

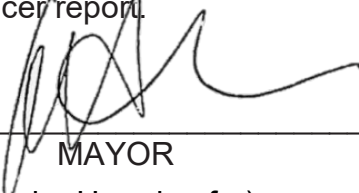
0150-10464-0005

TRANSMITTAL

TO The Council	DATE 05/06/2022	COUNCIL FILE NO. --
FROM The Mayor	COUNCIL DISTRICT Various	

**Proposed agreement with Motorola Solutions, Inc., and
the Los Angeles Police Department for the purchase, installation, and hosting of an
automated license plate recognition system**

The proposed agreement between the Los Angeles Police Department and Motorola Solutions, Inc., is transmitted for further processing. After receipt, the Council has 60 days to act, otherwise the matter will be deemed approved, pursuant to Los Angeles Administrative Code Section 10.5(a). See the attached City Administrative Officer report.



MAYOR
(Andre Herndon for)

MWS:DP: 04220089c

Report From
OFFICE OF THE CITY ADMINISTRATIVE OFFICER
Analysis of Proposed Contract
(\$25,000 or Greater and Longer than Three Months)

To: The Mayor	Date: 05-03-22	C.D. No. Various	CAO File No.: 0150-10464-0005	
Contracting Department/Bureau: Los Angeles Police Department		Contact: James Acheron (213) 486-0112		
Reference: Transmittal from the Board of Police Commissioners to the Office of the Mayor dated February 1, 2022; referred by the Mayor to the City Administrative Officer on March 3, 2022.				
Purpose of Contract: To provide automated license plate recognition services.				
Type of Contract: (X) New contract () Amendment, Contract No.		Contract Term Dates: Five years from the date of execution		
Contract/Amendment Amount: \$2,035,000				
Proposed amount \$ 2,035,000 + Prior award(s) \$ 0 = Total \$ 2,035,000				
Source of funds: Funds are available within the 006010 Office and Administrative Account Fund 100 Dept 70				
Name of Contractor: Motorola Solutions, Inc., a Delaware corporation				
Address: 500 West Monroe Street, Chicago, Illinois 60661				
	Yes	No	N/A	
			Contractor has complied with:	
1. Council has approved the purpose	X		8. Business Inclusion Program	X
2. Appropriated funds are available	X		9. Equal Benefits & First Source Hiring Ordinances	X
3. Charter Section 1022 findings completed	X		10. Contractor Responsibility Ordinance	X
4. Proposals have been requested			11. Disclosure Ordinances	X
5. Risk Management review completed	X		12. Bidder Certification CEC Form 50	X
6. Standard Provisions for City Contracts included	X		13. Prohibited Contributors (Bidders) CEC Form 55	X
7. Workforce that resides in the City: 4.4 %			14. California Iran Contracting Act of 2010	X

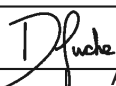
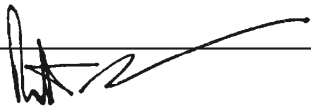
RECOMMENDATION

That the Council, subject to the approval of the Mayor, authorize the Los Angeles Police Department to execute the proposed agreement with Motorola Solutions, Inc., for automated license plate recognition services. The term of the agreement is five years from the date of execution, and a maximum allowable compensation not to exceed \$2,035,000, or \$407,000 annually, subject to the approval of the City Attorney as to form.

SUMMARY

At its meeting of February 1, 2022, the Board of Police Commissioners approved the proposed agreement with Motorola Solutions, Inc., (Contractor) to provide automated license plate recognition (LPR) technology services. The term of the proposed agreement is five years from the date of execution with a maximum allowable compensation not to exceed \$407,000 annually.

The Los Angeles Police Department (Department) has utilized automated license plate recognition technology on approximately 140 police vehicles for nearly a decade. This technology has been effective in reducing recovery times of stolen vehicles and is a valuable tool in criminal investigations. The Information Technology Bureau (ITB) further reports that the recent Separation Incentive Program

		
DP Analyst	04220089	City Administrative Officer

created a staffing void impacting the Department's ability to manage and maintain storage solutions housed with on-site servers maintained by experienced and knowledgeable City employees. The ITB proposes to shift the storage model to a cloud-based service that will be managed and maintained by the Contractor.

Under the terms of the proposed agreement, the Contractor shall provide the equipment, installation, and hosting services for Reaper High Definition Mobile LPR Camera Systems for the replacement of 28 Mobile LPR systems per year through the five-year term of this agreement. The Contractor shall also establish and maintain a formal, documented, mandated, company-wide information security program and have policies and procedures communicated to its respective employees. The Contractor agrees to comply with Federal Bureau of Investigation Criminal Justice Information Systems Security Policy incorporated as Attachment D. The purchase of the replacement systems also includes five years of hosting and warranty services and the integration and continued functionality of the legacy LPR system until full replacement and implementation. The Contractor will assign one certified technician for onsite support services. Funding for the hardware, installation, and hosting is available within the Department's Office and Administrative Account 006010 Fund 100.

The Department proposes to "piggyback" off the agreement between the Contractor and the Los Angeles Harbor Department (Port of LA). The Port of LA currently utilizes a mobile LPR system that consists of intelligent captured devices in two patrol vehicles and a mobile trailer. In October 2019, the Port of LA entered into Contract No. 39910 with Contractor for the expansion and installation of a fixed camera system in 11 locations. Pursuant to Charter Section 371, the Department is not required to enter into a competitive bidding process when utilizing cooperative arrangements with other governmental agencies, referred to as "piggyback".

In accordance with Charter Section 1022, the Personnel Department determined that City employees do not have the expertise to perform the work proposed since these services are only available from a sole source provider. Consistent with the Personnel Department, this Office finds that these services are for the performance of professional, scientific, expert and technical services for which the contracting authority finds that competitive bidding is not practicable or advantageous, as stated in Charter Section 371(e)(2), and would be considered "sole source". A Notice of Intent to Contract was submitted to the Employee Relations Division on February 10, 2022.

The proposed agreement is in compliance with Ordinance 187134, which incorporates the updated Standard Provisions that includes language requiring employees of City contractors and subcontractors to be fully vaccinated against the COVID-19 virus.

In accordance with Los Angeles Code Section 10.5(a), Council approval of the proposed agreement is required because the proposed contract term exceeds three years. To the best of our knowledge, the Contractor has complied with all standard provisions for City contracts, as well as City contracting requirements.

FISCAL IMPACT STATEMENT

Approval of the recommendation stated in this report will authorize the Los Angeles Police Department (Department) to enter into an agreement with Motorola Solutions, Inc., for automated license plate recognition services. The term of the agreement is five years with a maximum allowable compensation not to exceed \$407,000 annually, or \$2,035,000 over the five-year term. Funding for the purchase of

equipment, installation, licensing and hosting services is provided in the Department's 2021-22 Adopted Budget Office and Administrative Account. Funding for subsequent years is subject to approval by the Mayor and Council. There is no additional impact to the General Fund.

FINANCIAL POLICIES STATEMENT

The recommendation stated in this report is in compliance with the City's Financial Policies in that one-time revenues will be used to support one-time expenditures.

MWS:DP:04220089c

Attachment

LOS ANGELES POLICE COMMISSION

**BOARD OF
POLICE COMMISSIONERS**

WILLIAM J. BRIGGS, II
PRESIDENT

EILEEN M. DECKER
VICE PRESIDENT

DALE BONNER
MARIA LOU CALANCHE
STEVE SOBOROFF

MARIA SILVA
COMMISSION EXECUTIVE ASSISTANT II



ERIC GARCETTI
MAYOR

RICHARD M. TEFANK
EXECUTIVE DIRECTOR

MARK P. SMITH
INSPECTOR GENERAL

EXECUTIVE OFFICE
POLICE ADMINISTRATION BUILDING
100 WEST FIRST STREET, SUITE 134
LOS ANGELES, CA 90012-4112

(213) 236-1400 PHONE
(213) 236-1410 FAX
(213) 236-1440 TDD

February 1, 2022

BPC #22-028

The Honorable Eric Garcetti
Mayor, City of Los Angeles
City Hall, Room 303
Los Angeles, CA 90012

Attention: Heleen Ramirez

Dear Honorable Mayor:

RE: APPROVAL OF PROFESSIONAL SERVICES AGREEMENT BETWEEN THE CITY OF
LOS ANGELES AND MOTOROLA SOLUTIONS, INC. FOR AUTOMATED LICENSE
PLATE RECOGNITION SERVICES

At the regular meeting of the Board of Police Commissioners held Tuesday, February 1, 2022 the Board APPROVED the Department's report relative to the above matter.

This matter is being forwarded to you for approval.

Respectfully,

BOARD OF POLICE COMMISSIONERS

MARIA SILVA
Commission Executive Assistant

Attachment

c: Chief of Police

INTRADEPARTMENTAL CORRESPONDENCE

REVIEWED
[Signature] 1/28/22
RICHARD M. TEFANK DATE
EXECUTIVE DIRECTOR

RECEIVED

JAN 28 2022

POLICE COMMISSION

January 28, 2022

3.5

TO: The Honorable Board of Police Commissioners

FROM: Chief of Police

SUBJECT: REQUEST FOR APPROVAL OF PROFESSIONAL SERVICES AGREEMENT BETWEEN THE CITY OF LOS ANGELES AND MOTOROLA SOLUTIONS, INC. FOR AUTOMATED LICENSE PLATE RECOGNITION SERVICES

RECOMMENDED ACTIONS

1. That the Board of Police Commissioners (Board) REVIEW and APPROVE the attached Professional Services Agreement between the City and Motorola Solutions, Inc.
2. That the Board TRANSMIT the attached Professional Services Agreement to the Mayor's Office for review and approval.
3. That the Board AUTHORIZE the Chief of Police to execute the attached Professional Services Agreement upon Mayoral approval.

DISCUSSION

On January 3, 2019, the Los Angeles Harbor Department selected Vigilant Solutions LLC to provide the Los Angeles Port Police with an Automated License Plate Recognition (ALPR) camera system. Subsequently, the Harbor Department entered into Contract No. 39910 with Vigilant Solutions LLC, which was acquired by Motorola Solutions, Inc. (Contractor) on January 7, 2019. The Los Angeles Police Department (LAPD) now desires to take advantage of the Harbor Department's procurement process to purchase an ALPR camera system. The LAPD has utilized ALPR technology throughout the vehicle fleet for approximately a decade. It has proven to be a valuable tool in criminal investigations and in reducing recovery times of lost and stolen vehicles.

The attached Professional Services Agreement will provide the LAPD with an ALPR camera system for a period of five years from the date of contract execution for \$407,000 per year. The Office of the City Attorney has approved the attached Professional Services Agreement as to form.

The Honorable Board of Police Commissioners

Page 2

3.5

Should you have any questions concerning this request, please contact
Police Administrator II Thom Brennan, Commanding Officer, Fiscal Group, at (213) 486-8590.

Respectfully,



MICHEL R. MOORE
Chief of Police

Attachment

BOARD OF
POLICE COMMISSIONERS
Approved *February 1, 2022*
Secretary *María Selva*

INTRADEPARTMENTAL CORRESPONDENCE

January 26, 2022

3.5

TO: Chief of Police

FROM: Commanding Officer, Fiscal Group

SUBJECT: REQUEST FOR APPROVAL OF PROFESSIONAL SERVICES AGREEMENT BETWEEN THE CITY OF LOS ANGELES AND MOTOROLA SOLUTIONS, INC. FOR AUTOMATED LICENSE PLATE RECOGNITION SERVICES

It is requested that the Chief of Police review, approve and transmit to the Board of Police Commissioners the attached Professional Services Agreement (Agreement) between the City and Motorola Solutions, Inc. (Contractor) to provide Automated License Plate Recognition (ALPR) Equipment and Services to the Los Angeles Police Department (LAPD).

On January 3, 2019, the Los Angeles Harbor Department selected Vigilant Solutions LLC to provide the Los Angeles Port Police with an ALPR camera system. Subsequently, the Harbor Department entered into Contract No. 39910 with Vigilant Solutions LLC, which was acquired by Motorola Solutions, Inc. (Contractor) on January 7, 2019. The LAPD now desires to take advantage of the Harbor Department's procurement process to purchase an ALPR camera system. The LAPD has utilized ALPR technology throughout the vehicle fleet for approximately a decade. It has proven to be a valuable tool in criminal investigations and in reducing recovery times of lost and stolen vehicles.

The attached Professional Services Agreement will provide the LAPD with an ALPR camera system for a period of five years from the date of contract execution for \$407,000 per year. The Office of the City Attorney has approved the attached Professional Services Agreement as to form.

Should you have any questions concerning this request, please contact Senior Management Analyst II James T. Acheron, Officer in Charge, Contracts Section, Fiscal Group at (213) 486-0112.


