AGREEMENT NO. _____

AGREEMENT 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 ("City"), acting by and through its Board of Harbor Commissioners ("Board") and MOTOROLA SOLUTIONS, INC., a Delaware corporation, 500 W. Monroe Street, Chicago, IL 60661 ("Consultant").

WHEREAS, City requires a cyber-security solution for the Los Angeles Port Police mission-critical systems to ensure long-term cyber-security safety and success; and

WHEREAS, City requires the professional, expert and technical services of Consultant on a temporary or occasional basis to assist the City in providing deeper visibility and the ability to proactively detect cyber-security threats to the Los Angeles Port Police safety network; and

WHEREAS, Consultant possesses extensive experience in dealing with the complexities and critical nature of the ASTRO Radio, CAD and RMS systems currently utilized by the Los Angeles Port Police and is uniquely qualified to address cyber-security issues, system vulnerabilities, causes, prevention, network assessment, user training requirements and specific application understanding of the existing Motorola Solutions Inc. proprietary systems for which this solution is sought; and

WHEREAS, Consultant, by virtue of training, experience and specific knowledge of Motorola Solutions Inc. proprietary systems, is uniquely well qualified to provide such services to City; and

WHEREAS, City does not employ personnel with the required expertise nor is it feasible to do so on a temporary or occasional basis;

NOW, THEREFORE, IT IS MUTUALLY AGREED AS FOLLOWS:

1. SERVICES TO BE PERFORMED BY CONSULTANT

A. Consultant hereby agrees to render to City, as an independent contractor, certain professional, technical and expert services of a temporary and occasional character as set forth in Exhibit A ("Scope of Work").

B. Consultant, at its sole cost and expense, shall furnish all services, materials, equipment, subsistence, transportation and all other items necessary to perform the Scope of Work. As between City and Consultant, Consultant is solely responsible for any taxes or fees which may be assessed against it or its employees resulting from performance of the Scope of Work, whether social security, payroll or other, and

regardless of whether assessed by the federal government, any state, the City, or any other governmental entity.

C. Consultant acknowledges and agrees that it lacks authority to perform any services outside the Scope of Work. Consultant further acknowledges and agrees that any services it performs outside the Scope of Work are performed as a volunteer and shall not be compensable under this Agreement.

D. The Scope of Work shall be performed by personnel qualified and competent in the sole reasonable discretion of the Executive Director or his or her designee ("Executive Director"), whether performance is undertaken by Consultant or third-parties with whom Consultant has contracted ("Subconsultants"). Obligations of this Agreement, whether undertaken by Consultant or Subconsultants, are and shall be the responsibility of Consultant. Consultant acknowledges and agrees that this Agreement creates no rights in Subconsultants with respect to City and that obligations that may be owed to Subconsultants, including, but not limited to, the obligation to pay Subconsultants for services performed, are those of Consultant alone. Upon Executive Director's written request, Consultant shall supply City's Harbor Department ("Department") with all agreements between it and its Subconsultants.

2. SERVICES TO BE PERFORMED BY CITY

A. City shall furnish Consultant, upon its request, all documents and papers in possession of City which may lawfully be supplied to Consultant and which are necessary for it to perform its obligations.

B. The Executive Director or his or her designee is designated as the contract administrator for City and shall also decide any and all questions which may arise as to the quality or acceptability of the services performed and the manner of performance, the interpretation of instructions to Consultant and the acceptable completion of this Agreement and the amount of compensation due. Notwithstanding the preceding, the termination of this Agreement shall be governed by the provisions of Article 11 (Termination) hereof.

C. Consultant shall provide Executive Director with reasonable advance written notice if it requires access to premises of Department. Subsequent access rights, if any, shall be granted to Consultant at the sole reasonable discretion of Executive Director, specifying conditions Consultant must satisfy in connection with such access. Consultant acknowledges that such areas may be occupied or used by tenants or contractors of City and that access rights granted by Department to Consultant shall be consistent with any such occupancy or use.

3. EFFECTIVE DATE AND TERM OF AGREEMENT

A. Subject to the provisions of Charter Section 245, the effective date of this Agreement shall be the date of its execution by Executive Director upon authorization of the Board. Consultant is aware that the City Council, pursuant to Charter Section 245 of

the City of Los Angeles, has the right to review this Agreement. Accordingly, in no event shall this Agreement become effective until after the expiration of the fifth Council meeting day after Board action, or the date of City Council's approval of the Agreement.

B. This Agreement shall be in full force and effect commencing from the date of execution and shall continue until the earlier of the following occurs:

1. Three (3) years have lapsed from the effective date of this Agreement;

or

2. The Board of Harbor Commissioners, in its sole discretion, terminates and cancels all or part of this Agreement for any reason upon giving to Consultant ten (10) days' notice in writing of its election to cancel and terminate this Agreement.

4. TERMINATION DUE TO NON-APPROPRIATION OF FUNDS

This Agreement is subject to the provisions of the Los Angeles City Charter which, among other things, precludes the City from making any expenditure of funds or incurring any liability, including contractual commitments, in excess of the amount appropriated therefor.

The Board, in awarding this Agreement, is expected to appropriate sufficient funds to meet the estimated expenditure of funds through June 30 of the current fiscal year and to make further appropriations in each succeeding fiscal year during the life of the Agreement. However, the Board is under no legal obligation to do so.

The City, its boards, officers, and employees are not bound by the terms of this Agreement or obligated to make payment thereunder in any fiscal year in which the Board does not appropriate funds therefore. The Consultant is not entitled to any compensation in any fiscal year in which funds have not been appropriated for the Agreement by the Board.

Although the Consultant is not obligated to perform any work under the Agreement in any fiscal year in which no appropriation for the Agreement has been made, the Consultant agrees to resume performance of the work required by the Agreement on the same terms and conditions for a period of sixty (60) days after the end of the fiscal year if an appropriation therefore is approved by the Board within that 60-day period. The Consultant is responsible for maintaining all insurance and bonds during this 60-day period until the appropriation is made; however, such extension of time is not compensable.

If in any subsequent fiscal year funds are not appropriated by the Board for the work required by the Agreement, the Agreement shall be terminated. However, such termination shall not relieve the parties of liability for any obligation previously incurred.

5. COMPENSATION AND PAYMENT

A. As compensation for the satisfactory performance of the services required by this Agreement, City shall pay and reimburse Consultant at the rates set forth in Exhibit A.

B. The maximum payable under this Agreement, including reimbursable expenses (see Exhibit A), shall be One Million One Hundred Seventy-Seven Thousand Eight Hundred Eighty-Six Dollars and Eighty-Seven Cents ($1,177,886.87).

C. Consultant shall submit invoices in quadruplicate to City monthly following the effective date of this Agreement for services performed during the preceding month. Each such invoice shall be signed by the Consultant and shall include the following certification:

> "I certify under penalty of perjury that the above bill is just and correct according to the terms of Agreement No. _____ and that payment has not been received. I further certify that I have complied with the provisions of the City's Living Wage Ordinance.
>
> _____"
> (Consultant's Signature)

D. Consultant must include on the face of each itemized invoice submitted for payment its Business Tax Registration Certificate number, as required at Article 8 of this Agreement. No invoice will be processed for payment by City without this number shown thereon. All invoices shall be approved by the Executive Director or his or her designee prior to payment. All invoices due and payable and found to be in order shall be paid as soon as, in the ordinary course of City business, the same may be approved, audited and paid.

Consultant shall submit appropriate supporting documents with each invoice. Such documents may include provider invoices, payrolls, and time sheets. The City may require, and Consultant shall provide, all documents reasonably required to determine whether amounts on the invoice are allowable expenses under this Agreement.

Further, where the Consultant employs Subconsultants under this Agreement, the Consultant shall submit to City, with each monthly invoice, a Monthly Subconsultant Monitoring Report Form (Exhibit B) listing SBE/VSBE/MBE/WBE/DVBE/OBE amounts. Consultant shall provide an explanation for any item that does not meet or exceed the anticipated participation levels for this Agreement, with specific plans and recommendations for improved Subconsultant utilization. Invoices will not be paid without a completed Monthly Subconsultant Monitoring Report Form. All invoices are subject to audit. Consultant is not required to submit support for direct costs items of $25 or less.

E. For payment and processing, all invoices should be mailed to the following address:

Accounts Payable Section
Harbor Department, City of Los Angeles
P.O. Box 191
San Pedro, CA 90733-0191

6. RECORDKEEPING AND AUDIT RIGHTS

A. Consultant shall keep and maintain full, complete and accurate books of accounts and records of the services performed under this Agreement in accordance with generally accepted accounting principles consistently applied, which books and records shall be readily accessible to and open for inspection and copying at the premises by City, its auditors or other authorized representatives. Notwithstanding any other provision of this Agreement, failure to do so shall constitute a conclusive waiver of any right to compensation for such services as are otherwise compensable hereunder. Such books and records shall be maintained by Consultant for a period of three (3) years after completion of services to be performed under this Agreement or until all disputes, appeals, litigation or claims arising from this Agreement have been resolved.

B. During the term of this Agreement, City may audit, review and copy any and all writings (as that term is defined in Section 250 of the California Evidence Code) of Consultant and Subconsultants arising from or related to this Agreement or performance of the Scope of Work, whether such writings are (a) in final form or not, (b) prepared by Consultant, Subconsultants or any individual or entity acting for or on behalf of Consultant or a Subconsultant, and (c) without regard to whether such writings have previously been provided to City. Consultant shall be responsible for obtaining access to and providing writings of Subconsultants. Consultant shall provide City at Consultant's sole cost and expense a copy of all such writings within fourteen (14) calendar days of a written request by City. City's right shall also include inspection at reasonable times of the Consultant's office or facilities which are engaged in the performance of the Scope of Work. Consultant shall, at no cost to City, furnish reasonable facilities and assistance for such review and audit. Consultant's failure to comply with this Article 6 shall constitute a material breach of this Agreement and shall entitle City to withhold any payment due under this Agreement until such breach is cured. At no time will the Consultant be required to disclose cost and/or pricing data that is considered confidential or proprietary.

7. INDEPENDENT CONTRACTOR

Consultant, in the performance of the work required by this Agreement, is an independent contractor and not an agent or employee of City. Consultant shall not represent itself as an agent or employee of the City and shall have no power to bind the City in contract or otherwise.

8. BUSINESS TAX REGISTRATION CERTIFICATE

The City of Los Angeles Office of Finance requires the implementation and enforcement of Los Angeles Municipal Code Section 21.09 et seq. This Code Section provides that every person, other than a municipal employee, who engages in any business within the City of Los Angeles, is required to obtain the necessary Business Tax Registration Certificate and pay business taxes. The City Controller has determined that this Code Section applies to consulting firms that are doing work for the Department. See https://finance.lacity.org/how-register-btrc.

9. INDEMNIFICATION

Except for the sole negligence or willful misconduct of the City, or any of its Boards, Officers, Agents, Employees, Assigns and Successors in Interest, Consultant undertakes and agrees to defend, indemnify and hold harmless the City and any of its Boards, Officers, Agents, Employees, Assigns, and Successors in Interest from and against all suits and causes of action, claims, losses, demands and expenses, including, but not limited to, attorney's fees (both in house and outside counsel) and cost of litigation (including all actual litigation costs incurred by the City, including but not limited to, costs of experts and consultants), damages or liability of any nature whatsoever, for death or injury to any person, including Consultant's employees and agents, or damage or destruction of any property of either party hereto or of third parties, arising in any manner by reason of the negligent acts, errors, omissions or willful misconduct incident to the performance of this Agreement by Consultant or its subcontractors of any tier. Rights and remedies available to the City under this provision are cumulative of those provided for elsewhere in this Agreement and those allowed under the laws of the United States, the State of California, and the City.

