications.

5 Electronic Data Migration

This section covers the responsibilities of IDEMIA and MCSO with regard to the electronic migration of data from the MCSO legacy system to the new MBIS.

5.1 IDEMIA Responsibilities

Table 5 lists IDEMIA responsibilities for electronic data migration.

Table 5: IDEMIA Responsibilities for Electronic Data Migration

IDEMIA Responsibilities for Electronic Data Migration	
1	Provide a migration plan describing how the data migration will be performed
2	Work with the Customer to define NIST-compliant file formats for the legacy MorphoTrust electronic records.
3	• Process the data to: – Re-extract and replace all matching features for the tenprint data where the quality of the images permits. – Convert descriptor data from the legacy format to the replacement system format.

IDEMIA Responsibilities for Electronic Data Migration	
	– Add default values for new mandatory fields.
4	Add tenprint and mugshot data to the new system.
5	Create both the Advance Data Services (ADS) database and the Multi-Biometric Search Services (MBSS) database.
6	Perform both a primary migration and subsequent residuals to capture all the data up to the time of cutover.
7	Provide a migration report listing which records were migrated successfully and which could not be migrated, with explanations for the exceptions.

5.2 Monterey County Sheriff's Office Responsibilities

Table 6 lists MCSO responsibilities for electronic data migration.

Table 6: MCSO Responsibilities for Electronic Data Migration

MCSO Responsibilities for Electronic Data Migration	
1	• Review and approve the Data Migration Plan: – One aspect of migration is mapping fields from the legacy system to descriptors in the new database. The Customer must review the migration plan and verify that the mapping is correct, otherwise additional migration scripts may have to be run after the database load. – Additions to the proposed migration scope or changes after the Migration Plan has been approved require a Change Order. IDEMIA reserves the right to charge for Change Requests that involve additional equipment, functionality, or labor.
2	Provide access to the legacy system in order to copy the existing data as either a backup or an Oracle export, whichever is appropriate.
3	Provide remote access into the legacy system and replacement system for migration personnel for the duration of migration.
4	Ensure the quality of the data being provided.

EXHIBIT C

List of Deliverables

Table 7 provides a list of standard list of project deliverables. MCSO approval is required as indicated.

Table 7: Standard List of Deliverables and Customer Approvals

	Name	Customer Approval Required
1	Project Management Plan and Microsoft Project Schedule	Yes
2	Requirements Definition Document (RDD)	Yes
3	Data Dictionary	Yes
4	Interface Control Document(s) (ICDs) – one per interface Note: Customer should provide an ICD for any existing interface(s)	Yes
5	Status Reports	No
6	Site Preparation Plan	Yes
7	Data Migration Plan	Yes
8	Acceptance Test Plan	Yes
9	Training Plan	Yes
10	Installation & Deployment / Transition Plan	Yes
11	User Manuals	No
12	System Administrator Manuals	No
13	Hardware as described in the Proposal and / or requirements specification	No
14	Software as described in the Proposal and / or requirements specification	No
15	Third-party Software Licenses	No
16	Training Courses	No
17	Final Acceptance Certificate	Yes

IDEMIA's planning process is based upon a single review cycle for each document. Generally speaking, the process is as follows:

1. IDEMIA will deliver a document for the MCSO to review.
2. The MCSO will have one week to review and respond.
3. IDEMIA will then update the document and return it to the MCSO
4. The MCSO will have one week to review and approve the document.
5. If no agreement is reached, a conference call or meeting will be scheduled and the issues will be discussed until an agreement is reached. MCSO approval must not be unreasonably delayed.

If the MCSO and IDEMIA do not approve the documents by the scheduled date(s), the schedule must be re-planned once agreement is achieved. The schedule slip may be more or less than the actual approval delay based on the affected dependencies.

Additional documents required by the MCSO will need to be defined and require a Change Order.

EXHIBIT D

Customer Milestones

Customer milestones are incorporated into the project's Master Schedule. If these tasks are not completed by the dates listed in the schedule, the schedule may have to be re-planned after the tasks are completed. The schedule slip may be more or less than the actual delay, based on the affected dependencies. Significant schedule changes required as a result of missed customer milestones may result in a billable Change Order.