THOM BRENNAN, Police Administrator II
Commanding Officer
Fiscal Group

Attachments

PROFESSIONAL SERVICES AGREEMENT

CONTRACTOR: MOTOROLA SOLUTIONS, INC.

**TITLE: AUTOMATED LICENSE PLATE RECOGNITION SERVICES
(ALPRS)**

CITY CONTRACT No. _____

PROFESSIONAL SERVICES AGREEMENT No. _____
BETWEEN
THE CITY OF LOS ANGELES
AND MOTOROLA SOLUTIONS, INC.

THIS AGREEMENT (“Agreement”) is made and entered into by and between the City of Los Angeles, a municipal corporation (hereinafter referred to as the “City”), acting by and through the Los Angeles Police Department (hereinafter referred to as the “Department” or “LAPD”), and Motorola Solutions, Inc., a Delaware Corporation (hereinafter referred to as the “Contractor”) (each a “Party” and collectively the “Parties”).

RECITALS

WHEREAS, the LAPD has utilized an automated license plate recognition (ALPR) technology throughout its vehicle fleet for approximately a decade; and

WHEREAS, the ALPR has proven to be effective in reducing recovery times of stolen and lost vehicles, is a valuable tool in criminal investigations, and represents an important factor in building efficiencies within field operations; and

WHEREAS, on or about January 3, 2019, Port of Los Angeles (Port) selected Vigilant Solutions, LLC. as a sole source provider (Contract No. 39910) of a fixed ALPR camera system for installation to supplement its existing Vigilant Mobile ALPR system, which has been operational since January 1, 2018; and

WHEREAS, on or about January 7, 2019, Vigilant Solutions, LLC. was acquired by the Contractor; and

WHEREAS, it is in the City’s best interest to take advantage of the Port’s sole source procurement to the extent that it is relevant to properly address the LAPD’s new Department requirements for ALPR technology and enter into an Agreement with the Contractor for the limited services provided in this Agreement; and

WHEREAS, the services by the Contractor are the Contractor’s competency and are of an expert and technical nature; and

WHEREAS, the Contractor provides training on the use of its ALPR system at no additional cost to all law enforcement users, including a course approved by the State of California Commission on Peace Officer Standards and Training, which is only available from the Contractor and is needed by the LAPD to ensure its personnel are properly trained in the use of the ALPR camera system; and

WHEREAS, the City and the Contractor wish to enter into an Agreement pursuant to which the Contractor will perform the work and furnish the deliverables as described herein for consideration and upon the terms and conditions as hereinafter provided.

NOW, THEREFORE, in consideration of the above promises and of the terms, covenants and considerations set forth herein, the parties do agree as follows:

**SECTION 1.0
PARTIES TO THE AGREEMENT AND REPRESENTATIVES**

1.1 Parties to the Agreement

The parties to this Agreement are:

- A. The City of Los Angeles, a municipal corporation, acting by and through the Los Angeles Police Department having its principal office at 100 West First Street, Los Angeles, California 90012.
- B. The Contractor, Motorola Solutions, Inc., a Delaware corporation, having its principal office at 500 W. Monroe Street, Chicago, Illinois, 60661.

1.2 Representatives of the Parties

- A. The representatives of the respective parties who are authorized to administer this Agreement and to whom formal notices, demands and communications shall be given are as follows:

- 1. The City's Representative, unless otherwise stated in the Agreement:

Chief of Police
Los Angeles Police Department
100 West First Street, 10th Floor
Los Angeles, CA 90012

With copies to:

Commanding Officer
Information Technology Bureau
Los Angeles Police Department
100 West First Street, Suite 842
Los Angeles, CA 90012
(213) 486-0370

2. The Contractor's Representative is, unless otherwise stated in the Agreement:

Joe Warner, Senior Account Executive
Motorola Solutions, Inc.
725 South Figueroa Suite 1855
Los Angeles, CA 90017
(312) 204-9300
joseph.warner@motorolasolutions.com

- C. Formal notices, demands and communications to be given hereunder by either Party must be made in writing and may be effected by electronic mail (e-mail), personal delivery or by registered or certified mail, postage prepaid, return receipt requested and will be deemed communicated as of the date of mailing or email transmission.
- D. If the name of the person designated to receive the notices, demands or communications or the address of such person is changed, written notice must be given, in accord with this section, within five (5) working days of said change.

SECTION 2.0 TERM OF AGREEMENT

The term of this Agreement shall commence upon the date that all parties to the Agreement have signed the Agreement and the City Attorney has signed the Agreement as to form (the "Execution Date"). The Agreement shall terminate five years after the Execution Date unless otherwise terminated pursuant to PSC-9, Termination, of the Standard Provisions for City Contracts (Rev. 10/21) [v.4].

Performance will not begin until the Contractor has received approval of insurance and has an approved contract with the City as required herein.

SECTION 3.0 SERVICES TO BE PROVIDED

3.1 Scope of Services

- A. During the term of this Agreement, the Contractor shall provide the services, and deliver the equipment as provided in Attachment B, Scope of Services.
- B. All work, tasks, and deliverables are subject to City approval as provided in Section 4, Total Compensation, Payment, Taxes, and Invoices, of this

Agreement. Failure to receive approval may result in the withholding of compensation for such deliverables pursuant to Section 4 of this Agreement.

- C. The Contractor shall ensure that the Contractor's performance of the work under this Agreement does not interfere unnecessarily with the operation of the LAPD or any other City department.
- D. The Contractor shall be responsible for fixing any errors that occur during the term of the Agreement that result in a loss of, or decrease in, the functionality of the services or equipment.
- E. The Contractor represents and warrants that the equipment provided pursuant to this Agreement will be free of defects in workmanship and materials and shall conform to its specifications.
- F. For the term of this Agreement, the Contractor shall provide no replacement models or equipment, whether pursuant to agreement to replenish or as otherwise articulated in this Agreement, for which the functionality or service levels represent a material degradation of the functionality or service levels currently available to the City for the corresponding equipment or services as of the Execution Date.
- G. Notwithstanding anything in Attachment B, Scope of Services, to the contrary, the warranties that the Contractor provides the City for the equipment and services of this Agreement shall continue and remain in full force and effect for the entire term of this Agreement.

SECTION 4.0 TOTAL COMPENSATION, PAYMENT, TAXES, AND INVOICES

4.1 Total Compensation

The City will pay the Contractor for satisfactory services rendered in a total amount not to exceed Four Hundred Seven Thousand Dollars (\$407,000) per year including taxes, in accordance with Attachment B, Scope of Services.

The Contractor further understands and agrees that execution of this Agreement does not guarantee that any or all of these funds will be expended.

Notwithstanding any other provision of this Agreement, including any exhibit or attachments incorporated therein, and in order for the City to comply with its governing legal requirements, the City shall have no obligation to make any payments to the Contractor unless the City shall have first made an appropriation of funds equal to or in excess of its obligation to make any payments as provided

in said Agreement. The Contractor agrees that services provided by the Contractor, purchases made by the Contractor, or expenses incurred by the Contractor in excess of said appropriation(s) shall be free and without charge to City and the City shall have no obligation to pay for said services, purchases or expenses. The Contractor shall have no obligation to provide any services, provide any equipment or incur any expenses in excess of the appropriated amount(s) until City appropriates additional funds for this Agreement.

4.2 Payment

- A. The City shall pay the Contractor for those services and equipment articulated in Section 3.0 above, according to the Scope of Services, attached to this Agreement as Attachment B, Scope of Services, and incorporated herein by reference.
- B. The granting of any payment by the City, or the receipt thereof by the Contractor, in no way lessens the liability of the Contractor to replace unsatisfactory work, equipment, or materials although the unsatisfactory character of this work, equipment or materials may not have been apparent or detected at the time the payment was made. Materials, equipment, components, or workmanship that do not conform to the requirements of this Agreement may be rejected by the City and upon rejection must be replaced by the Contractor without delay.

4.3 Taxes

To the extent that any of the services or deliverables to be provided by the Contractor hereunder are subject to any California sales and use taxes, the City and the Contractor acknowledge and agree that such taxes shall be collected from the City. The Contractor acknowledges and agrees to remit the same to the appropriate tax collection authorities in the manner set forth under applicable law. The Contractor shall be solely responsible for any uncollected and unremitted taxes due and owing to the appropriate tax collection authorities and shall indemnify the City for any losses in connection with any uncollected and unremitted taxes due.

4.4 Invoices

- A. To ensure that services provided under personal services contracts are measured against services as detailed in the Agreement, the Controller of the City of Los Angeles has developed a policy requiring that specific supporting documentation be submitted with invoices.
- B. The Contractor shall submit invoices that conform to City standards and include, at a minimum, the following information:

1. Name and address of the Contractor
 2. Division and Department name and address where services were provided
 3. Date of invoice and period covered
 4. Agreement number or authority (purchase order) number
 5. Description of completed task and amount due for task, including:
 - i. Name of personnel working on task
 - ii. Hours spent on task and timesheet supporting charges (if applicable)
 - iii. Rate per hour and total due
 6. Certification by a duly authorized officer
 7. Taxes (indicate taxable and non-taxable items on invoice)
 8. Discount and terms (if applicable)
 9. Remittance Address (if different from the Contractor's address)
- C. All invoices must be submitted on the Contractor's letterhead, contain the Contractor's official logo, or other unique and identifying information such as the name and address of the Contractor. Evidence that tasks have been completed, in the form of a report, brochure, or photograph, shall be attached to all invoices. Invoices must be submitted within thirty (30) days of service, or monthly, and will be payable to the Contractor no later than 90 calendar days after acknowledged receipt of a complete invoice; provided however, that the City may withhold any portion of an invoice that it disputes in good faith. In the event an invoice, or portion thereof is in dispute, the City shall notify the Contractor of the potential disapproval action and afford it an opportunity to be heard prior to official disapproval. The City shall pay all undisputed portions of invoices in accordance with this Section. Invoices are considered complete when appropriate documentation or services provided are signed off as satisfactory by the City's Fiscal Officer. Nevertheless, the City will not pay any late charges, penalties, costs, fees, or interest as a result of any late payment by the City. The Contractor shall notify the City within 10 days of the date on which the Contractor has reached 80 percent of the Agreement's not to exceed amount.
- D. Invoices and supporting documentation must be prepared at the sole expense and responsibility of the Contractor. The City shall not compensate the Contractor for costs incurred in invoice preparation. The City may request, in writing, changes to the content and format of the invoice and supporting documentation at any time. The City reserves the right to request additional supporting documentation to substantiate costs at any time.
- E. Tasks that are completed by subcontractors must be supported by subcontractor invoices, copies of pages from reports, brochures,

photographs, or other unique documentation that substantiates their charges.

- F. Failure to adhere to these policies may result in nonpayment or non-approval of demands, pursuant to Charter Section 262(a), which requires the Controller to inspect the quality, quantity, and condition of services, labor, materials, supplies, or equipment received by any City office or department, and to approve demands before they are drawn on the Treasury.
- G. Invoices shall be submitted to:

Commanding Officer
Information Technology Bureau
Los Angeles Police Department
100 West First Street, Room 842
Los Angeles, CA 90012

SECTION 5.0 PERSONNEL

5.1 Key Personnel

- A. Project Manager. The Contractor shall assign a project manager with full authority to administer the Agreement for Contractor.
- B. Staff Size. The size of the staff employed by the Contractor in the performance of the services must be kept consistent with the staff size necessary to perform the services and deliver the equipment anticipated in this Agreement.

5.2 Changes in Key Personnel

The Contractor agrees to minimize changes to its key project personnel. The City shall have the right to request key project personnel changes and to review and approve key project personnel changes proposed by the Contractor. The City's approval of key project personnel assignments and changes shall not be unreasonably withheld.

5.3 Background Checks

To the extent permitted by applicable law, the City may conduct background checks at its expense on the Contractor, its employees, designated replacement employees, agents, and subcontractors who will have, or may have, access to City information and data during performance of this Agreement. The Contractor

recognizes the highly sensitive nature of such information and data and agrees to cooperate with the City and provide, to the extent permitted by applicable law, whatever information the City requires in order to conduct background checks, including verification of education and previous employment.

The City may request changes to Contractor personnel pursuant to Section 5.2 of this Agreement in response to background check information, and the Contractor will accommodate such request for personnel changes. Both parties agree to keep the results of any background checks confidential in accordance with the provisions of Section 11.0, as permitted by applicable law.

SECTION 6.0 SUBCONTRACTORS

6.1 Subcontracts/Joint Participation Agreements

With prior written approval of the Department, the Contractor may enter into subcontracts with other vendors for the performance of portions of this Agreement. The Contractor shall at all times be responsible for the acts and errors or omissions of its subcontractors in the performance of this Agreement. Nothing in this Agreement shall constitute any contractual relationship between any subcontractors and the Department or any obligation on the part of the Department to pay, or to be responsible for the payment of, any sums to any subcontractors.