10. INSURANCE

A. In addition to and not as a substitute for, or limitation of, any of the indemnity obligations imposed by Article 9, Consultant shall procure and maintain at its sole cost and expense and keep in force at all times during the term of this Agreement the following insurance:

(1) Commercial General Liability Insurance

Commercial general liability insurance covering personal and advertising injury, bodily injury, and property damage providing contractual liability, independent contractors, products and completed operations, and premises/operations coverage written by an insurance company authorized to do business in the State of California rated VII, A- or better in Best's Insurance Guide (or an alternate guide acceptable to City if Best's is not available) within Consultant's normal limits of liability but not less than Five Million Dollars ($5,000,000) per occurrence and Fifteen Million Dollars ($15,000,000) general aggregate. Where Consultant provides or dispenses alcoholic beverages, Host Liquor Liability coverage shall be provided as above. Where Consultant provides pyrotechnics, Pyrotechnics Liability shall be provided as above. Said limits shall

provide first dollar coverage except that Executive Director may permit a self-insured retention or self-insurance in those cases where, in his or her judgment, such retention or self-insurance is justified by the net worth of Consultant. The retention or self-insurance provided shall provide that any other insurance maintained by the Harbor Department shall be excess of Consultant's insurance and shall not contribute to it. In all cases, regardless of any deductible or retention, said insurance shall contain a defense of suits provision and a severability of interest clause. Each policy shall name the City of Los Angeles Harbor Department, its officers, agents and employees as Primary additional insureds.

Where Consultant's operations involve work within 50 feet of railroad track, Consultant's Commercial General Liability coverage shall have the railroad exclusion deleted.

(2) Automobile Liability Insurance

Automobile liability insurance written by an insurance company authorized to do business in the State of California rated VII, A- or better in Best's Insurance Guide (or an alternate guide acceptable to City if Best's is not available) within Consultant's normal limits of liability but not less than Five Million Dollars ($5,000,000) covering damages, injuries or death resulting from each accident or claim arising out of any one claim or accident. Said insurance shall protect against claims arising from actions or operations of the insured, or by its employees. Coverage shall contain a defense of suits provision. Each policy shall name the City of Los Angeles Harbor Department, its officers, agents and employees as Primary additional insureds.

(3) Workers' Compensation and Employer's Liability

Where applicable, Consultant shall comply with the provisions of Section 3700 of the California Labor code which requires every employer to be insured against liability for Workers' Compensation or to undertake self-insurance in accordance with the provisions of that Code, and that Consultant shall comply with such provisions before commencing the performance of the tasks under this Agreement. Coverage for claims under U.S. Longshore and Harbor Workers' Compensation Act, if required under applicable law, shall be included. Consultant shall submit Workers' Compensation policies whether underwritten by the state insurance fund or private carrier, which provide that the public or private carrier waives its right of subrogation against the City in any circumstance in which it is alleged that actions or omissions of the City contributed to the accident. Such Worker's Compensation and occupational disease requirements shall include coverage for all employees of Consultant, and for all employees of any subcontractor or other vendor retained by Consultant.

(4) Professional Liability Insurance and Technology Errors and Omissions Liability

Consultant is required to provide Professional Liability insurance with respect to negligent or wrongful acts, errors or omissions, or failure to render

services in connection with the professional services to be provided under this Agreement. This insurance shall protect against claims arising from professional services of the insured, or by its employees, agents, or contractors, and include coverage (or no exclusion) for contractual liability.

Consultant is required to provide Technology Errors and Omissions Liability Insurance with respect to negligent or wrongful acts, errors or omissions, in rendering or failing to render computer or information technology services or technology products in connection with the professional services to be provided under this Agreement. This insurance policy shall include coverage for Privacy and Network Security and protect against claims arising from products and services of the insured, or by its employees, agents, or contractors, and includes coverage (or no exclusion) for contractual liability. The limits disclosed herein shall neither increase nor decrease Consultant's liability as defined elsewhere in this Agreement.

Consultant certifies that it now has Professional Liability and Technology Errors and Omissions Liability Insurance in the amount of Ten Million Dollars ($10,000,000) per claim and Twenty Million Dollars ($20,000,000) annual aggregate, which shall cover the work to be performed pursuant to this Agreement and that it will keep such insurance or its equivalent in effect at all times during performance of said Agreement and until two (2) years following the completed term of this Agreement.

Notice of occurrences of claims under the policy shall be made to the City Attorney's office with copies to Risk Management.

B. Insurance Procured by Consultant on Behalf of City

In addition to and not as a substitute for, or limitation of, any of the indemnity obligations imposed by Article 9, and where Consultant is required to name the City of Los Angeles Harbor Department, its officers, agents and employees as Primary additional insureds on any insurance policy required by this Agreement, Consultant shall cause City to be named as an additional insured on all policies it procures in connection with this Article 10. Consultant shall cause such additional insured status to be reflected in the original policy or by additional insured endorsement (CG 2010 or equivalent) substantially as follows:

"Notwithstanding any inconsistent statement in the policy to which this endorsement is attached, or any endorsement or certificate now or hereafter attached hereto, it is agreed that City, Board, their officers, agents and employees, are additional insureds hereunder, and that coverage is provided for all contractual obligations, operations, uses, occupations, acts and activities of the insured under Agreement No. ___, and under any amendments, modifications, extensions or renewals of said Agreement regardless of where such contractual obligations, operations, uses, occupations, acts and activities occur.

"The policy to which this endorsement is attached shall provide a 10-days notice of cancellation for nonpayment of premium, and a 30-days notice of

cancellation for any other reasons to the Risk Manager.

"The coverage provided by the policy to which this endorsement is attached is primary coverage and any other insurance carried by City is excess coverage;

"In the event of one of the named insured's incurring liability to any other of the named insureds, this policy shall provide protection for each named insured against whom claim is or may be made, including claims by other named insureds, in the same manner as if separate policies had been issued to each named insured. Nothing contained herein shall operate to increase the company's limit of liability; and

"Notice of occurrences or claims under the policy shall be made to the Risk Manager of City's Harbor Department with copies to the City Attorney's Office."

C. Required Features of Coverages

Insurance procured by Consultant in connection with this Article 10 shall include the following features:

(1) Acceptable Evidence and Approval of Insurance

Electronic submission is the required method of submitting Consultant's insurance documents. Consultant's insurance broker or agent shall register with the City's online insurance compliance system **KwikComply** at https://kwikcomply.org/ and submit the appropriate proof of insurance on Consultant's behalf.

(2) Carrier Requirements

All insurance which Consultant is required to provide pursuant to this Agreement shall be placed with insurance carriers authorized to do business in the State of California and which are rated A-, VII or better in Best's Insurance Guide. Carriers without a Best's rating shall meet comparable standards in another rating service acceptable to City.

(3) Notice of Cancellation

For each insurance policy described above, Consultant shall give a 10-day prior notice of cancellation or reduction in coverage for nonpayment of premium, and a 30-day prior notice of cancellation or reduction in coverage for any other reason, by written notice via registered mail and addressed to the City of Los Angeles Harbor Department, Attn: Risk Manager and the City Attorney's Office, 425 S. Palos Verdes Street, San Pedro, California 90731.

(4) Modification of Coverage

Executive Director, at his or her sole reasonable discretion, based upon

recommendation of independent insurance consultants to City, may increase or decrease amounts and types of insurance coverage required hereunder at any time during the term hereof by giving ninety (90) days' prior written notice to Consultant.

(5) Renewal of Policies

Prior to the expiration of any policy required by this Agreement, Consultant shall renew or extend such policy in accordance with the requirements of this Agreement and direct their insurance broker or agent to submit to the City's online insurance compliance system **KwikComply** at https://kwikcomply.org/ a renewal endorsement or renewal certificate or, if new insurance has been obtained, evidence of insurance as specified above.

D. Right to Self-Insure

Upon written approval by the Executive Director, Consultant may self-insure if the following conditions are met:

1. Consultant has a formal self-insurance program in place prior to execution of this Agreement. If a corporation, Consultant must have a formal resolution of its board of directors authorizing self-insurance.

2. Consultant agrees to protect the City, its boards, officers, agents and employees at the same level as would be provided by full insurance with respect to types of coverage and minimum limits of liability required by this Agreement.

3. Consultant agrees to defend the City, its boards, officers, agents and employees in any lawsuit that would otherwise be defended by an insurance carrier.

4. Consultant agrees that any insurance carried by Department is excess of Consultant's self-insurance and will not contribute to it.

5. Consultant provides the name and address of its claims administrator.

6. Consultant submits its most recently filed 10-Q and its 10-K or audited annual financial statements for the three most recent fiscal years prior to Executive Director's consideration of approval of self-insurance and annually thereafter.

7. Consultant agrees to inform Department in writing immediately of any change in its status or policy which would materially affect the protection afforded Department by this self-insurance.

8. Consultant has complied with all laws pertaining to self-insurance.

E. Accident Reports

Consultant shall report in writing to Executive Director within fifteen (15) calendar days after it, its officers or managing agents have knowledge of any accident or occurrence involving death of or injury to any person or persons, or damage in excess of Five Hundred Dollars ($500.00) to property, occurring upon the premises, or elsewhere within the Port of Los Angeles if Consultant's officers, agents or employees are involved in such an accident or occurrence. Such report shall contain to the extent available (1) the name and address of the persons involved, (2) a general statement as to the nature and extent of injury or damage, (3) the date and hour of occurrence, (4) the names and addresses of known witnesses, and (5) such other information as may be known to Consultant, its officers or managing agents.

11. TERMINATION PROVISION

The Board of Harbor Commissioners, in its sole discretion, shall have the right to terminate and cancel all or any part of this Agreement for any reason upon giving the Consultant ten (10) days' advance, written notice of the Board's election to cancel and terminate this Agreement. It is agreed that any Agreement entered into shall not limit the right of the City to hire additional consultants or perform the services described in this Agreement either during or after the term of this Agreement. The City will be obligated to compensate the Consultant for any services rendered and equipment delivered up until the effective date of termination.

12. PERSONAL SERVICE AGREEMENT

A. During the term hereof, Consultant agrees that it will not enter into other contracts or perform any work without the written permission of the Executive Director where the work may conflict with the interests of the Department.

B. Consultant acknowledges that it has been selected to perform the Scope of Work because of its experience, qualifications and expertise. Any assignment or other transfer of this Agreement or any part hereof shall be void provided, however, that Consultant may permit Subconsultant(s) to perform portions of the Scope of Work in accordance with Article 1. All Subconsultants whom Consultant utilizes, however, shall be deemed to be its agents. Subconsultants' performance of the Scope of Work shall not be deemed to release Consultant from its obligations under this Agreement or to impose any obligation on the City to such Subconsultant(s) or give the Subconsultant(s) any rights against the City.