Table 8 lists the customer milestones.

Table 8: MCSO Milestones

MCSO Milestones	
1	Data migration – Availability of cards and or electronic data at required quality level
2	Approval of all documents listed in the Customer Approval List (Table 7)
3	Site readiness (To be confirmed for each site)
4	Network readiness (To be confirmed for each site)
5	Customer contractor readiness (Applies to third-party contractors who may be responsible for interfaces or other functionality)
6	Import payments and any other import facilitation, if applicable
7	Availability of customer resources for FAT, SAT, installation, training, and cutover

EXHIBIT E

Acceptance Process & Change Control

The acceptance process is characterized by running an acceptance test, documenting any anomalies with a plan to fix, signing the acceptance certificate, and putting the project into support mode. Table 9 provides a description of the Final Acceptance process.

Table 9: Final Acceptance Process

Final Acceptance Process	
1	The MCSO and IDEMIA run the previously agreed-to acceptance test procedure using an agreed-upon set of test data. This procedure includes a detailed set of tests covering all the requirements specified in the RDD.
2	Any anomalies are documented in the acceptance punch list. A plan to fix these anomalies by a specific date is entered into the punch list. IDEMIA's standard Severity Definitions are provided in **Error! Reference source not found.** as a reference. The MCSO and IDEMIA reach an agreement regarding which punch list items must be resolved prior to system cutover.
3	System cutover is performed according to the approved Transition Plan. The system going live signifies beneficial use and any applicable support period begins.
4	The system is monitored for one week (or as otherwise agreed to), during which time any newly-discovered issues are added to the punch list. At the end of the week, the MCSO and IDEMIA agree upon the issues that must be resolved in order to gain Final Acceptance. The list is frozen at this time and no new items are added unless Severity 1 issues occur prior to acceptance.
5	Once the agreed-upon punch list issues have been resolved, the acceptance certificate is signed with the following: – A reference to the punch list. – A statement that all invoices up until the time of acceptance will be paid by the MCSO. – A help desk support telephone number.

IDEMIA's Implementation Plan includes a change control / issue resolution process that defines the procedures by which the project scope may be changed, after agreement on system definition and design, during the project implementation or after acceptance. It includes the paperwork, tracking systems, and approvals necessary for authorizing changes.

The Change Order process ensures that the overall effect of the requested change is considered prior to the implementation of the change, and that the effect on the project work plan and schedule is considered. Note that a change request does not necessarily result in a change in price.

Change orders may either happen during initial project implementation or after the system has been up and running for some time, for example if a change in legislation or a need for business process improvements requires workflow change on the IDEMIA Cloud solution. In the later

case, if a cost is associated with the change, the MCSO may opt to fund the change from the accumulated unused capacity available at this time, thus eliminating the need for any extra expense (provided enough unused capacity is available at that time).

Table 10 provides a description of the Change Order process.

Table 10: Change Order Process

Change Order Process	
1	MCSO Change Requests are documented and submitted to the IDEMIA Program Manager.
2	The project team evaluates the proposed change and its impact to the project schedule and costs (if any).
3	The IDEMIA Program Manager drafts a Change Order for your review, including a description of the solution and the price, if any. ***Note:*** No-cost Change Orders may be provided to track changes.
4	IDEMIA and the MCSO review and then formally reject, postpone, or accept changes based on need, overall effect, cost, and schedules.
5	The Change Order is finalized and purchased by being signed by both parties prior to the Change Order's expiration date.
6	After the Change Order has been approved, the IDEMIA Program Manager makes any necessary adjustments to the Design Documents, project work plan, and any other impacted deliverables, such as the BOM.

NOTE: *Product functionality may change or may not be carried forward in newer models. If the MCSO desires that previous functionality be added to their new system, the IDEMIA Program Manager can discuss applicable requirements and provide a Change Order quote.*

EXHIBIT F

Support & Service Level Agreement (SLA)

Cloud MBIS Support

System support for both hardware and software issues includes access to our 24x7 helpdesk via:

- Telephone: 1.800.734.6241
- Email: BiometricsSupport@us.idemia.com

24x7 support coverage for Azure Cloud components (backend hardware and software) is included. Monterey County workstations come with standard 9x5 coverage, unless an issue with the workstation renders the system unusable as defined in Table 1 below (Severity Level 1). Severity Level 1 issues are always dealt with immediately on a 24x7 basis.