6.2 Provisions Bind on Subcontracts

The provisions of this Agreement, which by their nature are required to be imposed upon subcontractors, shall apply to all subcontractors in the same manner as to the Contractor. In particular, the LAPD will not pay, even indirectly, the fees and expenses of a subcontractor that do not conform to the terms of this Agreement.

SECTION 7.0 ACCESS TO CITY FACILITIES

- 7.1** The City shall provide the Contractor access to City facilities and personnel during City business hours. The City generally recognizes all State of California and National holidays.
- 7.2** In instances where the Contractor requires access to City facilities and personnel during off-hours, the Contractor shall provide the City with forty-eight (48) hours' notice prior to each requested access. Each such request shall be subject to approval by the City.

SECTION 8.0 SUCCESSORS AND ASSIGNS

All indemnifications and warranties provided by the Contractor pursuant to this Agreement shall be assumed by and binding upon the Contractor's successors and assigns. The provisions of this Section 8.0 shall survive termination of this Agreement.

SECTION 9.0 DISPUTES

Both parties shall undertake to reach an amicable settlement in cases of Dispute. If an amicable settlement cannot be reached, or in the event of default that could result in termination of this Agreement, the City and the Contractor shall schedule a meeting of their representatives in a good faith attempt to resolve the issues in Dispute. The meeting shall allow for a detailed presentation of each party's views on the issues and potential solutions to the Dispute or default. If possible, the meeting should result in an agreed upon course of action to resolve the Dispute or default.

The Contractor and the City shall continue to perform any obligations under this Agreement during any Dispute.

The provisions of Sections 5.169 and 5.170 (Div. 5, Ch. 10, Art. 1) of the Los Angeles Administrative Code and Section 350 of the City Charter shall govern the procedure and rights of the parties with regard to claims arising from this Agreement.

SECTION 10.0 AMENDMENTS

Any change in the terms of this Agreement, including changes in the services to be performed by the Contractor, and any increase or decrease in the amount of compensation which are agreed to by the City and the Contractor shall be incorporated into this Agreement by a written amendment properly executed and signed by the person(s) authorized to bind the parties thereto.

SECTION 11.0 CONFIDENTIALITY AND DISCLOSURE RESTRICTIONS

11.1 Confidentiality and Restrictions on Disclosure

- A. All documents, records, and information provided by the City to the Contractor, or accessed or reviewed by the Contractor, during performance of this Agreement, including but not limited to Criminal Offender Records Information ("CORI") will remain the property of the City.

All documents, records and information provided by the City to the Contractor, or accessed or reviewed by the Contractor during the performance of this Agreement, are confidential (hereinafter collectively referred to as "Confidential Information"). The Contractor agrees not to provide Confidential Information, nor disclose their content or any information contained in them, either orally or in writing, to any other person or entity. The Contractor agrees that all Confidential Information used or reviewed in connection with the Contractor's work for the City will be used only for the purpose of carrying out City business and cannot be used for any other purpose. The Contractor will be responsible for protecting the confidentiality and maintaining the security of City documents and records in its possession.

- B. The Contractor will make the Confidential Information provided by the City to the Contractor, or accessed or reviewed by the Contractor during performance of this Agreement, available to its employees, agents and subcontractors, only on a need to know basis. Further, the Contractor will provide written instructions to all of its employees, agents and subcontractors, with access to the Confidential Information about the penalties for its unauthorized use or disclosure.
- C. The Contractor will store and process Confidential Information in an electronic format in such a way that unauthorized persons cannot retrieve the information by computer, remote terminal or other means
- D. The Contractor must not remove Confidential Information or any other documents or information used or reviewed in connection with the Contractor's work for the City from City facilities without prior approval from the City. The Contractor will not use, other than in direct performance of work required pursuant to the Agreement, or make notes of any home address or home telephone numbers contained in Confidential Information provided by the City that are reviewed during work on this Agreement. The Contractor will, at the conclusion of this Agreement, or at the request of the City, promptly return any and all Confidential Information and all other written materials, notes, documents, or other information obtained by the Contractor during the course of work under this Agreement to the City. The Contractor will not make or retain copies of any such information, materials, or documents.
- E. Any reports, findings, deliverables, analyses, studies, notes, information, or data generated as a result of this Agreement are to be considered confidential. The Contractor will not make such information available to any individual, agency, or organization except as provided for in this Agreement or as required by law.

- F. The Contractor and its employees, agents, and subcontractors may have access to confidential criminal record and Department of Motor Vehicle record information, whose access is controlled by statute. Misuse of such information may adversely affect the subject individual's civil rights and violates the law. The Contractor will implement reasonable and prudent measures to keep secure and private criminal history information accessed by its employees, agents, and subcontractors during the performance of this Agreement. The Contractor will advise its employees, agents, and subcontractors of the confidentiality requirements of Title 42, United States Code, Section 3789(g) [42 U.S.C. 3789(g)], California Penal Code Sections 11075 through 11144, California Penal Code, Sections 13301 through 13305, and California Vehicle Code Section 1808.45.
- G. The Contractor will require that all its employees, agents, and subcontractors who will review, be provided, or have access to Confidential Information, during the performance of this Agreement, execute a confidentiality agreement that incorporates the provisions of this Section, prior to being able to access Confidential Information.
- H. The Contractor shall submit a signed copy of the Confidentiality Agreement, that is attached hereto as Attachment C, and incorporated herein, and require it from each employee and subcontractor.

11.2 Document Control Procedure

The Contractor will develop and administer a mutually acceptable Document Control Procedure over documents flowing to and from the City, in such a manner as to ensure that the confidentiality requirements of this Section 11.0 are met. Each document will be controlled through the use of a Document Control Number.

11.3 Information Sharing

For the avoidance of any doubt, no ALPR data collected by the Contractor for the LAPD pursuant to this Agreement shall be provided by the Contractor to any person or entity outside of the LAPD, except at the prior and express written direction of the Commanding Officer of Information Technology Bureau. Further, and notwithstanding anything in this Agreement to the contrary, the Contractor shall not provide any ALPR data or information, gathered from or for the LAPD as part of performing the services of this Agreement, with the U.S. Immigration and Customs Enforcement agency of the U.S. Department of Homeland Security.

11.4 Provisions Apply to Subcontracts

Any subcontract entered into pursuant to the terms of this Agreement will be subject to, and incorporate, the provisions of this Section 11.0.

11.5 Survival of Provisions

The provisions of this Section 11.0 will survive termination of this Agreement.

SECTION 12.0 DATA SECURITY

12.1 Data Ownership

As between the parties, the City is the sole and exclusive owner of all data and information provided to the Contractor by or on behalf of the City pursuant to this Agreement and any and all updates or modifications thereto or derivatives thereof made by the Contractor ("City Data"), and all intellectual property rights in the foregoing, whether or not provided to any other party under this Agreement. City Data is Confidential Information for the purposes of this Agreement. The Contractor shall not use City Data for any purpose other than that of rendering the services under this Agreement, nor sell, assign, lease, dispose of or otherwise exploit City Data. The Contractor shall not possess or assert any lien or other right against, or to City Data. The City may request an export of City Data stored within the systems or held by the Contractor in any form or format at no charge to the City.

Subject to the restrictions articulated elsewhere in this Agreement, the City grants the Contractor a non-transferable, non-exclusive, terminable at-will license, solely for the term of this Agreement, to use City Data solely for purposes of performing the services pursuant to this Agreement for the City's benefit. The Contractor shall submit a signed copy of Attachment C, Confidentiality Agreement, which is attached hereto and incorporated herein by reference.

12.2 Data Protection

- A. The Contractor shall use best efforts, but in no event less than information security industry standard protections, for the type of data at issue, to prevent unauthorized access to, or use, disclosure, or exposure of City Data. To this end, the Contractor shall safeguard the confidentiality, integrity, and availability of City Data.
- B. The Contractor shall implement and maintain appropriate administrative, technical, and organization security measures to safeguard against unauthorized access, disclosure, or theft of City Data or a candidate's personal information. Such security measures shall be in accordance with recognized industry best practices and the standard of care imposed by state and federal laws and regulations relating to the protection of such

information. In the absence of any legally imposed or industry standard of care, the Contractor shall safeguard City Data using measures no less stringent than the measures the Contractor applies to the Contractor's own personal data and non-public data of similar kind.

- C. Unless otherwise expressly agreed to by the City in writing, the Contractor shall encrypt all City Data at rest, where required given the nature of the data at issue, and in transit and limit access to only those individuals whose access is essential for performance of the services contemplated by this Agreement.
- D. At no time may any content or City processes be copied, disclosed, or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the City.
- E. At any time during the term of this Agreement, at the City's written request, the Contractor shall, and shall instruct all of its employees and subcontractors to, promptly return to the City all copies, whether in written, electronic, or other form of media, of City Data in its possession, or securely dispose of all such copies, and certify in writing to the City that such City Data has been returned to the City or disposed of securely. The Contractor shall comply with all reasonable directions provided by the City with respect to the return or disposal of City Data. Except as set forth in this provision, the Contractor's obligations to retain City Data are governed by Attachment A, Standard Provisions for City Contracts (Rev. 10/21) [v.4]. After the Contractor has retained City Data for the period(s) specified by Attachment A, Standard Provisions for City Contracts (Rev. 10/21) [v.4] ("Retention Period"), the Contractor shall securely dispose of all City Data, and certify in writing to the City, within 30 days of the expiration of Retention Period, that City Data has been securely disposed of.

12.3 Compliance with Privacy Laws

The Contractor shall ensure that the Contractor's performance of the Contractor's obligations under this Agreement complies with all applicable local, state, and federal privacy laws and regulations, including, but not limited to, laws relating to consent to make visual and audio recordings of individuals and consent to collect information from individuals. If this Agreement or any practices which could be, or are, employed in performance of this Agreement are inconsistent with or do not satisfy the requirements of any of these privacy laws and regulations, the City and the Contractor shall in good faith execute an amendment to this Agreement sufficient to comply with these laws and regulations and the Contractor shall complete and deliver any documents necessary to compliance.

12.4 Provision of Data

Upon termination of this Agreement for any cause or reason (including the City's breach), the Contractor shall provide the City with a copy of all City Data in the Contractor's possession in a mutually agreeable machine-readable format.

12.5 Data, Development and Access Point Location

Storage of City Data shall be located in the continental United States of America. The Contractor shall not allow its personnel or contractors to store City Data on portable devices, including personal computers, except for devices that are used and kept only at the Contractor's continental United States of America headquarters or data centers. The Contractor shall neither access, nor allow a third party to access systems housing City Data from any location outside of the continental United States of America. Notwithstanding anything to the contrary in this Agreement, and only after obtaining prior written approval of the City, the Contractor may grant personnel and contractors located outside the continental United States remote read-only access to City Data only as required to provide technical support in relation to the services contemplated herein. The Contractor shall obtain the City's prior written approval for each of its employees, contractors, officers, partners, consultants, principals, agents, affiliates, or subsidiaries who are essential for the purpose of providing the services under this Agreement ("Authorized Persons"). When the Contractor submits a request for the City's prior written approval, it shall describe the proposed Authorized Person's role and the necessity for the proposed Authorized Person to access City Data. The Contractor shall at all times cause such Authorized Persons to abide strictly by the Contractor's obligations under this Agreement and the industry standards for information security. The Contractor hereby agrees that only Authorized Persons who are bound in writing by confidentiality and other obligations sufficient to protect City Data in accordance with the terms and conditions of this Agreement will access City Data, and will do so only for the purpose of enabling the Contractor to perform its obligations under this Agreement.

12.6 Data Breach

The Contractor shall protect City Data using means and technology that is consistent with industry standards for the type of data at issue. The Contractor shall notify the City as soon as reasonably feasible, but in any event, within twenty-four (24) hours in writing and telephonically of the Contractor's discovery or reasonable belief of any unauthorized access of City Data (a "Data Breach"), or of any incident affecting, or potentially affecting City Data related to cyber security (a "Security Incident"), including, but not limited to, denial of service attack, and system outage, instability or degradation due to computer malware or virus. The Contractor shall begin remediation immediately. The Contractor shall provide daily updates, or more frequently if required by the City, regarding

findings and actions performed by the Contractor until the Data Breach or Security Incident has been effectively resolved to the City's satisfaction. The Contractor shall conduct an investigation of the Data Breach or Security Incident and shall share a summary of the investigation with the City. If directed by the City, the Contractor shall retain an independent third party to conduct the investigation at the Contractor's sole cost. The Contractor shall cooperate fully with the City, its agents and law enforcement. The Contractor is responsible for all costs associated with a Data Breach or Security Incident, including, if required by law, the provision of identity theft protection and/or credit monitoring services to individuals affected by the Security Incident. If required by law or directed by the City, the Contractor will be responsible for notifying individuals impacted by the Security Incident or Data Breach, with the City having final approval of the content of the notification. In the event the City incurs any costs related to the breach referenced above, the City will seek reimbursement from the Contractor or reduce the Contractor's invoice for costs associated with breach of security.