13. AFFIRMATIVE ACTION

The Consultant, during the performance of this Agreement, shall not discriminate in its employment practices against any employee or applicant for employment because of employee's or applicant's race, religion, national origin, ancestry, sex, age, sexual orientation, disability, marital status, domestic partner status, or medical condition. The provisions of Section 10.8.4 of the Los Angeles Administrative Code shall be incorporated and made a part of this Agreement. All subcontracts awarded shall contain a like

nondiscrimination provision. See Exhibit C.

14. SMALL/VERY SMALL BUSINESS ENTERPRISE PROGRAM AND LOCAL BUSINESS PREFERENCE PROGRAM

It is the policy of the Department to provide Small Business Enterprises (SBE), Very Small Business Enterprises (VSBE) and Minority-Owned, Women-Owned, Disabled Veteran Business Enterprises and all Other Business Enterprises (MBE/WBE/DVBE/OBE) an equal opportunity to participate in the performance of all City contracts in all areas where such contracts afford such participation opportunities. Consultant shall assist the City in implementing this policy and shall use its best efforts to afford the opportunity for SBEs, VSBEs, MBEs, WBEs, DVBEs, and OBEs to achieve participation in subcontracts where such participation opportunities present themselves and attempt to ensure that all available business enterprises, including SBEs, VSBEs, MBEs, WBEs, DVBEs, and OBEs, have equal participation opportunity which might be presented under this Agreement. See Exhibit D.

It is also the policy of the Department to support an increase in local and regional jobs. The Department's Local Business Preference Program aims to benefit the Southern California region by increasing jobs and expenditures within the local and regional private sector. Consultant shall assist the City in implementing this policy and shall use its best efforts to afford the opportunity for Local Business Enterprises to achieve participation in subcontracts where such participation opportunities present themselves.

Prior to being awarded a contract with the City, Consultant and all Subconsultants must be registered on the City's Contracts Management and Opportunities Database, Regional Alliance Marketplace for Procurement (RAMP), at http://www.RAMPLA.org. Consultant shall comply with all RAMP reporting requirements set forth in Executive Directive No. 35 (August 25, 2022), *Equitable Access to Contracting Opportunities*, during the term of this Agreement.

15. CONFLICT OF INTEREST

It is hereby understood and agreed that the parties to this Agreement have read and are aware of the provisions of Section 1090 et seq. and Section 87100 et seq. of the California Government Code relating to conflict of interest of public officers and employees, as well as the Los Angeles Municipal Code (LAMC) Municipal Ethics and Conflict of Interest provisions of Section 49.5.1 et seq. and the Conflict of Interest Codes of the City and the Department. All parties hereto agree that they are unaware of any financial or economic interest of any public officer or employee of City relating to this Agreement. Notwithstanding any other provision of this Agreement, it is further understood and agreed that if such financial interest does exist at the inception of this Agreement, City may immediately terminate this Agreement by giving written notice thereof.

During the term of this Agreement, Consultant shall inform the Department in writing when Consultant, or any of its Subconsultants, employs or hires in any capacity, and for any length of time, a person who has worked for the Department as a

Commissioner, officer or employee. Said notice shall include the individual's name and current position and their prior position and years of employment with the Department. Written notice shall be provided by Consultant to the Department within thirty (30) days of the employment or hiring of the individual.

16. COMPLIANCE WITH APPLICABLE LAWS

Consultant shall at all times in the performance of its obligations comply with all applicable laws, statutes, ordinances, rules and regulations, and with the reasonable requests and directions of Executive Director.

17. GOVERNING LAW / VENUE

This Agreement shall be governed by and construed in accordance with the laws of the State of California, without reference to the conflicts of law, rules and principles of such State. The parties agree that all actions or proceedings arising in connection with this Agreement shall be tried and litigated exclusively in the State or Federal courts located in the County of Los Angeles, State of California, in the judicial district required by court rules.

18. TRADEMARKS, COPYRIGHTS, AND PATENTS

Consultant agrees to save, keep, hold harmless, protect and indemnify the City and any of its officers or agents from any damages, cost, or expenses in law or equity from infringement of any patent, trademark, service mark or copyright of any person or persons, or corporations in consequence of the use by City of any materials supplied by Consultant in the performance of this Agreement.

19. CONFIDENTIAL AND PROPRIETARY INFORMATION

During the term of this Agreement, the Parties may provide each other with Confidential Information. The term "Confidential Information" means any information that is disclosed in written, graphic, verbal, or machine-recognizable form, and is marked, designated, or identified at the time of disclosure as being confidential or its equivalent; or if the information is in verbal form, it is either (a) identified as confidential at the time of disclosure and is confirmed in writing within thirty (30) days of the disclosure, or (b) is sensitive information related to City's system security or by the nature of the information should reasonably be treated as confidential even if it is not so marked. Confidential Information does not include any information that: is or becomes publicly known through no wrongful act of the receiving Party; is already known to the receiving Party without restriction when it is disclosed; is or becomes, rightfully and without breach of this Agreement, in the receiving Party's possession without any obligation restricting disclosure; is independently developed by the receiving Party without breach of this Agreement; or is explicitly approved for release by written authorization of the disclosing Party.

Each Party will: maintain the confidentiality of the other Party's Confidential Information and not disclose it to any third party, except as authorized by the disclosing

Party in writing or as required by a court of competent jurisdiction; restrict disclosure of Confidential Information to its employees who have a "need to know" and not copy or reproduce the Confidential Information; take necessary and appropriate precautions to guard the confidentiality of Confidential Information, including informing its employees who handle the Confidential Information that it is confidential and not to be disclosed to others, but those precautions will be at least the same degree of care that the receiving Party applies to its own confidential information and will not be less than reasonable care; and use the Confidential Information only in furtherance of the performance of this Agreement. Confidential Information is and will at all times remain the property of the disclosing Party, and no grant of any proprietary rights in the Confidential Information is given or intended, including any express or implied license, other than the limited right of the recipient to use the Confidential Information in the manner and to the extent permitted by this Agreement.

Motorola, the third-party manufacturer of any equipment, and the copyright owner of any software own and retain all of their respective intellectual property rights in the equipment and software, and nothing in this Agreement is intended to restrict their intellectual property rights. All intellectual property developed, originated, or prepared by Motorola in connection with providing to City the services remain vested exclusively in Motorola, and this Agreement does not grant to City any shared development rights of intellectual property. Except as explicitly provided in the Software License Agreement, if applicable, Motorola does not grant to City, either directly or by implication, estoppel, or otherwise, any right, title or interest in Motorola's intellectual property rights. City will not modify, disassemble, peel components, decompile, or otherwise reverse engineer or attempt to reverse engineer, derive source code or create derivative works from, adapt, translate, merge with other software, reproduce, or export the Software, or permit or encourage any third party to do so. The preceding sentence does not apply to Open Source Software which is governed by the standard license of the copyright owner

20. CONFIDENTIALITY

The data, documents, reports, or other materials which contain information relating to the review, documentation, analysis and evaluation of the work described in this Agreement and any recommendations made by Consultant relative thereto shall be considered Confidential Information and shall not be reproduced, altered, used or disseminated by Consultant or its employees or agents in any manner except and only to the extent necessary in the performance of the work under this Agreement. In addition, Consultant is required to safeguard such information from access by unauthorized personnel.

21. NOTICES

In all cases where written notice is to be given under this Agreement, service shall be deemed sufficient if said notice is deposited in the United States mail, postage prepaid. When so given, such notice shall be effective from the date of mailing of the same. For the purposes hereof, unless otherwise provided by notice in writing from the respective parties, notice to the Department shall be addressed to Executive Director of the Los Angeles Harbor Department, P.O. Box 151, San Pedro, California 90733-0151, and notice to Consultant shall be addressed to it at the address set forth above. Nothing

herein contained shall preclude or render inoperative service of such notice in the manner provided by law.

22. TAXPAYER IDENTIFICATION NUMBER (TIN)

The Internal Revenue Service (IRS) requires that all consultants and suppliers of materials and supplies provide a TIN to the party that pays them. Consultant declares that it has an authorized TIN which shall be provided to the Department prior to payment under this Agreement. No payments will be made under this Agreement without a valid TIN.

23. SERVICE CONTRACTOR WORKER RETENTION POLICY AND LIVING WAGE POLICY REQUIREMENTS

The Board of Harbor Commissioners of the City of Los Angeles adopted Resolution Nos. 19-8419 and 19-8420 on January 24, 2019, adopting the provisions of Los Angeles City Ordinance No. 185356 relating to Service Contractor Worker Retention (SCWR), Section 10.36 et seq. of the Los Angeles Administrative Code, as the policy of the Department. Further, Charter Section 378 requires compliance with the City's Living Wage requirements as set forth by ordinance, Section 10.37 et seq. of the Los Angeles Administrative Code. Consultant shall comply with the policy wherever applicable. Violation of this provision, where applicable, shall entitle the City to terminate this Agreement and otherwise pursue legal remedies that may be available. Consultant does not believe that these specific living wage laws apply to this agreement. However, Consultant will ensure that any subcontractors performing the actual work will comply with the applicable provisions.

24. WAGE AND EARNINGS ASSIGNMENT ORDERS / NOTICES OF ASSIGNMENTS

The Consultant and/or any Subconsultant are obligated to fully comply with all applicable state and federal employment reporting requirements for the Consultant and/or Subconsultant's employees.

The Consultant and/or Subconsultant shall certify that the principal owner(s) are in compliance with any Wage and Earnings Assignment Orders and Notices of Assignments applicable to them personally. The Consultant and/or Subconsultant will fully comply with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignments in accordance with Cal. Family Code Sections 5230 et seq. The Consultant or Subconsultant will maintain such compliance throughout the term of this Agreement.

25. EQUAL BENEFITS POLICY

The Board of Harbor Commissioners of the City of Los Angeles adopted Resolution No. 6328 on January 12, 2005, agreeing to adopt the provisions of Los Angeles City Ordinance No. 172,908, as amended, relating to Equal Benefits, Section 10.8.2.1 et seq. of the Los Angeles Administrative Code, as a policy of the Department. Consultant shall comply with the policy wherever applicable. Violation of this policy shall entitle the City to terminate any Agreement with Consultant and pursue any and all other legal

remedies that may be available. See Exhibit E.

26. COMPLIANCE WITH LOS ANGELES CITY CHARTER SECTION 470(c)(12)

The Consultant, Subconsultants, and their Principals are obligated to fully comply with City of Los Angeles Charter Section 470(c)(12) and related ordinances, regarding limitations on campaign contributions and fundraising for certain elected City officials or candidates for elected City office if the agreement is valued at $100,000 or more and requires approval of a City elected official. Additionally, Consultant is required to provide and update certain information to the City as specified by law. Any Consultant subject to Charter Section 470(c)(12), shall include the following notice in any contract with a subconsultant expected to receive at least $100,000 for performance under this Agreement:

> Notice Regarding Los Angeles Campaign Contribution and Fundraising Restrictions
>
> As provided in Charter Section 470(c)(12) and related ordinances, you are a subconsultant on Harbor Department Agreement No. _____. Pursuant to City Charter Section 470(c)(12), subconsultant and its principals are prohibited from making campaign contributions and fundraising for certain elected City officials or candidates for elected City office for 12 months after the Agreement is signed. Subconsultant is required to provide to Consultant names and addresses of the subconsultant's principals and contact information and shall update that information if it changes during the 12 month time period. Subconsultant's information must be provided to Consultant within 10 business days. Failure to comply may result in termination of the Agreement or any other available legal remedies including fines. Information about the restrictions may be found at the City Ethics Commission's website at http://ethics.lacity.org/ or by calling 213-978-1960.