Issue Severity Levels, Response Times, & Target Resolution Times

Table 11 defines IDEMIA's Response Times and Target Resolution Times for issue Severity Levels 1-5. Note that response and resolution targets for Severity Level 1 and Severity Level 2 issues assume that Monterey County has contacted the live IDEMIA Help Desk via telephone for issue reporting.

Table 11: IDEMIA Severity Levels of Escalation

Severity Level	Definition	Response Time	Target Resolution Time
1	**Total System Failure**: A total system failure occurs when the System is not functioning and there is no workaround, such as a Central Server is down or the workflow of an entire agency is not functioning.	Telephone conference within 1 hour of initial voice notification	Resolve within 24 hours of initial notification
2	**Critical Failure**: Critical process failure occurs when a crucial element in the System that does not prohibit continuance of basic operations is not functioning, and there is usually no suitable workaround. Note that this may not be applicable to intermittent problems.	Telephone conference within 3 Standard Business Hours of initial voice notification	Resolve within 3 days of initial notification

Severity Level	Definition	Response Time	Target Resolution Time
3	**Non-Critical Failure**: Non-Critical part or component failure occurs when a System component is not functioning, but the System is still useable for its intended purpose, or there is a reasonable workaround.	Telephone conference within 6 Standard Business Hours of initial notification	Resolve within 30 days of initial notification in a Seller-determined Patch or Release.
4	**Inconvenience**: An inconvenience occurs when System causes a minor disruption in the way tasks are performed, but does not stop the system workflows from proceeding.	Telephone conference within 2 Standard Business Days of initial notification	Resolve within 120 days of initial notification in a Seller-determined Patch or Release.
5	**Enhancement**: Customer request for an enhancement to System functionality is the responsibility of Seller's Product Management.	Determined by Seller's Product Management.	If accepted by Seller's Product Management, a release date will be provided with a fee schedule, when applicable.

Support Escalation Process

Table 12 defines IDEMIA's tiered support structure within the automated escalation process.

Table 12: IDEMIA Support Levels of Escalation

Support Level	Responsibility	Goals
Level 1 Support (Help Desk)	Full-time help desk support. Answer support calls, place trouble tickets, work on Severity 3 problems for up to 60 minutes and Severity 4 problems for up to 4 hours, document tickets and escalate to appropriate Level 2 support. Immediately escalate Severity 1 and Severity 2 problems to appropriate Level 2 support.	Resolution of 80% of incoming calls
Level 2 Support	Queue monitoring, network management, workstation monitoring. Place trouble tickets for software-related problems. Take calls from Level 1, IDEMIA, and Level 3 escalation. Assume ownership of call until resolution.	Resolution of 100% of calls at Level 2

Support Level	Responsibility	Goals
Level 3 Support	Must provide immediate support to Level 2 for all Severity 1 issues. Agree to help with all problems unsolved by Level 2 within Service Level Agreement (SLA) resolution period.	No direct problem ownership

Service Response

Table 13 is a matrix for IDEMIA's service escalations by Severity Level, showing how quickly Monterey County can expect system, application, and hardware issues to be addressed, escalated, and resolved.

Table 13: IDEMIA Response Escalations Based On Severity Level

	Severity 1	Severity 2	Severity 3	Severity 4
Help Desk (Level 1) Response	Immediate, plus escalation to: Level 2 Level 3 Program Manager Cloud Team Regional Service Manager	Immediate, plus escalation to: Level 2 Regional Service Manager	Immediate	30 Minutes
Level 2 Response	Immediate	Immediate	60 Minutes	4 Hours
Level 3 Response	Immediate	60 Minutes	12 Hours	N/A
Updates	Every 60 Minutes	Every 4 Hours	Every 5 Days	Every 10 Days
Target Resolution	24 Hours	3 Days	30 Days	120 Days

Most importantly, ANY issue that impacts the availability of the supported system is an IDEMIA-managed issue until resolved, regardless if the issue is due to a network, customer interface, or third-party software problem. Often, downtime is extended if IDEMIA does not lead the resolution of such issues.