- A. Data Breach Liability. If the City is subject to any claims relating to any Data Breach or Security Incident, the Contractor shall fully indemnify and hold harmless the City and defend the City against any such claims, including reimbursement of any costs incurred by the City relating to those claims. This obligation is in addition to any of the Contractor's other indemnification obligations in this Agreement.

12.7 Firewalls and Access Controls

- A. Access Precautions. The Contractor shall use precautions, including, but not limited to, physical software and network security measures, employee screening, training and supervision, and appropriate agreements with employees to:
1. Prevent anyone other than the City, the Contractor, and authorized City or Contractor personnel from monitoring, using, gaining access to, or learning the import of City Data;
 2. Protect appropriate copies of City Data from loss, corruption, or unauthorized alteration; and
 3. Prevent the disclosure of City and Contractor passwords and other access control information to anyone other than authorized City personnel.
- B. Security Best Practices. The Contractor shall implement the following security best practices with respect to any service provided:
1. Least Privilege: The Contractor shall authorize access only to the minimum amount of resources required for a function.

2. Separation of Duties: The Contractor shall divide functions among its staff members to reduce the risk of one person committing fraud undetected.
 3. Role-Based Security: The Contractor shall restrict access to authorized users and base access control on the role a user plays in an organization.
- C. Access Restrictions. The Contractor shall restrict the use of, and access to, administrative credentials for City accounts and the Contractor's systems to only those of the Contractor's employees and other agents whose access is essential for the purpose of providing the services of this Agreement. The Contractor shall require these personnel to log on using an assigned user-name and password when administering City accounts or accessing City Data. These controls must enable the Contractor to promptly revoke or change access in response to terminations or changes in job functions, as applicable. The Contractor shall encrypt all passwords, passphrases, and PINs, using solutions that are certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and keying material are not stored with any associated data. The Contractor will implement any City request to revoke or modify user access within twenty-four (24) hours or the next business day of receipt of City's request. The Contractor will disable user accounts for fifteen (15) minutes upon five (5) consecutive invalid authentication attempts.

12.8 Vulnerability Management and Patching

At least annually, the Contractor shall perform at the Contractor's expense vulnerability tests and risk assessments of all systems that contain City Data. For the Contractor's internet perimeter network, and any of the Contractor's applications that process City Data, such testing must also include (i) penetration tests, including by use of intercept proxies to identify security vulnerabilities that cannot be discovered using automated tools, and (ii) code review or other manual verification. All tests must be performed by the Contractor's compliance team using industry recommended network security tools to identify vulnerability information. Upon written request from the City, the Contractor shall provide to the City a Vulnerability Testing & Risk Assessment Report at the organization level including an executive summary of the results.

12.9 Right of Audit by the City

Without limiting any other audit rights of the City, upon reasonable advance notice of at least thirty (30) days, and no more than once per calendar year, the City may review the Contractor's data privacy and data security program prior to

the commencement of this Agreement and from time to time during the term of this Agreement. During the performance of this Agreement, upon reasonable advance notice of at least thirty (30) days, and no more than once per calendar year, the City, may, by itself or by retaining a certified public accounting firm or information security professional, perform, or have performed, an on-site audit of the Contractor's data privacy and information security program. In lieu of an on-site audit, at the City's discretion and upon request by the City, the Contractor agrees to complete, within fourteen (14) days of receipt, an audit questionnaire provided by the City regarding the Contractor's data privacy and information security program. These audit rights are in addition to any other audit rights set forth Attachment A, Standard Provisions for City Contracts (Rev. 10/21) [v.4].

12.10 Written Information Security Policy

The Contractor shall establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards, and procedures (collectively "Information Security Policy"), and communicate the Information Security Policy to all of its respective employees and contractors in a relevant, accessible, and understandable form. The Contractor shall regularly review and evaluate the Information Security Policy to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks. Upon execution of this Agreement and thereafter within three (3) business days of the City's request, the Contractor shall make available for the City's review the Contractor's Information Security Policy and any related SOC audits, information security certifications, or other evidence that the Contractor has in place appropriate policies and procedures regarding information protection and security.

12.11 Change in Service

The Contractor shall notify the City of any changes, enhancement, and upgrades to the Contractor's systems, or changes in other related software services, as applicable, which could impact the security of the services.

12.12 Third Party Software

In the event the Contractor provides any third-party software (the "Third-Party Software"), including Open Source Software, to the City in connection with this Agreement for which the City would be obligated to accept and be bound by any third-party terms and conditions, the following shall apply: (1) the Contractor shall specifically identify in writing all Third-Party Software; (2) the Contractor shall provide written copies of all third-party license agreements applicable to the City; and (3) the Contractor warrants that (i) it has the right to license any Third-Party Software licensed to the City under this Agreement; (ii) to the best of the Contractor's knowledge, the Third-Party Software does not, and the use of the Third-Party Software by the City as contemplated by this Agreement will not,

infringe any intellectual property rights of any third party; and (iii) unless specifically provided otherwise herein, the City shall have no obligation to pay any third party any fees, royalties, or other payments for the City's use of any Third-Party Software in accordance with the terms of this Agreement. With regard to (i) Open Source Software, (ii) any Third-Party Software that the Contractor fails to identify in writing, and (iii) any third-party software embedded in the Licensed Software for which the City is not required to accept any third-party terms and conditions, all such software shall be considered, as appropriate, part of and included in the definition of "Licensed Software" and subject to all warranties, indemnities, and other requirements of this Agreement, including scope of license and maintenance and support, relating to the Licensed Software. To the extent permitted by law or contract, the Contractor shall pass through to the City the warranties for the Third-Party Software. For purposes of this provision, "Open Source Software" means any software, programming, or other intellectual property that is subject to (i) the GNU General Public License, GNU Library General Public License, Artistic License, BSD license, Mozilla Public License, or any similar license, including, but not limited to, those licenses listed at www.opensource.org/licenses or (ii) any agreement with terms requiring any intellectual property owned or licensed by the City to be (a) disclosed or distributed in source code or object code form; (b) licensed for the purpose of making derivative works; or (c) redistributable.

12.13 Criminal Justice Information Systems

The Contractor agrees to and shall comply with the Federal Bureau of Investigation Criminal Justice Information Systems Security Policy (the "Security Policy"), as amended from time to time, which document is incorporated into and made a part of this Agreement by reference. The Contractor shall ensure that the Contractor's security, technical, personnel, and administrative practices, meet no less than those standards articulated in the Security Policy.

12.14 Security Addendum

The Contractor agrees to and shall comply with Attachment D, The Federal Bureau of Investigation Criminal Justice Information Systems Security Addendum, which document is incorporated into and made a part of this Agreement by reference.

12.15 Provisions Apply to Subcontracts

Any subcontract entered into pursuant to the terms of this Agreement will be subject to, and incorporate, the provisions of this Section 12.0.

12.16 Survival of Provisions

The provisions of this Section 12.0 will survive termination of this Agreement.

SECTION 13.0 MISCELLANEOUS

13.1 Standard Provisions

The Contractor must comply with the requirements of the Standard Provisions for City Contracts (Rev. 10/21) [v.4], attached hereto as Attachment A and incorporated herein by reference, with the exception of PSC-22, Data Breach, the subject matter of which is otherwise addressed in this Agreement.

13.2 Disclosure of Border Wall Contracting

The Contractor shall comply with Los Angeles Administrative Code ("LAAC") Section 10.50 et seq., "Disclosure of Border Wall Contracting." The City may terminate this Contract at any time if the City determines that the Contractor failed to fully and accurately complete the required affidavit and disclose all Border Wall Bids and Border Wall Contracts, as defined in LAAC Section 10.50.1. The required affidavit must be submitted online at www.labavn.org.

13.3 Severability/Ambiguity

In the event a court of competent jurisdiction holds any provision of this Agreement to be invalid, such holding shall have no effect on the remaining provisions of this Agreement, and they shall continue in full force and effect. No ambiguity in this Agreement may be interpreted against any one party by virtue of that party being drafter of the Agreement. The parties acknowledge that they have read and understood this Agreement and had the opportunity to consult with counsel of their choosing regarding this Agreement.

13.4 Use of Marks

Except as expressly provided in this Agreement, the Contractor shall not use the City or LAPD's names, logos, seals, insignia or other words, names, symbols or devices that identify the City or LAPD, for any purpose except with the prior written consent of, and in accordance with restrictions required by the City.

13.5 Media, Publicity, and Case Studies

The Contractor shall refer all inquiries from the news media to LAPD, shall immediately contact LAPD to inform the City of the inquiry, and shall comply with the procedures of LAPD's Public Affairs staff regarding statements to the media relating to this Agreement or the Contractor's services under this Agreement. The Contractor shall not use the City as a reference or case study absent receipt of the City's prior written approval. The Contractor shall further provide the City with the opportunity to review and approve any such reference or case study prior to publication, which approval the City shall not unreasonably withhold.

13.6 No Third-Party Beneficiaries

Nothing herein is intended to create a third-party beneficiary in any subcontractor. The City has no obligation to any subcontractor. No privity is created with any subcontractor by this Agreement. Even if the Contractor uses subcontractors, the Contractor remains responsible for complete and satisfactory performance of the terms of this Agreement.

13.7 Non-Exclusive Agreement

The City and the Contractor understand and agree that this is a non-exclusive Agreement to provide services to the City and the LAPD and that the City and the LAPD reserve the right to enter into one or more agreements with other contractors to provide similar services during the term of this Agreement.

SECTION 14.0 ENTIRE AGREEMENT

14.1 Complete Agreement

This Agreement contains the full and complete Agreement between the parties. No verbal agreement or conversation with any officer or employee of either party shall affect or modify any of the terms and conditions of this Agreement. No-shrink-wrap, click-wrap, privacy policy, or other terms and conditions or agreements ("Additional Contractor Software Terms") provided with any products, services, documentation, or software hereunder shall be binding on the City, even if use of the foregoing requires an affirmative "acceptance" of those Additional Contractor Software Terms before access is permitted. All such Additional Contractor Software Terms shall be of no force or effect and shall be deemed rejected by the City in their entirety.

14.2 Counterparts/Electronic Signature

This Agreement may be executed in one or more counterparts, and by the parties in separate counterparts, each of which when executed shall be deemed to be an original but all of which taken together shall constitute one and the same agreement. The parties further agree that facsimile signatures or signatures scanned into .pdf (or signatures in another electronic format designated by the City) and sent by e-mail shall be deemed original signatures.

14.3 Number of Originals and Attachments

This Agreement includes twenty-two (22) pages and five (5) attachments. Attachments A-E listed below are incorporated herein by this reference:

Attachment A – Standard Provisions for City Contracts (Rev. 10/21) [v.4]
Attachment B – Scope of Services
Attachment C – Confidentiality Agreement
Attachment D – The Federal Bureau of Investigation Criminal Justice Information
Systems Security Addendum
Attachment E – Enterprise Service Agreement

14.4 Order of Precedence

In the event of any inconsistency between the terms, attachments, specifications or provisions which constitute this Agreement, the following order of precedence shall apply in the order listed herein:

1. This Agreement between the City of Los Angeles and Motorola Solutions, Inc.
2. Attachment A, Standard Provisions for City Contracts (Rev. 10/21) [v.4]
3. Attachment B, Scope of Services
4. Attachment C, Confidentiality Agreement
5. Attachment D, The Federal Bureau of Investigation Criminal Justice Information Systems Security Addendum
6. Attachment E, Enterprise Service Agreement

[Signature Page Follows]

[Remainder of the Page Intentionally Left Blank]

IN WITNESS THEREOF, the parties hereto have caused this Agreement to be executed by their respective duly authorized representatives.

THE CITY OF LOS ANGELES

MOTOROLA SOLUTIONS, INC.

By: _____
MICHEL R. MOORE
Chief of Police

By: Jerry Burch
JERRY BURCH
Vice President

Date: _____

Date: 1/25/2022

APPROVED AS TO FORM:

MICHAEL N. FEUER, City Attorney

(2nd Corporate Officer)

By: _____
SAMUEL PETTY
Deputy City Attorney

By: Elizabeth Heintzman
ELIZABETH HEINTZMAN
Director of Sales

Date: _____

Date: 1/25/2022

ATTEST:

HOLLY L. WOLCOTT, City Clerk

By: _____
Deputy City Clerk

Date: _____

City Business License Number: 0000749148-0001-7

Internal Revenue Service Taxpayer Identification Number: 36-1115800

City Contract Number: _____

ATTACHMENT A

STANDARD PROVISIONS FOR CITY CONTRACTS (Rev. 10/21) [v.4]

Required Insurance and Minimum Limits

Name: MOTOROLA SOLUTIONS, INC.