Consultant, Subconsultants, and their Principals shall comply with these requirements and limitations. Violation of this provision shall entitle the City to terminate this Agreement and pursue any and all legal remedies that may be available.

27. STATE TIDELANDS GRANTS

This Agreement is entered into in furtherance of and as a benefit to the State Tidelands Grant and the trust created thereby. Therefore, this Agreement is at all times subject to the limitations, conditions, restrictions and reservations contained in and prescribed by the Act of the Legislature of the State of California entitled "An Act Granting to the City of Los Angeles the Tidelands and Submerged Lands of the State Within the Boundaries of Said City," approved June 3, 1929 (Stats. 1929, Ch. 651), as amended, and provisions of Article VI of the Charter of the City of Los Angeles relating to such lands. Consultant agrees that any interpretation of this Agreement and the terms contained herein must be consistent with such limitations, conditions, restrictions and reservations.

28. INTEGRATION

This Agreement contains the entire understanding and agreement between the parties hereto with respect to the matters referred to herein. No other representations, covenants, undertakings, or prior or contemporaneous agreements, oral or written, regarding such matters which are not specifically contained, referenced, and/or incorporated into this Agreement by reference shall be deemed in any way to exist or bind any of the parties. Each party acknowledges that it has not been induced to enter into the Agreement and has not executed the Agreement in reliance upon any promises, representations, warranties or statements not contained, referenced, and/or incorporated into the Agreement. **THE PARTIES ACKNOWLEDGE THAT THIS AGREEMENT IS INTENDED TO BE, AND IS, AN INTEGRATED AGREEMENT.**

29. SEVERABILITY

Should any part, term, condition or provision of this Agreement be declared or determined by any court of competent jurisdiction to be invalid, illegal or incapable of being enforced by any rule of law, public policy, or city charter, the validity of the remaining parts, terms, conditions or provisions of this Agreement shall not be affected thereby, and such invalid, illegal or unenforceable part, term, condition or provision shall be treated as follows: (a) if such part, term, condition or provision is immaterial to this Agreement, then such part, term, condition or provision shall be deemed not to be a part of this Agreement; or (b) if such part, term, condition or provision is material to this Agreement, then the parties shall revise the part, term, condition or provision so as to comply with the applicable law or public policy and to effect the original intent of the parties as closely as possible.

30. CONSTRUCTION OF AGREEMENT

This Agreement shall not be construed against the party preparing the same, shall be construed without regard to the identity of the person who drafted such and shall be construed as if all parties had jointly prepared this Agreement and it shall be deemed their joint work product; each and every provision of this Agreement shall be construed as though all of the parties hereto participated equally in the drafting hereof; and any uncertainty or ambiguity shall not be interpreted against any one party. As a result of the foregoing, any rule of construction that a document is to be construed against the drafting party shall not be applicable.

31. TITLES AND CAPTIONS

The parties have inserted the Article titles in this Agreement only as a matter of convenience and for reference, and the Article titles in no way define, limit, extend or describe the scope of this Agreement or the intent of the parties in including any particular provision in this Agreement.

32. MODIFICATION IN WRITING

This Agreement may be modified only by written agreement of all parties. Any such modifications are subject to all applicable approval processes required by, without limitation, City's Charter and City's Administrative Code.

33. WAIVER

A failure of any party to this Agreement to enforce the Agreement upon a breach or default shall not waive the breach or default or any other breach or default. All waivers shall be in writing.

34. EXHIBITS; ARTICLES

All exhibits, including the terms and conditions in Consultant's July 17, 2024 Proposal attached as Exhibit A, to which reference is made in this Agreement are deemed incorporated in this Agreement, whether or not actually attached. To the extent the terms of an exhibit conflict with or appear to conflict with the terms of the body of the Agreement, the terms of the body of the Agreement shall control. References to Articles are to Articles of this Agreement unless stated otherwise.

35. COUNTERPARTS

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which shall constitute together one and the same instrument.

////

////

(Signature page follows)

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the date to the left of their signatures.

THE CITY OF LOS ANGELES, by its Board of Harbor Commissioners

By signing below, I attest that I have no personal, financial, beneficial, or familial interest in this Agreement.

Dated: _____, 2025

By: _____
EUGENE D. SEROKA
Executive Director

Attest: _____
AMBER M. KLESGES
Board Secretary

MOTOROLA SOLUTIONS, INC.

Dated: _____, 2025

By: _____
Jerry Burch, MSSSI Vice President
(Print/type name and title)

By: _____
Ryan Christensen, Assistant Corporate Secretary
(Print/type name and title)

APPROVED AS TO FORM AND LEGALITY

1/22, 2025
HYDEE FELDSTEIN SOTO, City Attorney
STEVEN Y. OTERA, General Counsel

By: _____
JOHN T. DRISCOLL, Deputy

JTD:mc
Attachments

Date: November 22, 2024

Contractor/Vendor Name: Motorola Solutions, Inc.

Account# 542000/542025 W.O. #

Ctr/Div 52010 Job Fac.#

Proj/Prog# 60000044 (starting in FY26)

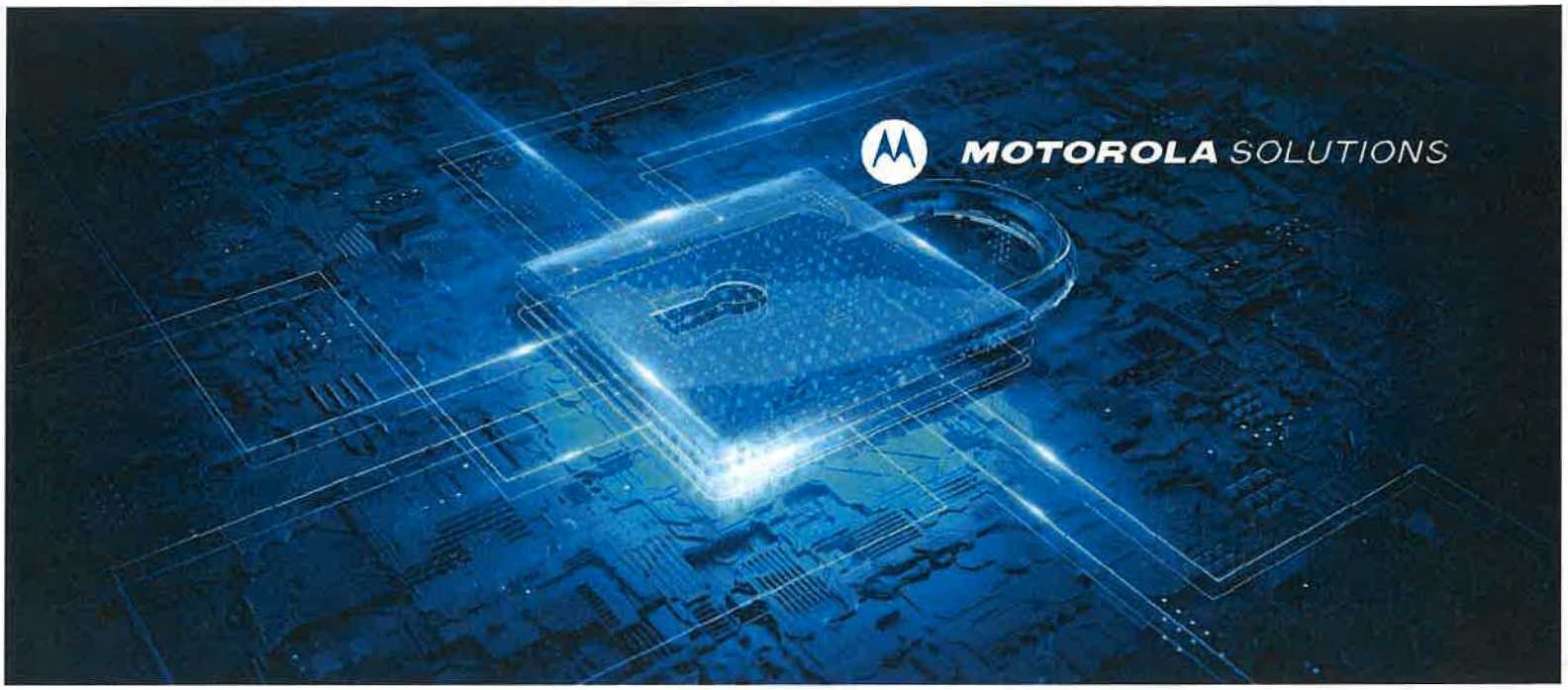
Account	FY24/25:	FY25/26	FY26/27	**Total**
542000	265,919.41	161,115.21	167,559.82	**594,594.44**
542025	316,480.00	130,790.40	136,022.03	**583,292.43**
Total	**582,399.41**	**291,905.61**	**303,581.85**	**1,177,886.87**

For Acct/Budget Div. Use Only

Verified by: Melody M. Ugalde Melody Ugalde 2024.11.25 13:40:29 -08'00'

Verified Funds Available: Digitally signed by Frank Liu Date: 2024.11.25 15:30:13 -08'00'

Date Approved: 11/25/24



Firm Fixed Price Proposal

Port of Los Angeles

Cybersecurity Managed Detection & Response and Professional Services

24-175548 / ASTRO 25 and PremierOne

July 17, 2024

Table of Contents

MOTOROLA SOLUTIONS

Motorola Solutions, Inc.
500 W Monroe Street, Ste 4400
Chicago, IL 60661-3781
USA

July 17, 2024

Captain Daniel R. Cobos
Commanding Officer, Support Services Division
425 South Palos Verdes Street
San Pedro, CA 90731

RE: ASTRO® 25 and PremierOne Managed Detection & Response and Professional Services

Dear Mr. Cobos,

Motorola Solutions, Inc. (Motorola) appreciates the opportunity to provide Port of Los Angeles quality cybersecurity services. Motorola's project team has taken great care to propose a solution to address your needs and provide exceptional value to Port of Los Angeles through the following:

- Providing a market leading MDR solution for each of Port of Los Angeles' networks (ASTRO®, PremierOne) with Motorola's SOAR platform, known as ActiveEye
- Providing geographically redundant Security Operations Centers (SOC) operating 24 hours a day, 7 days per week, 365 days per year
- Notifying Port of Los Angeles of active threats and the activities used to detect/investigate possible threats through threat hunting services
- Conducting Cybersecurity Advisory services to achieve a lower risk profile and increased cyber resilience

We are confident that Motorola can provide a best in class premier offering of MDR and risk mitigation services to Port of Los Angeles. Motorola Solutions' proposal is conditioned upon Port of Los Angeles acceptance of the terms and conditions included with this proposal, or a mutually negotiated version thereof. This proposal shall remain valid until December 15, 2024. Any questions Port of Los Angeles has regarding this proposal can be directed to Andrew Gretencord, Cybersecurity Account Manager at 317-201-7903 or by email at andrew.gretencord@motorolasolutions.com. The Port of Los Angeles may accept this solution by returning a signed copy of this proposal to Motorola.

Our goal is to provide you with the best products and services available in the industry to address your ongoing Cybersecurity needs. We thank you for the opportunity to provide this proposal for Managed Detection and Response and Professional Services for Port of Los Angeles, and we hope to strengthen our relationship by implementing this project.