Date: 12/3/2021

Agreement/Reference: AUTOMATED LICENSE PLATE RECOGNITION SERVICES

Evidence of coverages checked below, with the specified minimum limits, must be submitted and approved prior to occupancy/start of operations. Amounts shown are Combined Single Limits ("CSLs"). For Automobile Liability, split limits may be substituted for a CSL if the total per occurrence equals or exceeds the CSL amount.

Limits

Workers' Compensation (WC) and Employer's Liability (EL)

WC Statutory
EL 1,000,000

Waiver of Subrogation in favor of City

Longshore & Harbor Workers

Jones Act

General Liability City of Los Angeles must be named as an additional insured party

1,000,000

Products/Completed Operations

Sexual Misconduct

Fire Legal Liability

Automobile Liability (for any and all vehicles used for this contract, other than commuting to/from work)

1,000,000

Professional Liability (Errors and Omissions)

Discovery Period _____

Property Insurance (to cover replacement cost of building - as determined by insurance company)

All Risk Coverage

Boiler and Machinery

Flood

Builder's Risk

Earthquake

Surety Bonds - Performance and Payment (Labor and Materials) Bonds

Crime Insurance

Other: Provided to: Nicholas Webster, Serial No. N6652 (213) 486-0395

If a contractor has no employees and decides to not cover herself/himself for workers' compensation, please complete the form entitled "Request for Waiver of Workers' Compensation Insurance Requirement" located at: <http://cao.lacity.org/risk/InsuranceForms.htm>

In the absence of imposed auto liability requirements, all contractors using vehicles during the course of their contract must adhere to the financial responsibility laws of the State of California.

ATTACHMENT B

SCOPE OF SERVICES



MOTOROLA SOLUTIONS

Quote for:

Los Angeles Police Department

Attn:

Jens Back

Reference:

Annual Offer

Quote By:

Tony Gonzalez

Date:

11-04-21

Motorola Solutions is about protecting officers, families and communities. Motorola is about saving lives – creating innovative and essential intelligence solutions for law enforcement that enhance policing efforts.

Intelligence can solve crimes, prevent crime before they occur, and improve safety for officers and the public that they serve and protect. Motorola's solutions are designed to collect, organize and share data to credentialed law enforcement personnel, making intelligence actionable and readily accessible.

WHAT WE DO:



**REDUCE
CRIME RATES**



**OFFICER
SAFETY**




**INCREASE
EFFICIENCY &
PRODUCTIVITY**



**REVENUE
DISCOVERY/
RECOVERY**

OUR PRODUCTS:

- License Plate Recognition (LPR) Data and Analytics
- Fixed and Mobile LPR Cameras
- Ballistics Analysis
- Crime Mapping and Analytics
- Campus Safety Solutions
- Parking Enforcement Solutions
- Corporate Security Solutions

		Motorola Solutions, LLC 1152 Stealth Street Livermore, California 94551 (P) 925-398-2079 (F) 925-398-2113	
Issued To:	Los Angeles Police Department - Attention: Jens Back	Date:	01-22-21
Project Name:	Annual Offer	Quote ID:	GSM-1316-04

PROJECT QUOTATION

We at Motorola Solutions, LLC are pleased to quote the following systems for the above referenced project:

Mobile Units

5 Years of Hosting and Warranty Included

Qty	Item #	Description
(28)	Mobile LPR SYS-1 CDM-2-34--RHD	Mobile LPR 2-Camera Reaper High-Definition System (Expandable to 4 Cams) <u>Hardware:</u> <ul style="list-style-type: none"> • Qty=1 12mm lens package • Qty=1 16mm lens package • VLP-5200 Processing Unit • Wiring harness w/ ignition control (Direct to Battery) <ul style="list-style-type: none"> ◦ Single point power connection • Field installed GPS antenna <u>Software:</u> <ul style="list-style-type: none"> • CarDetector Mobile LPR software application for MDC unit <ul style="list-style-type: none"> ◦ LPR vehicle license plate scanning / real time alerting ◦ Full suite of LPR tools including video tool set
(28)	VS-LBB-02-E	LPR Camera Mounting Brackets - Light Bar Mounting Style - Complete Set <ul style="list-style-type: none"> • LPR Camera Mounting Bracket - Rooftop under light bar • Compatible with most Whelen, Code3, TOMAR, Federal Signal, Arjent S2 Light Bars • Mounts up to four (4) LPR cameras
(28)	Installation	Installation of 2-Camera Mobile System
(5)	VSBSCSVC-04	Vigilant LPR Basic Service Package for Hosted/Managed LPR Deployments <ul style="list-style-type: none"> • Managed/hosted server account services by Vigilant <ul style="list-style-type: none"> ◦ Includes access to all LEARN or Client Portal and CarDetector software updates • Priced per camera per year for over 60 total camera units • Requires new/existing Enterprise Service Agreement (ESA)
(5)	VSPK1SVC-04	Vigilant LPR Standard Service Package for Hosted/Managed LPR Deployments <ul style="list-style-type: none"> • Optional Service Package Benefits <ul style="list-style-type: none"> ◦ Extended access to Vigilant 'Private Data' via CarDetector Mobile Hit Hunter ◦ Unlimited access to Vigilant's Mobile Companion LPR application for Smartphones • Priced per camera per year for over 60 total camera units

		<ul style="list-style-type: none"> o Requires Basic Service Package
(28)	CDMS24HWW	2-Camera Mobile LPR System - Extended Hardware Warranty - Years 2 through 5 <ul style="list-style-type: none"> • Full mobile LPR hardware component replacement warranty • Applies to 2-Camera hardware system kit • Valid for 4 years from standard warranty expiration
(28)	SSU-SYS-COM	Vigilant System Start Up & Commissioning of 'In Field' LPR system <ul style="list-style-type: none"> • Vigilant technician to visit customer site • Includes system start up, configuration and commissioning of LPR system • Applies to mobile (1 System) and fixed (1 Camera) LPR systems
(28)	VS-SHP-01	Vigilant Shipping Charges <ul style="list-style-type: none"> • Applies to each Mobile LPR System • Shipping Method is FOB Shipping
(1)	VS-TRVL-01	Vigilant Travel via Client Site Visit <ul style="list-style-type: none"> • Vigilant certified technician to visit client site • Includes all travel costs for onsite support services
Subtotal Price (Excluding sales tax)		\$365,777.00

Commercial Data

One Year

Qty	Item #	Description
(1)	VS-IDP-08	Investigative Data Platform - Annual Subscription for up to 10,000 Sworn - State and Local <ul style="list-style-type: none"> • Commercial LPR Data access - For up to 10,000 Sworn <ul style="list-style-type: none"> o Access to all Vigilant commercially acquired national vehicle location data o Unlimited use by authorized agency personnel to complete suite of LEARN data analytics o Includes full use of hosted/managed LPR server account via LEARN
Subtotal Price (Excluding sales tax)		\$25,130.00

Intergration/Migration of Existing Units

Qty	Item #	Description
(140)	VS-CIP-M	Competitive System Historical Data Migration - One-Time Fee <ul style="list-style-type: none"> • Engineering service to migrate historical data to LEARN account <ul style="list-style-type: none"> o NO disruption of existing LPR operations • Priced per camera
(1)	VS-CIP-I	Vigilant Competitive LPR Integration Service

		<ul style="list-style-type: none"> Includes software module for installation on competitive LPR server or system Near-real-time monitoring and copying of new LPR data to LEARN account Engineering services included for remote analysis of existing Non-Vigilant LPR data
(140)	VS-CIP-S-04	Competitive System Annual Licensing Fee - 60 or More Cameras <ul style="list-style-type: none"> Hosted/managed LEARN LPR server account <ul style="list-style-type: none"> Access to all competitive LPR data (From Non-Vigilant Server/Camera Integration) Includes all LEARN SW updates w/ database optimization/maintenance Priced per Non-Vigilant camera on an annual basis
Subtotal Price (Excluding sales tax)		\$0.00

Qty	Item #	Description
(1)	Tax	Tax on Hardware at 9.5%
Subtotal Price		\$16,093.00

Quote Notes:

- All prices are quoted in USD and **will** remain firm and in effect for 60 days.
- Returns or exchanges will incur a 15% restocking fee.
- Orders requiring immediate shipment may be subject to a 15% QuickShip fee.
- No permits, start-up, installation, and or service included in this proposal unless explicitly stated above.
- This Quote does not include anything outside the above stated bill of materials.
- Quote includes 5 years of hosting and warranty for Vigilant equipment included on this quote.
- One year of commercial data is included for each annual renewal under this five year proposal.
- Vigilant will host all existing 140 PIPs unit until they are no longer in service so long as annual commitment is kept.
- Any additional units outside of the existing original 140 PIPs units can be added at a cost of \$1,500 per year.
- This quote contains annual pricing under a five year proposal and is intended to be acted upon on an annual basis.
- LAPD will receive the equipment and services listed above once a year for five years with each annual renewal.
- LAPD will receive the latest most current model of the Mobile LPR 2-Camera High-Definition System available.

Quoted by: Tony Gonzalez - tony.gonzalez@motorolasolutions.com

Annual Price	\$407,000.00
---------------------	---------------------

Total Cost for 5 Years	\$2,035,000.00
-------------------------------	-----------------------

ATTACHMENT C

CONFIDENTIALITY AGREEMENT

Los Angeles Police Department

Confidentiality Agreement

I, _____, or the entity for which I am an employee, independent contractor, or subcontractor (hereinafter referred to as "Contractor"), have entered into a contract (hereinafter referred to as the "Agreement") with the City of Los Angeles to provide various services to the City of Los Angeles (hereinafter referred to as "City").

I will provide temporary services to City and as part of these services I will have access to confidential information. "Confidential Information" includes all data, records, documents, audio or visual recordings, materials, products, technology, computer programs, specifications, manuals, business plans, software, marketing plans, financial information, and other information disclosed or submitted, orally, in writing, or by any other media, to me by City pursuant to the Agreement or this Confidentiality Agreement, regardless of whether the information is marked or otherwise identified in writing as confidential, and regardless of whether the Confidential Information is received prior to execution of this Confidentiality Agreement.

I further understand that all Confidential Information provided to me by City, or accessed or reviewed by me during the performance of this assignment will remain the property of City.

I agree to use Confidential Information solely in connection with providing services to City under the Agreement and for no other purpose.

I agree not to provide Confidential Information, nor disclose its content or any information contained in it, either orally or in writing or in any form to transmit information, to any other person or entity, unless required by law or court order. I further agree not to make copies of any Confidential Information unless a formal request is made and approved by City.

I agree to promptly notify City of all requests, notices, subpoenas, pleadings, or other means, for the release of Confidential Information received by me.

I agree that I will not divulge to any unauthorized person, Confidential Information or any other information obtained while performing work pursuant to the Agreement between me and City.

I will be responsible for protecting the confidentiality and maintaining the security of all Confidential Information in my possession. I agree to use the same standard of care to protect City's Confidential Information as I use to protect my

own confidential and proprietary information, but not less than a reasonable standard.

Upon request by City, or completion or termination of my assignment under the Agreement, I will promptly return or destroy all Confidential Information in my possession at City's discretion, and provide City with written certification stating that such Confidential Information has been returned or destroyed.

This Confidentiality Agreement is to apply in conjunction with any prior confidentiality agreement between myself and City, and will not nullify such agreements; however, this Confidentiality Agreement will take precedence. Any conflicts with any other agreements will be modified to comply with the terms and intent of this Confidentiality Agreement.

I acknowledge that violation of this Confidentiality Agreement may subject me to civil and/or criminal action and that City will seek all possible legal redress.

Name of Signatory Contractor Signature

Signatory Title Date

Contractor Address:

Agreement Number _____

ATTACHMENT D

**THE FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION
SYSTEMS SECURITY ADDENDUM**

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

ATTACHMENT E

ENTERPRISE SERVICE AGREEMENT

Enterprise Service Agreement (ESA)

This Motorola Solutions, Inc. Enterprise Service Agreement (the "Agreement") is made and entered into as of the effective date of the Professional Services Agreement between the City of Los Angeles and Motorola Solutions, Inc., by and between **Motorola Solutions, Inc.**, a Delaware corporation, having its principal place of business at 500 West Monroe St., Chicago IL 60661 ("MSI") and the Los Angeles Police Department, a law enforcement agency (LEA) or other governmental agency ("Affiliate").

WHEREAS, MSI designs, develops, licenses and services advanced video analysis software technologies for the law enforcement and security markets;

WHEREAS, MSI provides access to license plate data as a value-added component of the MSI law enforcement package of license plate recognition equipment and software, stores and disseminates to law enforcement agencies publicly and commercially gathered license plate recognition (LPR) data ("Commercial LPR Data") as a valued added component of the MSI law enforcement package of software, and provides integration services to integrate Affiliate's LPR data into the LEARN server;

WHEREAS, Affiliate will separately purchase License Plate Recognition (LPR) hardware components from MSI and/or its authorized reseller for use with the Software Products (as defined below);

WHEREAS, Affiliate desires to license from and receive service for the Software Products provided by MSI, to access Commercial LPR Data, and to integrate Affiliate's LPR data collected from third-party LPR cameras, into the LEARN server;

THEREFORE, In consideration of the mutual covenants contained herein this Agreement, Affiliate and MSI hereby agree as follows:

I. Definitions:

"CJIS Security Policy" means the FBI CJIS Security Policy document as published by the FBI CJIS Information Security Officer.

"CLK" or "Camera License Key" means an electronic key that will permit each license of MSI's CarDetector brand LPR software (one CLK per camera) to be used with other MSI approved and licensed LPR hardware components (i.e., cameras and other hardware components provided by MSI or provided by a MSI certified reselling partner that has authority from MSI to deliver such MSI-authorized components) and Software Products. CLKs shall be not issuable and if issued in error shall be removed and immediately rendered null and void for cameras and other hardware components that are not MSI-authorized cameras and other hardware components or are delivered to Affiliate by another vendor that is not a MSI certified reselling partner.

"

"Commercial LPR Data" refers to LPR data collected by private sources and available on LEARN with a paid subscription.

“Confidential Information” Refers to any and all (i) rights of MSI associated with works of authorship, including exclusive exploitation rights, copyrights, moral rights and mask works, trademark and trade name rights and similar rights, trade secrets rights, patents, designs, algorithms and other industrial property rights, other intellectual and industrial property and proprietary rights of every kind and nature, whether arising by operation of law, by contract or license, or otherwise; and all registrations, applications, renewals, extensions, combinations, divisions or reissues of the foregoing; (ii) product specifications, data, know-how, formulae, compositions, processes, designs, sketches, photographs, graphs, drawings, samples, inventions and ideas, and past, current and planned research and development; (iii) current and planned manufacturing and distribution methods and processes, customer lists, current and anticipated customer requirements, price lists, market studies, and business plans; (iv) computer software and programs (including object code and source code), database technologies, systems, structures, architectures, processes, improvements, devices, discoveries, concepts, methods, and information of MSI; (v) any other information, however documented, of MSI that is a trade secret within the meaning of applicable state trade secret law or under other applicable law, including but not limited to the Software Service, and the Commercial LPR Data; (vi) information concerning the business and affairs of MSI (which includes historical financial statements, financial projections and budgets, historical and projected sales, capital spending budgets and plans, the names and backgrounds of key personnel, contractors, agents, suppliers and potential suppliers, personnel training techniques and materials, and purchasing methods and techniques, however documented; and (vii) notes, analysis, compilations, studies, summaries and other material prepared by or for MSI containing or based, in whole or in part, upon any information included in the foregoing.

“Criminal Justice Information Services Division” or “CJIS” means the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

“Effective Date” means sixty (60) days subsequent to the date set forth in the first paragraph of this Agreement.

“Enterprise License” means a non-exclusive, non-transferable, revocable license to install and operate the Software Products, on applicable media provided by MSI or MSI’s certified reselling partners. This Enterprise Service Agreement allows Affiliate to install the Software Products on such devices, in accordance with the selected Service Package(s), and allow benefits of all rights granted hereunder this Agreement.

“LEA” refers to a Law Enforcement Agency.

“LEA LPR Data” refers to LPR data collected by LEAs and available on LEARN for use by other LEAs. LEA LPR Data is freely available to LEAs at no cost and is governed by the contributing LEA’s retention policy.

“License Plate Recognition (“LPR”)” refers to the process of utilizing cameras, either stationary or mounted on moving vehicles, to capture and interpret images of vehicle license plates.

“LPR Data” refers to both LEA LPR Data and Commercial LPR Data.

“LEARN” refers to Law Enforcement Archival and Reporting Network, which is a web based (hosted) suite of software applications consisting of analytical and investigative software located on a physical database server that also hosts LPR Data.

“Service Fee” means the amount due from Affiliate prior to the renewal of this Agreement as consideration for the continued use of the Software Products and Service Package benefits according to Section VIII of this Agreement.

“Service Package” means the Affiliate designated service option(s) which defines the extent of use of the Software Products, in conjunction with any service and/or benefits therein granted as rights hereunder this Agreement.

“Service Period” has the meaning set forth in Section III (A) of this Agreement.

“Software Products” means MSI’s Law Enforcement & Security suite of Software Products including CarDetector, Law Enforcement Archival & Reporting Network (LEARN), PlateSearch, Mobile Companion for Smartphones, Target Alert Service (TAS) server/client alerting package, and other software applications considered by MSI to be applicable for the benefit of law enforcement and security practices. Software Products shall only be permitted to function on approved MSI cameras and other hardware components provided by MSI or through MSI certified reselling partners. Software Products shall not be permitted to operate on third-party provided or not MSI-authorized hardware components, and if found to be operating on third-party provided hardware components Software Products shall be promptly removed by Affiliate.

“Technical Support Agents” means Affiliate’s staff person specified in the Contact Information Worksheet of this Agreement responsible for administering the Software Products and acting as Affiliate’s Software Products support contact.

“User License” means a non-exclusive, non-transferable license to install and operate the Software Products, on applicable media, limited to a single licensee.

“Users” refers to individuals who are agents and/or sworn officers of the Affiliate and who are authorized by the Affiliate to access LEARN on behalf of Affiliate through login credentials provided by Affiliate.

II. Enterprise License Grant; Duplication and Distribution Rights:

- (a) **License Grant.** Subject to the terms and conditions of this Agreement, MSI hereby grants Affiliate (1) an Enterprise License to the Software Products for the Term provided in Section III below, (2) a non-exclusive, non-transferable, revocable right and license to access MSI’s Commercial LPR Data. Except as expressly permitted by this Agreement, Affiliate or any third party acting on behalf of Affiliate shall not copy, modify, distribute, loan, lease, resell, sublicense or otherwise transfer any right in the Software Products. Except as expressly permitted by this Agreement, no other rights are granted by implication, estoppels or otherwise. Affiliate shall not eliminate, bypass, or in any way alter the copyright screen (also known as the “splash” screen) that may appear when Software Products are first started on any computer. Any use or redistribution of Software Products in a manner not explicitly stated in this Agreement, or not agreed to in writing by MSI, is strictly prohibited.

- (b) **Restrictions on Use of Software Product.** Except as expressly permitted under this Agreement, Agency agrees that it shall not, nor will it permit a User or any other party to, without the prior written consent of MSI, (i) copy, duplicate or grant permission to the Software Products or any part thereof, or the Commercial LPR Data; (ii) create, attempt to create, or grant permission to the source program and/or object program associated with the Software Product; (iii) decompile, disassemble or reverse engineer any software component of the Software Product for any reason, including, without limitation, to develop functionally similar computer software or services; or (iv) modify, alter or delete any of the copyright notices embedded in or affixed to the copies of any components of the Software Product. Agency shall instruct each User to comply with the preceding restrictions.
- (c) **Third Party Software and Data.** If and to the extent that MSI incorporates the software and/or data of any third party into the Software Product, including but not limited to the LEA LPR Data, and use of such third party software and/or data is not subject to the terms of a license agreement directly between Agency and the third party licensor, the license of Agency to such third party software and/or data shall be defined and limited by the license granted to MSI by such third party and the license to the Software Product granted by MSI under this Agreement. Agency specifically acknowledges that the licensors of such third party software and/or data shall retain all ownership rights thereto, and Agency agrees that it shall not (i) decompile, disassemble or reverse engineer such third party software or otherwise use such third party software for any reason except as expressly permitted herein; (ii) reproduce the data therein for purposes other than those specifically permitted under this Agreement; or (iii) modify, alter or delete any of the copyright notices embedded in or affixed to such third party software. Agency shall instruct each User to comply with the preceding restrictions.
- (d) **Non-Exclusive Licensed Access.** Agency acknowledges that the right or ability of MSI to license other third parties to use the Software Product is not restricted in any manner by this Agreement, and that it is MSI's intention to license a number of other LEAs to use the Software Product. MSI shall have no liability to Agency for any such action.

III. Term; Termination.

A. **Term.** The initial term of this Agreement is for five (5) years beginning on the Effective Date, unless earlier terminated as provided herein. Sixty (60) days prior to the expiration of the first year's Service Period and each subsequent Service Period, MSI will provide Affiliate with an invoice for the Service Fee due for the subsequent twelve (12) month period (each such period, a "Service Period"). This Agreement and the Enterprise License granted under this Agreement will be extended for a Service Period upon Affiliate's payment of that Service Period's Service Fee, which is due 30 days prior to the expiration of the Initial Term or the existing Service Period, as the case may be. Pursuant to Section XIII below, Affiliate may also pay in advance for more than one Service Period.

B. **Affiliate Termination.** Affiliate may terminate this Agreement at any time by notifying MSI of the termination in writing thirty (30) days prior to the termination date and deleting all copies of the Software Products. If Affiliate terminates this Agreement prior to the end of the Initial Term, MSI will not refund or prorate any license fees, nor will it reduce or waive any license fees still owed to MSI by Affiliate. Upon termination of the Enterprise License, Affiliate shall immediately cease any further use of Software Products. Affiliate may also terminate this agreement by not paying an invoice for a subsequent year's Service Fee within sixty (60) days of invoice issue date.

C. MSI Termination. MSI has the right to terminate this Agreement by providing thirty (30) days written notice to Affiliate. If MSI's termination notice is based on an alleged breach by Affiliate, then Affiliate shall have thirty (30) days from the date of its receipt of MSI's notice of termination, which shall set forth in detail Affiliate's purported breach of this Agreement, to cure the alleged breach. If within thirty (30) days of written notice of violation from MSI Affiliate has not reasonably cured the described breach of this Agreement, Affiliate shall immediately discontinue all use of Software Products and certify to MSI that it has returned or destroyed all copies of Software Products in its possession or control. If MSI terminates this Agreement prior to the end of a Service Period for breach, no refund for any unused Service Fees will be provided. If MSI terminates this Agreement prior to the end of a Service Period for no reason, and not based on Affiliate's failure to cure the breach of a material term or condition of this Agreement, MSI shall refund to Affiliate an amount calculated by multiplying the total amount of Service Fees paid by Affiliate for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365.

D. Effect of Termination. Upon termination or expiration of this Agreement for any reason, all licensed rights granted in this Agreement will immediately cease to exist and Affiliate must promptly discontinue all use of the Software Products, erase all LPR Data accessed through the Software Service from its computers, including LPR Data transferred through an API, and return all copies of any related documentation and other materials.

IV. **Warranty and Disclaimer; Infringement Protection; Use of Software Products Interface.**

A. Warranty and Disclaimer. MSI warrants that the Software Products will be free from all Significant Defects (as defined below) during the term of this Agreement (the "Warranty Period"). "Significant Defect" means a defect in a Software Product that impedes the primary function of the Software Product. This warranty does not include products not manufactured by MSI. MSI will repair or replace any Software Product with a Significant Defect during the Warranty Period; *provided, however*, if MSI cannot substantially correct a Significant Defect in a commercially reasonable manner, Affiliate may terminate this Agreement and MSI shall refund to Affiliate an amount calculated by multiplying the total amount of Service Fees paid by Affiliate for the then-current Service Period by the percentage resulting from dividing the number of days remaining in the then-current Service Period, by 365. The foregoing remedies are Affiliate's exclusive remedy for defects in the Software Product. MSI shall not be responsible for labor charges for removal or reinstallation of defective software, charges for transportation, shipping or handling loss, unless such charges are due to MSI's gross negligence or intentional misconduct. MSI disclaims all warranties, expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose. In no event shall MSI be liable for any damages whatsoever arising out of the use of, or inability to use, the Software Products.

B. Infringement Protection. If an infringement claim is made against Affiliate by a third-party in a court of competent jurisdiction regarding Affiliate's use of any of the Software Products, MSI shall indemnify Affiliate, and assume all legal responsibility and costs to contest any such claim. If Affiliate's use of any portion of the Software Products or documentation provided to Affiliate by MSI in connection with the Software Products is enjoined by a court of competent jurisdiction, MSI shall do one of the following at its option and expense within sixty (60) days of such enjoinder: (1) Procure for Affiliate the right to use such infringing portion; (2) replace such infringing portion with a non-infringing portion providing equivalent functionality; or (3) modify the infringing portion so as to eliminate the infringement while providing equivalent functionality.

C. Use of Software Products Interface. Under certain circumstances, it may be dangerous to operate a moving vehicle while attempting to operate a touch screen or laptop screen and any of their applications. It is agreed by Affiliate that Affiliate's users will be instructed to only utilize the interface to the Software Products at times when it is safe to do so. MSI is not liable for any accident caused by a result of distraction such as from viewing the screen while operating a moving vehicle.