Sincerely,

Jim Nelson

Vice President (MSSSI), & Director of Cybersecurity Services
MOTOROLA SOLUTIONS, INC.

Section 1

Executive Summary

Motorola is pleased to build upon our years of ongoing support to Port of Los Angeles with a response that efficiently meets the needs for your ASTRO® 25 Managed Detection and Response (MDR) solution. We are a national and global leader in the cybersecurity community with our recent acquisitions of both Delta Risk and Lunarline in 2020. We have evolved into a holistic mission critical technology provider, placing Information Technology (IT), as well as cybersecurity, at the forefront of importance to protect our customers against threats to the confidentiality, integrity and availability of their operation.

ASTRO 25 Managed Detection and Response

Motorola's ASTRO 25 MDR provides radio network security element monitoring by experienced, specialized security technologists with extensive experience working with ASTRO 25 mission-critical networks. For highly complex or unusual security events, Motorola's technologists have direct access to Motorola engineers for rapid resolution.

Our solution provides 24x7x365 Security Operations Center Support. This is a component of our broader proprietary SOC 2 Type 2 certified Managed Security Platform targeted to Public Safety, Critical Infrastructure, and State/Local municipalities.

Cybersecurity Advisory Services

Motorola's Cybersecurity Advisory Services provides recommendations for our customers to leverage processes and systems to achieve a lower risk profile and increased cyber resilience. Our services deliver this through assessments utilizing the industry-standard cybersecurity frameworks, vulnerability scanning, and system configuration reviews.

Cybersecurity Advisory Services recommendations are in alignment with the following control sets:

- Criminal Justice Information Services (CJIS) Security Policy
- National Institute of Standards and Technology (NIST) SP800-53r5
- Center for Internet Security (CIS) Common Security Controls (CSC)
- Health Insurance Portability and Accountability Act (HIPAA)
- International Standards Organization (ISO) 27001

The ActiveEye℠ Platform

In 2020, Motorola acquired Delta Risk, a leading Managed Security Services Provider (MSSP). The acquisition now allows Motorola to extend the ActiveEye℠ platform to our customers and deliver a co-managed approach to 24/7 security monitoring operations across IT enterprise environments. The benefits of the ActiveEye℠ platform are demonstrated below:

- **Included Public Safety Threat Data Feed** — Threat reports covering potential attack vectors based on dark web research. Summaries of actual attacks against public safety and state/local municipalities. Indicator data pulled from a large network of deployed public safety sensors and state/local municipality environments.

- **Advanced Threat Detection & Response** — Consolidate SIEM data and direct threat inputs from endpoint security, network sensors, and cloud/SaaS applications. Pre-built custom playbooks to process alerts and reduce/eliminate manual analyst effort.
- **Single Dashboard for Threat Visibility** — Prioritize based on actual assets in the environment. Asset inventory created manually or automatically with Managed Vulnerability Assessment Service - external and authenticated scans of assets, providing a complete attack surface map.

Chief Information Security Officer (CISO) Benefits

Main dashboard displays and aggregates all of the important and relevant risk information from across the organization, helping decision makers to make better-informed decisions to balance cybersecurity efforts and operational efficiencies.

Main dashboard provides key performance metrics and indicators that can inform an admin at a glance to the activity that is occurring throughout their environment.

Create ad-hoc reports and notifications based on available data and ActiveEye^{SM} parameters.

Transparency into the service that Motorola is providing. The dashboard will provide the key indicators to the number of events that are handled on a daily, weekly, monthly basis and how those events are handled by the Motorola Security Operations Center (SOC).

Public Safety Threat Alliance

Cyber threats to public safety agencies are increasing in scope, scale, and complexity; however, most agencies lack the cybersecurity capabilities required to mitigate risk and ensure continuity of public safety operations. To address this critical need, Motorola has established a cyber threat information sharing and analysis organization (ISAO) for public safety called The Public Safety Threat Alliance (PSTA). The PSTA is recognized by the U.S. Cybersecurity and Infrastructure Security Association (CISA), and highlights Motorola's commitment to public safety agencies and the communities they serve.

The PSTA will leverage cybersecurity risk information from across Motorola's Cybersecurity Services. This, paired with information from members and trusted partners including CISA, other ISAOs, and nonprofits dedicated to sharing cyber threat intelligence, will help generate actionable intelligence to improve members' cybersecurity posture, defense, and resilience against evolving threats to their public safety missions. In addition to the intelligence alerts and reports provided, other benefits included access to an automated threat feed, with context and tags, that can be fed into your SIEM or MDR solution and Dark Web monitoring that checks for activity, including the sale of credentials or mention of your organization's name. There is no cost for membership to the PSTA.

Learn more about membership to the PSTA at: https://motorolasolutions.com/public-safety-threat-alliance.

PSTA
Public Safety Threat Alliance
Public Safety ISAO

ABOUT MOTOROLA

Company Background and History

Motorola creates innovative, mission-critical communication solutions and services that help public safety and commercial customers build safer cities and thriving communities. You can find our products at work in a variety of industries including law enforcement, fire, emergency medical services, national government security, utilities, mining, energy, manufacturing, hospitality, retail, transportation and logistics, education, and public services. Our communication solutions span infrastructure, devices, services and software to help our public safety and commercial customers be more effective and efficient.

OUR VALUES

WE ARE INNOVATIVE

WE ARE PASSIONATE

WE ARE DRIVEN

WE ARE ACCOUNTABLE

WE ARE PARTNERS

Company Overview

Since 1928, Motorola Solutions, Inc. (formerly Motorola, Inc.) has been committed to innovation in communications and electronics. Our company has achieved many milestones in its history. We pioneered mobile communications in the 1930s with car radios and public safety networks. We made the equipment that carried the first words from the moon in 1969. We commercialized the first handheld portable scanner in 1980. Today, as a global industry leader, excellence in innovation continues to shape the future of the Motorola brand.

We help people be their best in the moments that matter.

Motorola connects people through technology. Public safety and commercial customers around the world turn to Motorola innovations when they want highly connected teams that have the information they need throughout their workdays and in the moments that matter most to them.

Our customers rely on us for the expertise, services, and solutions we provide, trusting our years of invention and innovation experience. By partnering with customers and observing how our products can help in their specific industries, we are able to enhance our customers' experience every day.

Motorola's Corporate Headquarters is located at 500 West Monroe Street, Chicago, IL 60661. Telephone is +1 847.576.5000, and the website is www.motorolasolutions.com.

Section 2

Solution Description – ASTRO MDR

2.1 Solution Overview

Motorola Solutions, Inc. (Motorola) is pleased to present the proposed cybersecurity Managed Detection and Response (MDR) services for Port of Los Angeles (hereinafter referred to as "Customer").

Identifying and mitigating cyber threats requires a reliable solution that supplies the right data to cybersecurity experts. Motorola will provide access to our ActiveEye℠ Security Platform, along with 24x7 support from specialized security technologists, who will monitor your mission critical network against threat and intrusion.

The following ASTRO® 25 MDR features and services are included in our proposal:

- **ActiveEye℠ Managed Detection and Response Elements**
  - ActiveEye℠ Security Management Platform
  - ActiveEye℠ Remote Security Sensor (AERSS)
- **Service Modules**
  - Log Collection / Analytics
  - Network Detection
  - Attack Surface Management
- **Security Operations Center Monitoring and Support**

2.1.1 Site Information

The following site information is included in the scope of our proposal:

Table 2-1: Site Information

Site / Location	Quantity
Core Site	1
DSR	1
Control Room CEN	1
Co-located CEN	1
Network Management Clients	4
Dispatch Consoles	11
AIS	1
CEN Endpoints	20

Services Included

The ActiveEye℠ service modules included in our proposal are shown in the tables below. The **Network Environment** column will designate the location of each module: ASTRO 25 Radio Network Infrastructure (RNI), Customer Enterprise Network (CEN), or the Control Room CEN.

Table 2-2: Service Modules

Service Module	Features Included	Network Environment
Log Collection / Analytics	Online Storage Period: 30 Day Storage Extended Log Storage Length: 12 Months	RNI CEN
Network Detection	Up to 1 Gbps per sensor port	RNI CEN
Attack Surface Management	Features in Section 3.2.3.3	RNI CEN

2.2 Service Description

Managed Detection and Response is performed by Motorola's Security Operations Center (SOC) using the ActiveEye℠ security platform. The SOC's cybersecurity analysts monitor for alerts 24x7x365. If a threat is detected, analysts will investigate and initiate an appropriate Customer engagement. Customer engagements may include, but are not limited to: requesting additional information from the Customer, continuing to monitor the event for further development, or informing the Customer to enact the Customer's documented Incident Response plan.

SOC analysts rely on monitoring elements to detect signs of a potential threat impacting the Customer's ASTRO 25 network and applicable Customer Enterprise Network (CEN) systems. These elements are described below.

The MDR service includes the deployment and optimization of these elements into the Customer's network.

2.2.1 Managed Detection and Response Elements

This section and its subsections describe Managed Detection and Response elements, and their applicability for specific infrastructure.

2.2.1.1 ActiveEye℠ Security Platform

Motorola's ActiveEye℠ security platform collects and analyzes security event streams from ActiveEye℠ Remote Security Sensors (AERSS) in the Customer's ASTRO 25 network and applicable CEN systems, using security orchestration and advanced analytics to identify the most important security events from applicable systems. The ActiveEye platform is provided in the English language.

The platform automates manual investigation tasks, verifies activity with external threat intelligence sources, and learns what events will require rapid response action.

The Customer will receive access to the ActiveEye[SM] platform as part of this service. ActiveEye[SM] will serve as a single interface to display system security information. Using ActiveEye[SM], the Customer will be able to configure alerts and notifications, review security data, and perform security investigations.

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

2.2.1.2 ActiveEye[SM] Managed Security Portal

The ActiveEye[SM] Managed Security Portal will synchronize security efforts between the Customer and Motorola. From this central point, the Customer will be able to view threat insights, event investigations, security reports, threat advisories, and status of any security cases.

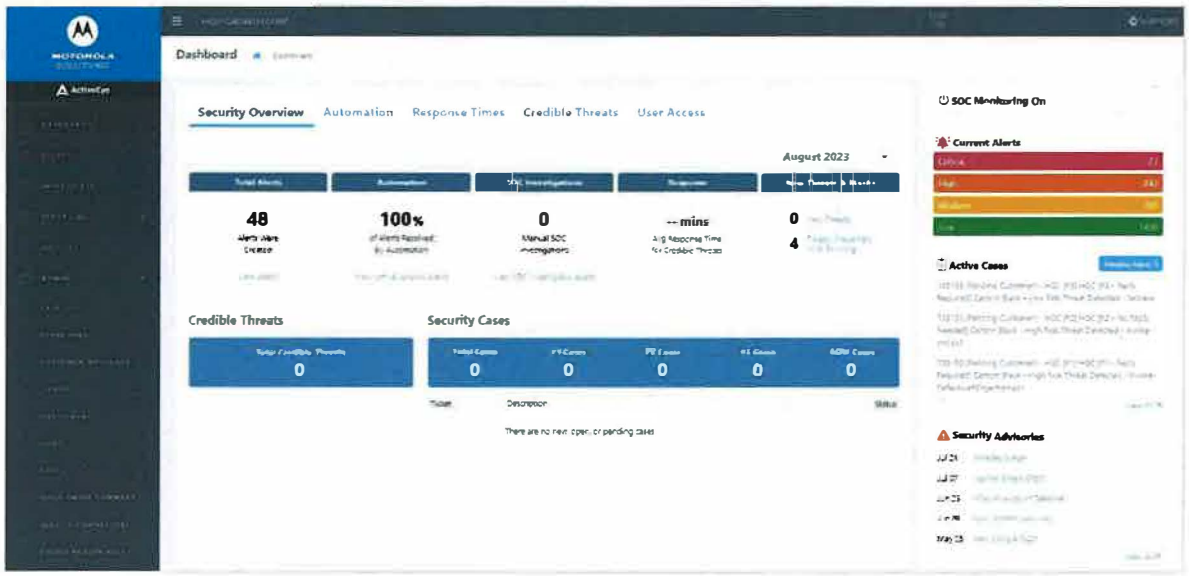


Figure 2-1: ActiveEye[SM] Portal

Dashboard

Key information in the ActiveEye[SM] Portal is summarized on the dashboard. This dashboard provides details about open alerts, an overview of alert categories, alert processing, key performance indicators (KPI), open security cases, and recent threat advisories. Also, users can access more in-depth information like security cases, alert details, alert trends, reports, and group communications.

Security Cases

When the Customer and Motorola identify a threat, the SOC will create a security case. Through the ActiveEye[SM] Portal, the Customer can view details of current or past cases, create new cases, or respond to ongoing cases.

Alert Details and Trends

Alerts can be evidence of a past, active, or developing threat. ActiveEye[SM] records relevant data for each alert, enabling users to quickly view its triggers, systems it impacts, and any actions taken to address the alert. ActiveEye[SM] Portal also provides tools for reviewing groups of alerts based on key attributes or time periods. Attribute filters enable users to toggle which alert groups ActiveEye[SM] Portal

shows, helping to spot trends or threat activity. Users can also compare alert logs for specific time periods to determine if specific trends are associated with a threat or are false positives.

Investigations and Reporting

ActiveEye℠ Portal includes robust *ad hoc* reporting capabilities, which will provide important, additional information about active and historical threats. Users can share information outside of ActiveEye℠ Portal by downloading reports in .csv or .json format.

In addition to *ad hoc* reporting, ActiveEye℠ Portal can provide a daily email summary and monthly report. Daily email summaries can include alert counts, security cases opened or closed, saved queries that have new data, and detailed endpoint security statistics. If needed, ActiveEye℠ Portal can send one or more summary emails with different content for different groups. Monthly reports are available as a PDF download.

Security Advisories

Security Advisories are messages initiated from the SOC that share information on active threats with the Customer's security teams. These advisories guide security teams on how to best take action against a threat and tell them where they can find further information.

Information Sharing

The ActiveEye℠ Portal includes several functions for sharing information. Automatic security alerts notify pre-defined contacts of incidents, based on incident priority. Other information sharing functions include:

- **SOC Bulletins** - Instructions from the Customer, or the SOC, that SOC analysts reference when creating security cases. These can communicate short-term situations where a security case may not be needed, such as during testing or maintenance windows.
- **Customer Notebook** - The SOC will use the Customer Notebook to document the Customer's environment and any specific network implementation details that will help the SOC investigate security cases.
- **Contact Procedures** - Escalation procedures and instructions on who to contact if an incident occurs. Contact procedures include instructions and procedures for specific security incident levels. The SOC and the Customer will jointly manage contact procedures.

User Access

The ActiveEye℠ Portal provides the ability to add, update, and remove user access. Every ActiveEye℠ user can save queries, customize reports, and set up daily email summaries. Users may be given administrative access, allowing them to perform administrative tasks, such as setting up new service connectors, resetting passwords, and setting up multi-factor authentication for other users.

2.2.1.3 ActiveEye℠ Remote Security Sensor

One or more AERSS will be deployed into the ASTRO 25 network and if applicable to CEN environments to deliver the service. These sensors monitor geo diverse sites for security events and pass security information to the ActiveEye℠ platform.

AERSS integrate the ActiveEye℠ platform with network elements, enabling it to collect logs from Syslog, as well as to analyze network traffic over port(s) and scan elements for vulnerabilities.

The following are the environmental requirements and specifications the Customer must provide to prepare for the AERSS deployment.

Specifications	Requirements
Rack Space	1U
Power Consumption (Max)	550 Watts (Redundant Power Supply)
Power Input	100-240V AC
Current	3.7 A – 7.4 A
Circuit Breaker	Qty. 2
Line Cord	NEMA 5-15P
Heat Dissipation (max)	2107 BTU/hr.
Internet Service Bandwidth	Bandwidth throughput 10Mbps per zone

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

2.2.1.4 Internetworking Firewall

Motorola introduces a formalized and centralized Internet connection to the ASTRO® 25 system using an Internetworking Firewall. The Internetworking Firewall serves as a security barrier and demarcation point between a master site and the Internet (or a customer network leading to the Internet). The Internetworking Firewall supports traffic for various ASTRO® 25 features that require access to the Internet. The Internetworking Firewall sits between the Demilitarized Zone (DMZ) and the Internet (or customer network leading to the Internet).

The following are the environmental requirements and specifications the Customer must provide to prepare for the Internetworking Firewall deployment, if one is required.

Specifications	Requirement
Rack Space	1U
Power Consumption (Max)	28.6 W (Single Power Supply)
Power Input	100-240V AC
Current	.52 A
Circuits Breaker	Qty. 1
Heat Dissipation (Max)	97.6 BTU/hr.
Line Cord	NEMA 5-15P
Internet Service Bandwidth	Bandwidth throughput 10 MB High availability Internet Connection (99.99% (4-9s) or higher). Packet loss < 0.5%. Jitter <10 ms. Delay < 120 ms. RJ45 Port Speed - Auto Negotiate

2.2.2 Service Modules

ActiveEye℠ delivers service capability by integrating one or more service modules. These modules provide ActiveEye℠ analytics more information to correlate and a clearer vision of events on Customer's network. In addition, modules enable security teams and analysts to more easily access and compare data from these disparate systems. The following subsections describe each ActiveEye℠ service module in detail.

2.2.2.1 Log Collection / Analytics

The AERSS deployed in the system collects logs and other security information from applicable servers, workstations, switches, routers, Network Detection, and firewalls. This information is forwarded to the ActiveEye℠ platform, which uses advanced analytics to identify signs of security incidents. If it identifies signs of a security incident, ActiveEye℠ notifies the SOC for further analysis.

Collected events will be stored in the ActiveEye℠ Security Management Platform to enable historical searching or threat hunting as needed. Some high volume, repetitive logs may be aggregated as noted in the documentation. The default storage time period is one year, but no longer than 90 days, following expiration or termination of the Agreement. A longer time period can be provided if subscribed, see Table 2-2: Service Modules for subscription details.

2.2.2.2 Network Detection

The AERSS supports Network Detection, constantly monitoring traffic passing across, into, or out of infrastructure. Network Detection analyzes traffic for signs of malicious activity in real time, and performs packet level and flow level analysis to enable communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including traffic using encrypted connections. Network Detection forwards detected suspicious activity to the SOC for further analysis.

2.2.2.3 Attack Surface Management

Attack Surface Management is provided for the ASTRO® internet-facing, external network interfaces. The scan is enabled from an internet cloud hosted service outside the ASTRO® network. Discovery and vulnerability scans will be run quarterly or on a less frequent schedule defined with the Customer.

2.2.3 Security Operations Center Services

Motorola delivers SOC Monitoring using one or more SOC facilities. The SOC includes any centralized hardware and software used to deliver this Service and its service modules. The SOC and its centralized hardware and software are housed within an SSAE-18 compliant data center.

Motorola's SOC is staffed with security experts who will use ActiveEye℠ Security Management Platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate and triage detected threats, and to recommend responses to the Customer.

Section 3

Statement of Work – ASTRO MDR

3.1 Overview

In accordance with the terms and conditions of the Agreement, this Statement of Work (SOW), including all of its subsections and attachments, defines the principal activities and responsibilities of all parties for the delivery of Motorola Solutions, Inc. (Motorola) Cybersecurity services as presented in this proposal to Port of Los Angeles (Customer).

Motorola's ASTRO® 25 MDR provides monitoring of radio network security information by specialized cybersecurity analysts with extensive experience working with ASTRO® 25 mission-critical networks.

The following sections describe the deliverables of the service, its technologies, and service obligations.

In order to receive the services as defined within this SOW, the Customer is required to keep the system within a standard support period as described in Motorola's Software Support Policy (SwSP). Contact your local Customer Support Manager for details.

3.2 Description of Service

3.2.1 Deployment Timeline and Milestones

The following phase descriptions lay out the necessary deployment activities and milestones required to achieve service readiness:

Phase 1: Service Onboarding

After contract signature, Motorola will schedule a service kick-off meeting with the Customer and provide information-gathering documents. This kick-off meeting is conducted remotely at the earliest, mutually available opportunity within 30 days of contract signing. Customer is to identify and ensure participation of key team members in kickoff and project initiation activities.

The Customer will be provisioned onto the ActiveEye℠ MDR portal and be able to configure key contacts for interaction with the Security Operations team. The portal will enable service notifications, access to vulnerability scans and cybersecurity advisories. The first vulnerability scan will be conducted and reported within the first 30-day period. The Customer will receive instructions for accessing the Security Operations Center and Incident Response (IR) teams within the first 30 days. Once access is provisioned, the customer will receive any assistance required from the IR team.

Phase 2: Infrastructure Readiness

Motorola will provide detailed requirements regarding Customer infrastructure preparation actions after kick-off meeting. It is the Customer's responsibility to accomplish all agreed upon infrastructure preparations. It is Motorola's responsibility to separately complete any obligated and/or agreed infrastructure readiness tasks.

Phase 3: System Buildout and Deployment

Motorola Solutions will build and provision tools in accordance with the requirements of this proposal and consistent with information gathered in earlier phases. Motorola Solutions will also provide detailed requirements regarding Customer deployment actions. The Customer may be required to deploy software and/or configurations in cases where Motorola Solutions does not manage the device and does not have access or authorization to perform the installation.

Phase 4: Monitoring "Turn Up"

Motorola will verify all in-scope assets are forwarding logs or events. Motorola will notify Customer of any exceptions. Motorola will begin monitoring any properly connected in-scope sources after the initial tuning period.

Phase 5: Tuning/Report Setup

Motorola will conduct initial tuning of the events and alarms in the service and conduct an additional ActiveEye^{SM} Portal training session.

Service Commencement

The Service will commence with the Service Onboarding phase or within 30 days of contract signature, whichever event occurs soonest for existing customers.

In the case of a new ASTRO system, the Service will commence in parallel to the commencement date of the core ASTRO Service package "Turn Up" date. Motorola and the Customer will collaborate to complete the additional deployment tasks.