V. **Software Support, Warranty and Maintenance.**

Affiliate will receive technical support by submitting a support ticket to MSI's company support website or by sending an email to MSI's support team. Updates, patches and bug fixes of the Software Products will be made available to Affiliate at no additional charge, although charges may be assessed if the Software Product is requested to be delivered on physical media. MSI will provide Software Products support to Affiliate's Technical Support Agents through e-mail, fax and telephone.

VI. **Camera License Keys (CLKs).**

Affiliate is entitled to use of the Software Products during the term of this Agreement to set up and install the Software Products on an unlimited number of media centers within Affiliate's agency in accordance with selected Service Options. As Affiliate installs additional units of the Software Products and connects them to LPR cameras, Affiliate is required to obtain a Camera License Key (CLK) for each camera installed and considered in active service. A CLK can be obtained by Affiliate by going to MSI's company support website and completing the online request form to MSI technical support staff. Within two (2) business days of Affiliate's application for a CLK, Affiliate's Technical Support Agent will receive the requested CLK that is set to expire on the last day of the Initial Term or the then-current Service Period, as the case may be.

VII. **Ownership of Software.**

A. Ownership of Software Products. The Software Products are copyrighted by MSI and remain the property of MSI. The license granted under this Agreement is not a sale of the Software Products or any copy. Affiliate owns the physical media on which the Software Products are installed, but MSI retains title and ownership of the Software Products and all other materials included as part of the Software Products. Nothing in this Agreement shall be deemed to convey to Affiliate or to any other party, any ownership interest in any Software Products.

B. Rights in Software Products. MSI represents and warrants that: (1) it has title to the Software and the authority to grant license to use the Software Products; (2) it has the corporate power and authority and the legal right to grant the licenses contemplated by this Agreement; and (3) it has not and will not enter into agreements and will not take or fail to take action that causes its legal right or ability to grant such licenses to be restricted.

VIII. **Data Sharing, Access and Security.**

If Affiliate is a generator as well as a consumer of LPR Data, Affiliate at its option may share its LEA LPR Data with similarly situated LEAs who contract with MSI to access LEARN (for example, LEAs who share LEA LPR Data with other LEAs). MSI will not share any LEA LPR Data generated by the Affiliate without the permission of the Affiliate.

MSI has implemented procedures to allow for adherence to the FBI CJIS Security Policy. The hosting facility utilizes access control technologies that meet or exceed CJIS requirements. In addition, MSI has installed and configured network intrusion prevention appliances, as well as ensured that the configuration of the Microsoft environment adhere to the Windows Server Security Guide.

LPR Data must reside within the Software Product and cannot be copied to another system, unless Affiliate purchases MSI's API. MSI offers an API whereby Affiliate may load LPR Data and provide for ongoing updating of LPR Data into a third-party system of Affiliate's choosing. This service is offered as an optional service and in addition to the annual subscription fee described herein.

IX. Ownership and Authorized Use of Data.

MSI retains all title and rights to Commercial LPR Data. Nothing in this Agreement shall be deemed to convey to Affiliate or to any other party, any ownership interest in any Commercial LPR Data.

Users shall not utilize Commercial LPR Data on the behalf of other local, state or Federal LEAs. Affiliate retains all rights to LEA LPR Data generated by the Affiliate. Should Affiliate terminate agreement with MSI, a copy of all LEA LPR Data generated by the Affiliate will be created and provided to the Affiliate. After the copy is created, all LEA LPR Data generated by the Affiliate will be deleted from LEARN at the written request of an authorized representative of the Affiliate or per the Affiliate's designated retention policy, whichever occurs first. Commercial LPR Data and LEA LPR Data should be used by the Affiliate for law enforcement purposes only.

Affiliate is prohibited from accessing the Software Products, and the Commercial LPR Data for purposes other than for law enforcement purposes.

X. Loss of Data, Irregularities and Recovery.

MSI places imperative priority on supporting and maintaining data center integrity. Using redundant disk arrays, there is a virtual guarantee that any hard disk failure will not result in the corruption or loss of the valuable LPR data that is essential to the LEARN system and clients.

XI. Data Retention and Redundancy.

LEA LPR Data is governed by the contributing LEA's retention policy. LEA LPR Data that reaches its expiration date will be deleted from LEARN. MSI's use of redundant power sources, fiber connectivity and disk arrays ensure no less than 99% uptime of the LEARN LPR database server system.

XII. Account Access.

A. **Eligibility.** The Software Products, LPR Data, Commercial LPR Data, and associated analytical tools, and LEARN, are accessible to LEAs only. Affiliate shall only authorize individuals who satisfy the eligibility requirements of "Users" to access LEARN. MSI in its sole discretion may deny access to LEARN to any individual based on such person's failure to satisfy such eligibility requirements. User logins are restricted to agents and sworn officers of the Affiliate.

No User logins may be provided to agents or officers of other local, state, or Federal LEAs without the express written consent of MSI.

B. Security. Affiliate shall be responsible for assigning an Agency Manager who in turn will be responsible for assigning to each of Affiliate's Users a username and password (one per user account). A limited number of User accounts is provided. Affiliate will cause the Users to maintain username and password credentials confidential and will prevent use of such username and password credentials by any unauthorized person(s). Affiliate shall notify MSI immediately if Affiliate believes the password of any of its Users has, or may have, been obtained or used by any unauthorized person(s). In addition, Affiliate must notify MSI immediately if Affiliate becomes aware of any other breach or attempted breach of the security of any of its Users' accounts.

C. CJIS Requirements. Affiliate certifies that its LEARN users shall comply with the CJIS requirements outlined in Exhibit A.

D. Manner of Use. Affiliate must use its account in a manner that demonstrates integrity, honesty, and common sense.

E. Survival of Restrictions and Other Related Matters.

- i. Affiliate shall cause each User to comply with the provisions of this **Section XII. E.**
- ii. Affiliate agrees to notify MSI immediately upon discovery of any unauthorized use or disclosure of Confidential Information or any other breach of this **Section XII. E** by Affiliate or any User, and Affiliate shall reasonably cooperate with MSI to regain possession of the Confidential Information, prevent its further unauthorized use, and otherwise prevent any further breaches of this **Section XII. E.**
- iii. Affiliate agrees that a breach or threatened breach by Affiliate or a User of any covenant contained in this **Section XII. E** will cause irreparable damage to MSI and that MSI could not be made whole by monetary damages. Therefore, MSI shall have, in addition to any remedies available at law, the right to seek equitable relief to enforce this Agreement.
- iv. No failure or delay by MSI in exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise of any such right, power or privilege preclude any other or further exercise thereof.
- v. The restrictions set forth in this **Section XII. E** shall survive the termination of this Agreement for an indefinite period of time.

XIII. Service Package, Fees and Payment Provisions.

(1) Service Package and Fees.

The licenses granted in this Agreement are based on the continued, yearly payment of the Service Fees for the software services and software products set forth below, at a yearly Service Fee of \$407,000 for five (5) years from the Effective Date:

- A. Service Fee for hosting LPR Data collected by Affiliate using MSI cameras. The Service Fee for hosting LPR Data collected using MSI cameras is based on the number of MSI CLK's issued.

Affiliate and MSI agree that the number of CLKs issued as of the Effective Date of this Agreement is twenty-eight (28). Additional CLKs shall be subject to additional Service Fees.

- B. Service Fee for integrating and hosting LPR Data collected by Affiliate using non-MSI cameras ("Competitive Camera System"). Affiliate and MSI agree that the number of Competitive Camera systems as of the Effective Date of this Agreement is one hundred and forty (140). Should integration and hosting services be desired for additional Competitive Camera Systems which are outside the existing, original one hundred and forty (140) Competitive Camera Systems, additional Competitive Camera Systems can be added at a cost of \$1,500 per year.
- C. Service Fee for access to MSI's Commercial LPR Data
- D. API functionality

Payment of Service Fees entitles Affiliate to use of the Software Products, replacement of CLKs, access to Commercial LPR Data, camera integration, LPR Data hosting, and access to the updates and releases of the Software Products and associated equipment driver software to allow the Software Products to remain current and enable the best possible performance, for the relevant Service Period.

(2) Payment.

Payment of the Service Fee is due thirty (30) days prior to the renewal of the then-current Service Period. All Service Fees are exclusive of any sales, use, value-added or other federal, state or local taxes (excluding taxes based on MSI's net income) and Affiliate agrees to pay any such tax. Service Fees may increase by no higher than 4% per year for years after the first year of this agreement.

A. **Advanced Service Fee Payments.** MSI will accept advanced Service Fee payments on a case by case basis for Affiliates who wish to lock in the Service Fee rates for subsequent periods at the rates currently in effect, as listed in the table above. If Affiliate makes advanced Service Fee payments to MSI, advanced payments to MSI will be applied in full to each subsequent Service Period's Service Fees until the balance of the credits is reduced to a zero balance. System based advanced credits shall be applied to subsequent Service Fees in the amount that entitles Affiliate continued operation of the designated camera unit systems for the following Service Period until the credits are reduced to a zero balance.

B. **Price Adjustment.** After the initial term of the Agreement, MSI has the right to increase or decrease the annual Service Fee from one Service Period to another; *provided, however*, that in no event will a Service Fee be increased by more than 4% of the prior Service Period's Service Fees. If MSI intends to adjust the Service Fee for a subsequent Service Period, it must give Affiliate notice of the proposed increase on or before the date that MSI invoices Affiliate for the upcoming Service Period.

XIV. Miscellaneous.

A. Limitation of Liability. IN NO EVENT SHALL MSI BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL DAMAGES INCLUDING DAMAGES FOR LOSS OF USE, DATA OR PROFIT, ARISING OUT OF OR CONNECTED WITH THE USE OF THE SOFTWARE PRODUCTS, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF MSI HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IN NO EVENT WILL MSI'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE FEES PAID BY AFFILIATE TO MSI FOR THE SOFTWARE PRODUCTS LICENSED UNDER THIS AGREEMENT.

B. Confidentiality. (a) Affiliate acknowledges that Software Products contain valuable and proprietary information of MSI and Affiliate will not disassemble, decompile or reverse engineer any Software Products to gain access to confidential information of MSI.

(1) Non-Disclosure of Confidential Information. Affiliate and each User will become privy to Confidential Information during the term of this Agreement. Affiliate acknowledges that a large part of MSI's competitive advantage comes from the collection and analysis of this Confidential Information and Affiliate's use, except as expressly permitted under this Agreement, and disclosure of any such Confidential Information would cause irreparable damage to MSI.

(2) Restrictions. As a result of the sensitive nature of the Confidential Information, Affiliate agrees, except to the extent expressly permitted under this Agreement, (i) not to use or disclose, directly or indirectly, and not to permit Users to use or disclose, directly or indirectly, any LPR location information obtained through Affiliate's access to the Software Service or any other Confidential Information; (ii) not to download, copy or reproduce any portion of the LPR Data and other Confidential Information; and (iii) not to sell, transfer, license for use or otherwise exploit the LPR Data and other Confidential Information in any way. Additionally, Affiliate agrees to take all necessary precautions to protect the Confidential Information against its unauthorized use or disclosure and exercise at least the same degree of care in safeguarding the Confidential Information as Affiliate would with Affiliate's own confidential information and to promptly advise MSI in writing upon learning of any unauthorized use or disclosure of the Confidential Information.

(3). Third Party Information. Affiliate recognizes that MSI has received, and in the future will continue to receive, from LEAs associated with MSI their confidential or proprietary information ("**Associated Third Party Confidential Information**"). By way of example, Associated Third Party Confidential Information includes LEA LPR Data. Affiliate agrees, except to the extent expressly permitted by this Agreement, (i) not to use or to disclose to any person, firm, or corporation any Associated Third Party Confidential Information, (ii) not to download, copy, or reproduce any Associated Third Party Confidential Information, and (iii) not to sell, transfer, license for use or otherwise exploit any Associated Third Party Confidential Information. Additionally, Affiliate agrees to take all necessary precautions to protect the Associated Third Party Confidential Information against its unauthorized use or disclosure and exercise at least the same degree of care in safeguarding the Associated Third Party Confidential Information as Affiliate would with Affiliate's own confidential information and to promptly advise MSI in writing upon learning of any unauthorized use or disclosure of the Associated Third Party Confidential Information.

C. Assignment. Neither MSI nor Affiliate is permitted to assign this Agreement without the prior written consent of the other party. Any attempted assignment without written consent is void.

D. Amendment; Choice of Law. No amendment or modification of this Agreement shall be effective unless in writing and signed by authorized representatives of the parties. This Agreement shall be governed by the laws of the state of Texas without regard to its conflicts of law.

E. Complete Agreement. This Agreement constitutes the final and complete agreement between the parties with respect to the subject matter hereof, and supersedes any prior or contemporaneous agreements, written or oral, with respect to such subject matter.