3.2.2 General Responsibilities

3.2.2.1 Motorola Responsibilities

- Provide, maintain, and when necessary, repair under warranty hardware and software required to monitor the ASTRO 25 network and applicable CEN systems Inclusive of the AERSS and all software operating on it.
  - If the Centralized Event Logging feature is not installed on the Customer's ASTRO 25 RNI, Motorola will install it as part of this service.
- Coordinate with the Customer on any system changes necessary to integrate the AERSS into the system and establish necessary connectivity.
- Provide software and licenses to the Customer necessary to remotely monitor the ASTRO 25 network and applicable CEN environments.
- Verify connectivity and monitoring is active prior to start of service.
- Coordinate with the Customer to maintain Motorola service authentication credentials.
- Monitor the Customer's ASTRO 25 network and applicable CEN systems 24/7/365 for malicious or unusual activity.
- Respond to security incidents in the Customer's system in accordance with Section 3.3.6: Incident Priority Level Definitions and Response Times. This may include, but is not limited to, requesting additional information from the Customer, continuing to monitor the event for further development or informing the Customer to enact the Customer's documented Incident Response plan.

- Assist the Customer with identifying devices that support logging within the ASTRO 25 network and that applicable CEN systems have been configured to forward Syslog events to the AERSS.
- Provide the Customer with access to the ActiveEye[SM] platform enabling Customer access to security event and incident details.

3.2.2.2 Customer Responsibilities

- The ASTRO 25 MDR service requires a connection from the Customer's ASTRO 25 network and applicable CEN systems to the Internet. Establish connectivity with sufficient bandwidth before service commences. Internet service bandwidth requirements are as follows:
  - Bandwidth throughput of 10MB
  - High availability Internet Connection (99.99% (4-9s) or higher)
  - Packet loss < 0.5%
  - Jitter <10 ms
  - Delay < 120 ms
  - RJ45 Port Speed - Auto Negotiate
- Maintain an active subscription for:
  - Security Update Service (SUS) (or Remote Security Update Service), ensuring patches and antivirus definitions are applied according to the release cadence of the service.
  - ASTRO Dispatch Service and ASTRO Infrastructure Response.
- The ASTRO 25 Managed Detection and Response service requires an ASTRO 25 WAVE SUS subscription.
- If a Control Room CEN is included, it will require a static gateway IP and sufficient capacity on the switch (3 ports – 2 active connections and 1 mirror port). It is the Customer's responsibility or the contracted maintainer to install the AERSS device in the Control Room CEN.
- Allow Motorola continuous remote access to monitor the ASTRO 25 network and applicable CEN systems. This includes keeping the connection active, providing passwords, and working with Motorola to understand and maintain administration privileges.
- Provide continuous utility service(s) to any equipment installed or utilized at the Customer's premises to support service delivery and remote monitoring.
- Provide Motorola with contact information necessary to complete the Customer Support Plan (CSP). Notify the Customer's Customer Support Manager (CSM) within two weeks of any contact information changes.
- Notify Motorola if any components are added to or removed from the environment as it may be necessary to update or incorporate in Managed Detection and Response. Changes to monitored components may result in changes to the pricing of the Managed Detection and Response service.
- As necessary, upgrade the ASTRO 25 system, on-site systems, and third-party software or tools to supported releases.
- Allow Motorola's dispatched field service technicians physical access to monitoring hardware when required.

- Cooperate with Motorola and perform all acts that are required to enable Motorola to provide the services described in this SOW.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEye[SM] sensor for applicable CEN systems.
- Respond to Cybersecurity Incident Cases created by the Motorola SOC.

3.2.3 Service Modules

The following subsections describe the delivery of the service modules selected in Table 2-2: Service Modules.

3.2.3.1 Log Analytics

The AERSS deployed in the system collects logs and other security information from applicable servers, workstations, switches, routers, Network Detection, and firewalls. This information is forwarded to the ActiveEye[SM] platform, which uses advanced analytics to identify signs of security incidents. If it identifies signs of a security incident, ActiveEye[SM] notifies the SOC for further analysis.

Motorola Responsibilities

- Consult with and advise the Customer on performing necessary system configurations to direct log sources to the appropriate Remote Security Sensor.
- The SOC will consult with the Customer to identify appropriate log sources for the level of threat detection desired in each environment.

Customer Responsibilities

- If applicable, configure customer-managed networking infrastructure to allow AERSS to Communicate with ActiveEye[SM] as defined.
- If applicable, configure any Customer managed devices in the CEN to forward data to ActiveEye[SM].

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

3.2.3.2 Network Detection

The AERSS deploys a Network Intrusion Detection System (NIDS), constantly monitoring traffic passing across, into, or out of infrastructure. Network Detection analyzes traffic for signs of malicious activity in real time and performs packet level and flow level analysis to enable communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including traffic using encrypted connections. Network Detection forwards detected suspicious activity to the SOC for further analysis.

Motorola Responsibilities

- Work with the Customer to integrate AERSS.
- Optimize the policies and configuration to tune out noise and highlight potential threats.
- The SOC consults with the Customer to identify the appropriate deployment of Network Detection Service Components. The SOC will monitor and update the security policy of each

sensor to tune out unnecessary alerting and flow monitoring so that the system is optimized to detect true malicious activity.

Customer Responsibilities

- If necessary, configure Customer's networking infrastructure to allow AERSS to communicate with ActiveEye℠ as defined.
- For Customer's owned CEN infrastructure, configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a port(s) on a switch) network traffic to the ActiveEye℠ sensor.
- Initiate recommended response actions when active attacks are detected.

Applies to included ASTRO 25 RNI, CEN, and Control Room CEN infrastructure.

3.2.3.3 Attack Surface Management

Attack Surface Management is provided for the ASTRO® internet-facing, external network interfaces. The scan is enabled from an internet cloud hosted service outside the ASTRO® network. Discovery and vulnerability scans will be run quarterly or on a less frequent schedule defined with the Customer.

The initial scan results will be discussed with the Customer during service onboarding. Subsequent scans will be reviewed by a cybersecurity analyst. If any new findings of interest surface, a ticket will be created to communicate these findings with the customer defined contacts.

Motorola Responsibilities

- Configure scans to match the Customer's preferences for external scope.
- Verify vulnerability scans are operating correctly.
- Make generated results available in the Customer's ActiveEye℠ portal.
- Create ticket notifications for significant, new findings of interest.

Customer Responsibilities

- During Service Onboarding kickoff, provide Motorola with the IP addresses and/or domain names to be included in the external vulnerability scans.
- In accepting this Statement of Work, the Customer authorizes Motorola to engage in external vulnerability scans of internet-facing, external assets disclosed by the Customer.
- Update Motorola with any changes to the IP addresses and/or domain names of the internet-facing, external assets subject to the external vulnerability scans.
- If the information required to enable vulnerability scanning of the internet-facing, external assets is not provided initially or is not current at any time during the term, Motorola will suspend scans until it is reasonably satisfied that it has been provided with the most current information.
- Review all quarterly vulnerability reports, and tickets of new findings.
- Perform any remediation actions required to address identified vulnerabilities.

Applies to Internet facing assets only.

3.3 Security Operations Center Monitoring and Support

3.3.1 Scope

Motorola delivers SOC Monitoring using one or more SOC facilities. The SOC includes any centralized hardware and software used to deliver this Service and its service modules. The SOC and its centralized hardware and software are housed within an SSAE-18 compliant data center.

Motorola's SOC is staffed with security experts who will use ActiveEye℠ Security Management Platform to monitor elements integrated by service modules. In addition, SOC staff will take advantage of their extensive experience to investigate, and triage detected threats, and to recommend responses to the Customer. Customer support is provided in the English language.

Motorola will start monitoring the ASTRO® 25 MDR service in accordance with Motorola processes and procedures after deployment, as described in Section 3.2.1: Deployment Timeline and Milestones.

The SOC receives system-generated alerts 24x7 and provides the Customer with a toll-free telephone number and email address for support requests, available 24x7. Support requests are stored in a ticketing system for accountability and reporting. The SOC will respond to detected events in accordance with Section 3.3.6: Incident Priority Level Definitions and Response Times.

3.3.2 Ongoing Security Operations Center Service Responsibilities

Motorola Responsibilities

If a probable security incident is detected, provide phone and email support to:

- Engage the Customer's defined Incident Response Process.
- Gather relevant information and attempt to determine the extent of compromise using existing monitoring capabilities in place as part of the ASTRO 25 MDR service.
- Analysis and support to help the Customer determine if the Customer's corrective actions are effective.
- Continuous monitoring, in parallel with analysis, to support incident response.

Customer Responsibilities

- Provide Motorola with accurate and up-to-date information, including the name, email, landline telephone numbers, and mobile telephone numbers for all designated, authorized Customer escalation Points of Contact (PoC).
- Provide a timely response to SOC security incident tickets or investigation questions.
- Notify Motorola at least 24 hours in advance of any scheduled maintenance, network administration activity, or system administration activity that would affect Motorola's ability to perform the Managed SOC Service, as described in this SOW.

3.3.3 Technical Support

ActiveEye℠ Security Management Technical Support provides the Customer with a toll-free telephone number and email address for ActiveEye℠ Security Management support requests, available Monday through Friday from 8am to 7pm CST.

Motorola Responsibilities

- Notify Customer of any scheduled maintenance or planned outages.
- Provide technical support, security control, and service improvements related to ActiveEye[SM].

Customer Responsibilities

- Provide sufficient information to allow Motorola technical support agents to diagnose and resolve the issue.

Limitations and Exclusions

Technical support is limited to the implementation and use of the ActiveEye[SM] Security Management platform and does not include use or implementation of third-party components.

3.3.4 Incident Response

An Indicator of Compromise (IoC) is an observable event that Motorola Security Analysts have determined will jeopardize the confidentiality, integrity, or availability of the system. Examples of IoC include ransomware or malicious use of PowerShell.

When an IoC is observed, the Motorola Security Operations team will engage with the customer to investigate the issue, determine the extent of the compromise and contain the activity to the extent possible with the Motorola security controls deployed within the environment. This expert guidance is available upon contract signature and extends through MDR infrastructure deployment phases and the term of the contract.

When an IoC is observed by the Security Analyst, Motorola and Customer will be responsible for the tasks defined in the following subsections.

Motorola Responsibilities

- Upon the identification of an IoC, notify the Customer's documented contact and initiate the escalation plan.
- Take documented, Customer approved actions in an attempt to contain an IoC to the extent enabled via Motorola managed technology. Communicate to the Customer any additional potential containment actions and incident response resources that can be taken across the Customer's managed IT infrastructure.
- Perform investigation using the ActiveEye[SM] Managed Detection and Response integrated and enabled data sources in an initial attempt to determine the extent of an IoC.
- Document and share IoC and artifacts discovered during investigation. Motorola services exclude performing on-site data collection or official forensic capture activities on physical devices.

Customer Responsibilities

- Maintain one named PoC to coordinate regular team discussions and organize data collection and capture across the Customer and Motorola teams.
- If determined to be required by Customer, contract an Incident Response service provider to perform procedures beyond the scope of this Agreement such as forensic data capture, additional malware removal, system recovery, ransomware payment negotiation, law enforcement engagement, insurance provider communications, identify patient zero, etc.

3.3.5 Event Response and Notification

Motorola will analyze events created and/or aggregated by the Service, assess their type, and notify the Customer in accordance with the following table.

Table 3-1: Event Handling

Event Type	Details	Notification Requirement
False Positive or Benign	Any event(s) determined by Motorola Solutions to not likely have a negative security impact on the organization.	None
Event of Interest (EOI)	Any event(s) determined by Motorola Solutions to likely have a negative security impact on the organization.	Escalate to Customer in accordance with routine notification procedure. Escalate in accordance with urgent notification procedure when required by agreed-upon thresholds and SOC analysis. Notification procedures are included in Table 3-2: Notification Procedures.