F. Relationship. The relationship created hereby is that of contractor and customer and of licensor and Affiliate. Nothing herein shall be construed to create a partnership, joint venture, or agency relationship between the parties hereto. Neither party shall have any authority to enter into agreements of any kind on behalf of the other and shall have no power or authority to bind or obligate the other in any manner to any third party. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever. Each party hereto represents that it is acting on its own behalf and is not acting as an agent for or on behalf of any third party.

G. No Rights in Third Parties. This agreement is entered into for the sole benefit of MSI and Affiliate and their permitted successors, executors, representatives, administrators and assigns. Nothing in this Agreement shall be construed as giving any benefits, rights, remedies or claims to any other person, firm, corporation or other entity, including, without limitation, the general public or any member thereof, or to authorize anyone not a party to this Agreement to maintain a suit for personal injuries, property damage, or any other relief in law or equity in connection with this Agreement.

H. Construction. The headings used in this Agreement are for convenience and ease of reference only, and do not define, limit, augment, or describe the scope, content or intent of this Agreement. Any term referencing time, days or period for performance shall be deemed calendar days and not business days, unless otherwise expressly provided herein.

I. Severability. If any provision of this Agreement shall for any reason be held to be invalid, illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this Agreement, such provision shall be construed so as to make it enforceable to the greatest extent permitted, such provision shall remain in effect to the greatest extent permitted and the remaining provisions of this Agreement shall remain in full force and effect.

J. Federal Government. Any use, copy or disclosure of Software Products by the U.S. Government is subject to restrictions as set forth in this Agreement and as provided by DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227 (ALT III), as applicable.

K. Right to Audit. Affiliate, upon thirty (30) days advanced written request to MSI, shall have the right to investigate, examine, and audit any and all necessary non-financial books, papers, documents, records and personnel that pertain to this Agreement and any other Sub Agreements.

L. Notices; Authorized Representatives; Technical Support Agents. All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person; (b) sent by facsimile transmission indicating receipt at the facsimile number where sent; (c) one (1) business day after being deposited with a reputable overnight air courier service; or (d) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. All notices and communications regarding default or termination of this Agreement shall be delivered by hand or sent by certified mail, postage pre-paid and return receipt requested. Either party may from time to time change the notice address set forth below by delivering 30 days advance notice to the other party in accordance with this section setting forth the new address and the date on which it will become effective.

<p>Motorola Solutions, Inc. Attn: Sales Administration 500 W. Monroe St. Chicago, IL 60661</p>	<p>Affiliate: _____ Attn: _____ Address: _____ _____</p>
--	--

M. Authorized Representatives; Technical Support Agents. Affiliate's Authorized Representatives and its Technical Support Agents are set forth below in the Contact Information Worksheet. Affiliate's Authorized Representative is responsible for administering this Agreement and Affiliate's Technical Support Agents are responsible for administering the Software Products and acting as Affiliate's Software Products support contact. Either party may from time to time change its Authorized Representative, and Affiliate may from time to time change its Technical Support Agents, in each case, by delivering 30 days advance notice to the other party in accordance with the notice provisions of this Agreement.

O. No Exclusivity. MSI may at any time, directly or indirectly, engage in similar arrangements with other parties, including parties which may conduct operations in geographic areas in which Affiliate operates. Additionally, MSI reserves the right to provide LPR Data to third-party entities for purposes of promotions, marketing, business development or any other commercially reasonable reason that MSI deems necessary and appropriate.

P. No Reliance. Affiliate represents that it has independently evaluated this Agreement and is not relying on any representation, guarantee, or statement from MSI or any other party, other than as expressly set forth in this Agreement.

Q. Force Majeure. Neither party will be liable for failure to perform or delay in performing any obligation under this Agreement if nonperformance is caused by an occurrence beyond the reasonable control of such party and without its fault or negligence such as acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, delays of common carriers, or any other cause beyond the reasonable control of such party.

Enterprise Service Agreement

Contact Information Worksheet

Please complete the following contact information for your MSI Enterprise License program.

Enterprise License Agreement Holder			
Company / Agency Name:			
Company / Agency Type:			
Address:			
Primary Contact			
Name:			
Title:		Phone:	
Email:			
Supervisor Information			
Name:			
Title:		Phone:	
Email:			
Financial Contact (Accounts Payable)			
Name:			
Title:		Phone:	
Email:			
Technical Support Contact # 1			
Name:			
Title:		Phone:	
Email:			
Technical Support Contact # 2			
Name:			
Title:		Phone:	
Email:			

For questions or concerns, please contact MSI sales team for Vigilant products:

sales@vigilantsolutions.com

1-925-398-2079

Exhibit A: CJIS Requirements

MSI and the Affiliate agree on the importance of data security, integrity and system availability and that these security objectives will only be achieved through shared responsibility. MSI and the Affiliate agree they will more likely be successful with information security by use of the MSI supplied technical controls and client Affiliate use of those controls; in conjunction with agency and personnel policies to protect the systems, data and privacy.

MSI and the Affiliate agree that Affiliate owned and FBI-CJIS supplied data in MSI systems does not meet the definition of FBI-CJIS provided Criminal Justice Information (CJI). Regardless, MSI agrees to treat the Affiliate-supplied information in MSI systems as CJI. MSI will strive to meet those technical and administrative controls; ensuring the tools are in place for the proper protection of systems, information and privacy of individuals to the greatest degree possible.

MSI and the Affiliate agree that information obtained or incorporated into MSI systems may be associated with records that are sensitive in nature having, tactical, investigative and Personally Identifiable Information. As such, that information will be treated in accordance with applicable laws, policies and regulations governing protection and privacy of this type of data.

MSI and the Affiliate agree that products and services offered by MSI are merely an investigative tool to aid the client in the course of their duties and that MSI make no claims that direct actions be initiated based solely upon the information responses or analytical results. Further, MSI and the Affiliate agree that the Affiliate is ultimately responsible for taking the appropriate actions from results, hits, etc. generated by MSI products and require ongoing training, human evaluation, verifying the accuracy and currency of the information, and appropriate analysis prior to taking any action.

As such, the parties agree to do the following:

MSI:

1. MSI has established the use of FBI-CJIS Security Policy as guidance for implementing technical security controls in an effort to meet or exceed those Policy requirements.
2. MSI agrees to appoint a CJIS Information Security Officer to act as a conduit to the client Contracting Government Agency, Agency Coordinator, to receive any security policy information and disseminate to the appropriate staff.
3. MSI agrees to adhere to FBI-CJIS Security Policy Awareness Training and Personnel Screening standards as required by the Affiliate.
4. MSI agrees, by default, to classify all client supplied data and information related to client owned infrastructure, information systems or communications systems as "Criminal Justice Data". All client information will be treated at the highest level of confidentiality by all MSI staff and authorized partners. MSI has supporting guidance/policies for staff handling the full life cycle of information in physical or electronic form and has accompanying disciplinary procedures for unauthorized access, misuse or mishandling of that information.
5. MSI will not engage in data mining, commercial sale, unauthorized access and/or use of any of Affiliate owned data.
6. MSI and partners agree to use their formal cyber Incident Response Plan if such event occurs.
7. MSI agrees to immediately inform Affiliate of any cyber incident or data breach, to include DDoS, Malware, Virus, etc. that may impact or harm client data, systems or operations so proper analysis can be performed and client Incident Response Procedures can be initiated.

8. MSI will only allow authorized support staff to access the Affiliate's account or Affiliate data in support of Affiliate as permitted by the terms of contracts.
9. MSI agrees to use training, policy and procedures to ensure support staff use proper handling, processing, storing, and communication protocols for Affiliate data.
10. MSI agrees to protect client systems and data by monitoring and auditing staff user activity to ensure that it is only within the purview of system application development, system maintenance or the support roles assigned.
11. MSI agrees to inform the Affiliate of any unauthorized, inappropriate use of data or systems.
12. MSI will design software applications to facilitate FBI-CJIS compliant information handling, processing, storing, and communication of Affiliate.
13. MSI will advise Affiliate when any software application or equipment technical controls are not consistent with meeting FBI-CJIS Policy criteria for analysis and due consideration.
14. MSI agrees to use the existing Change Management process to sufficiently plan for system or software changes and updates with Rollback Plans.
15. MSI agrees to provide technical security controls that only permit authorized user access to Affiliate owned data and MSI systems as intended by the Affiliate and data owners.
16. MSI agrees to meet or exceed the FBI-CJIS Security Policy complex password construction and change rules.
17. MSI will only provide access to MSI systems and Affiliate owned information through Affiliate managed role-based access and applied sharing rules configured by the Affiliate.
18. MSI agrees to provide technical controls with additional levels of user Advanced Authentication in Physically Non-Secure Locations.
19. MSI agrees to provide compliant FIPS 140-2 Certified 128-bit encryption to Affiliate owned data during transport and storage ("data at rest") while in the custody and control of MSI.
20. MSI agrees to provide firewalls and virus protection to protect networks, storage devices and data.
21. MSI agrees to execute archival, purges and/or deletion of data as configured by the data owner.
22. MSI agrees to provide auditing and alerting tools within the software applications so Affiliate can monitor access and activity of MSI support staff and Affiliate users for unauthorized access, disclosure, alteration or misuse of Affiliate owned data. (MSI support staff will only have access when granted by the Affiliate.)
23. MSI will only perform direct support remote access to Affiliate systems/infrastructure when requested, authorized and physically granted access to the applications/systems by the Affiliate. This activity will be documented by both parties.
24. MSI creates and retains activity transaction logs to enable auditing by the Affiliate data owners and MSI staff.
25. MSI agrees to provide physical protection for the equipment-storing Affiliate data along with additional technical controls to protect physical and logical access to systems and data.
26. MSI agrees to participate in any Information or Technical Security Compliance Audit performed by the Affiliate, state CJIS System Agency or FBI-CJIS Division.
27. MSI agrees to perform independent employment background screening for its' staff and participate in additional fingerprint background screening as required by Affiliate.
28. MSI agrees that the Affiliate owns all Affiliate contributed data to include "hot-lists", scans, user information etc., is only shared as designated by the client and remains the responsibility and property of the Affiliate.

Affiliate:

1. Affiliate agrees to appoint an Agency Coordinator as a central Point of Contact for all FBI-CJIS Security Policy related matters and to assign staff that are familiar with the contents of the FBI-CJIS Security Policy.

2. Affiliate agrees to have the Agency Coordinator provide timely updates with specific information regarding any new FBI-CJIS, state or local information security policy requirements that may impact MSI compliance or system/application development and, to facilitate obtaining certifications, training, and fingerprint-based background checks as required.
3. Affiliate agrees to inform MSI when any FBI-CJIS Security Awareness Training, personnel background screening or execution of FBI-CJIS Security Addendum Certifications are required.
4. Affiliate agrees to immediately inform MSI of any relevant data breach or cyber incident, to include DDoS, Malware, Virus, etc. that may impact or harm MSI systems, operations, business partners and/or other Affiliates, so proper analysis can be performed, and Incident Response Procedures can be initiated.
5. Affiliate agrees that they are responsible for the legality and compliance of information recorded, submitted or placed in MSI systems and use of that data.
6. Affiliate agrees that they are responsible for proper equipment operation and placement of equipment.
7. Affiliate agrees that they are responsible for vetting authorized user access to MSI systems with due consideration of providing potential access to non-Affiliate information.
8. Affiliate agrees that responsibility and control of persons granted access to purchased MSI systems, along with data stored and transmitted via MSI systems, is that of the Affiliate.
9. Affiliate agrees that they have responsibility for all data security, handling and data protection strategies from point of acquisition, during transport and until submission ("Hotlist upload") into MSI systems.
10. Affiliate agrees to reinforce client staff policies and procedures for secure storage and protection of MSI system passwords.
11. Affiliate agrees to reinforce client staff policies for creating user accounts with only government domain email addresses. Exceptions will be granted in writing.
12. Affiliate agrees to reinforce client staff policies for not sharing user accounts.
13. Affiliate agrees to use MSI role-based access as designed to foster system security and integrity.
14. Affiliate agrees that they control, and are responsible for, appropriate use and data storage policies as well as procedures for the data maintained outside the MSI systems. This includes when any information is disseminated, extracted or exported out of MSI systems.
15. Affiliate agrees that they control and are responsible for developing policies, procedures and enforcement for applying deletion/purging and dissemination rules to information within and outside the MSI systems.
16. Affiliate agrees that it is their responsibility to ensure data and system protection strategies are accomplished through the tools provided by MSI for account and user management features along with audit and alert threshold features.
17. Affiliate agrees to use the "virtual escorting" security tools provided for managing client system remote access and monitor MSI support staff when authorized to assist the client.
18. Affiliate agrees that the MSI designed technical controls and tools will only be effective in conjunction with Affiliate created policies and procedures that guide user access and appropriate use of the system.
19. Affiliate agrees that information and services provided through MSI products do not provide any actionable information, Affiliate users are responsible for the validity and accuracy of their data and developing procedures to verify information with the record owner and other systems (NCIC) based upon the potential lead generated.