Notification

Motorola will establish notification procedures with the Customer, generally categorized in accordance with the following table.

Table 3-2: Notification Procedures

Notification Procedure	Details
Routine Notification Procedure	The means, addresses, format, and desired content (within the capabilities of the installed technology) for Events of Interest. These can be formatted for automated processing, e.g., by ticketing systems.
Urgent Notification Procedure	Additional, optional means and addresses for notifications of Events of Interest that require urgent notification. These usually include telephone notifications.

Motorola will notify the Customer according to the escalation and contact procedures defined by the Customer and Motorola during the implementation process.

Tuning

Motorola will assess certain events to be environmental noise, potentially addressable configuration issues in the environment, or false positives. Motorola may recommend these be addressed by the Customer to preserve system and network resources.

Motorola will provide the Customer with the ability to temporarily suppress alerts reaching ActiveEye[SM], enabling a co-managed approach to tuning and suppressing events or alarms. The SOC may permanently suppress particular alerts and alarms if not necessary for actionable threat detection.

Tuning Period Exception

The tuning period is considered to be the first 30 days after each service module has been confirmed deployed and configured and starts receiving data. During the tuning period, Motorola may make recommendations to the Customer to adjust the configurations of their installed software so Services can be effectively delivered. Service Availability will not be applicable during the tuning period and

responses or notifications may not be delivered. However, Motorola will provide responses and notifications during this period.

Motorola may continue to recommend necessary tuning changes after this period, with no impact on Service Availability.

3.3.6 Incident Priority Level Definitions and Response Times

Priority for an alert-generated incident or EOI is determined by the ActiveEye℠ Platform analytics that process multiple incoming alert feeds, automation playbooks, and cybersecurity analyst knowledge.

Table 3-3: Priority Level Definitions and Response Times

Incident Priority	Incident Definition	Notification Time
Critical P1	Security incidents that have caused or are suspected to have caused significant damage to the functionality of Customer's ASTRO 25 system or information stored within it. Effort to recover from the incident may be significant. Examples: • Malware that is not quarantined by anti-virus. • Evidence that a monitored component has communicated with suspected malicious actors.	Response provided 24 hours, 7 days a week, including US public holidays.
High P2	Security incidents that have localized impact and may become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant. Examples: • Malware that is quarantined by antivirus. • Multiple behaviors observed in the system that are consistent with known attacker techniques.	Response provided 24 hours, 7 days a week, including US public holidays.
Medium P3	Security incidents that potentially indicate an attacker is performing reconnaissance or initial attempts at accessing the system. Effort to recover from the incident may be low to moderate. Examples include: • Suspected unauthorized attempts to log into user accounts. • Suspected unauthorized changes to system configurations, such as firewalls or user accounts. • Observed failures of security components. • Informational events. • User account creation or deletion. • Privilege change for existing accounts.	Response provided on standard business days, Monday through Friday 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.

Incident Priority	Incident Definition	Notification Time
Low P4	These are typically service requests from the Customer.	Response provided on standard business days, Monday through Friday from 8:00 a.m. to 5:00 p.m. CST/CDT, excluding US public holidays.

3.3.6.1 Response Time Goals

Priority	Response Time
Critical P1	An SOC Cybersecurity Analyst will make contact with the customer technical representative within one (1) hour of the request for support being logged in the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.
High P2	An SOC Cybersecurity Analyst will make contact with the customer technical representative within four (4) hours of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action. Continual effort will be maintained to identify the extent of the incident and provide actions for containment.
Medium P3	An SOC Cybersecurity Support Engineer will make contact with the customer technical representative within the next business day of the request for support being logged at the issue management system or the creation of an alert suggesting a cybersecurity incident that requires action.
Low P4	An SOC Cybersecurity Support Engineer will make contact with the Customer technical representative within seven business days of the logged request for support at the issue management system.

3.3.6.2 ActiveEye℠ Platform Availability

The platform utilizes a multi-zone architecture which can recover from failures in different data collection, enhancement, analysis, and visualization tiers. Motorola will make commercially reasonable efforts to provide monthly availability of 99.9% for the ActiveEye℠ Platform services. Service availability is subject to limited scheduled downtime for servicing and upgrades, as well as unscheduled and unanticipated downtime resulting from circumstances or events outside of Motorola's reasonable control, such as disruptions of, or damage, to the Customer's or a third-party's information or communications systems or equipment, telecommunication circuit availability/performance between Customer sites, any on-premises core and/or between on-premises equipment and the ActiveEye℠ Platform.

3.3.6.3 ActiveEye℠ Remote Security Sensor

One or more AERSS may be deployed as part of the MDR solution. The AERSS is configured with multiple local redundancy features such as hot-swap hard disk drives in a redundant drive array configuration and dual redundant power supplies.

The AERSS and all components of ActiveEye℠ are monitored by a dedicated Site Reliability Engineering team. In cases of hardware failure of the AERSS, Motorola will provide, subject to active service subscriptions in the Customer contract, onsite services to repair the AERSS and restore

service. AERSS operation and outage troubleshooting requires network connection to the ActiveEye[SM] Platform which may be impacted by customer configuration changes, telecommunications connectivity, and/or customer network issues/outages.

Section 4

Solution Description – PremierOne MDR

4.1 Solution Overview

Motorola Solutions ("Motorola") is pleased to present the proposed cybersecurity services for Port of Los Angeles (hereinafter referred to as "Customer").

The following cybersecurity services are included in our proposal for the Customer's PremierOne system:

- **ActiveEye℠ Managed Detection & Response for PremierOne**
  - ActiveEye Remote Security Sensor (AERSS)
  - Network Detection
  - Endpoint Detection and Response
- **Motorola Security Operations Center (SOC) Services**

4.2 Services Included

The ActiveEye service modules included in our proposal are presented below

Table 4-1. Service Modules

Service Module	Features Included	Site/Environment
ActiveEye Remote Security Sensor (AERSS)	Number of sensors: 2	Customer Enterprise Environment
Network Detection	• (2) Gbps monitored across all sensors	PremierOne System
Endpoint Detection and Response (EDR)	• Carbon Black Defense + Threat Hunter • (123) EDR Total Endpoints • Online Storage Period: 30 Day Storage	**LAPP Site** PremierOne (119) CAD (6) Mobile (75) RMS (35) CommandCentral (3) **LAPP Management Server** CAD (1) Commsys (3)
Security Operations Center (SOC)	• Monitoring and Support	Service modules

4.3 Service Description

The ActiveEye Security Platform collects, manages, and analyzes security events. Built-in analytics examine multiple real-time threat intelligence feeds, reference past events, and follow playbooks to automate most actions. Analytics also prioritize events to quickly identify those that require remediation.

As a Security Orchestration, Automation and Response (SOAR) platform, ActiveEye speeds up remediation, using predefined or custom playbooks to automatically investigate and respond to threats. ActiveEye's automatic investigation capabilities include looking up threat intelligence, querying past data, adding recommended action notes to cases, and bringing event details to the main investigation screen. Its automated response capabilities include changing alert priorities, closing alerts, blocklisting files, removing files from systems or isolating hosts from the network.

This automated approach to threat identification and remediation eliminates more than 95 percent of false positives, allowing your team or our SOC analysts to shift their focus to more complex investigation and response tasks.

4.3.1 ActiveEye Managed Security Portal

The ActiveEye Security Portal, a cloud-based web application, enables improved coordination of cybersecurity efforts between your agency and Motorola Solutions. From this central platform, your agency's personnel will be able to view threat insights, event investigations, security reports, threat advisories, and the status of cases.

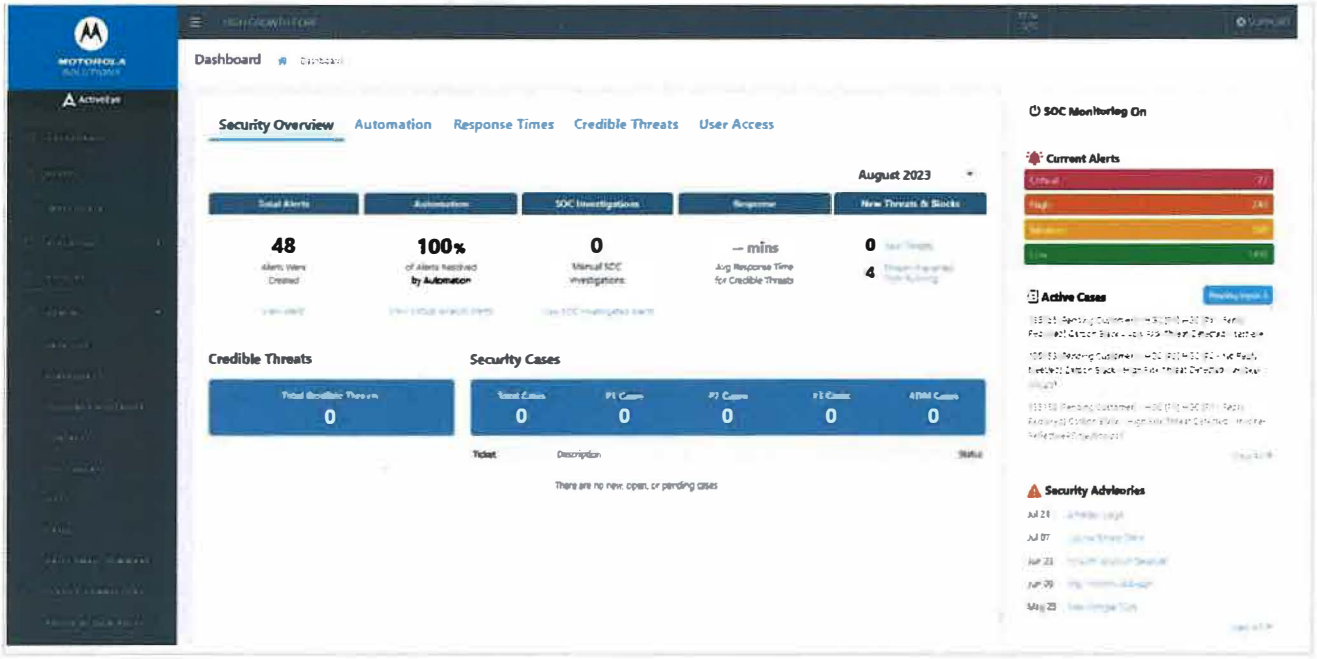


Figure 4-1 ActiveEye Portal

Dashboard

The ActiveEye dashboard provides a summary of key information It includes a snapshot of open alerts, alert categories, key performance indicators (KPI), open cases, and recent threat advisories. Users can also see more in-depth information, such as the number of security cases, alert details, alert trends, reports, and group communications.

Security Cases

When a threat is identified, the SOC will create a security case. Through the ActiveEye Portal, your agency's personnel will be able to view details of current or past cases, create new cases, or respond to ongoing cases.

Alert Details and Trends

Alerts can be evidence of a past, active, or developing threat. ActiveEye records relevant data for each alert, enabling users to quickly view its trigger, the systems it impacts, and any actions taken to address the alert.

ActiveEye also provides tools for reviewing groups of alerts based on key attributes or time periods. Attribute filters enable users to toggle which alert groups are shown in ActiveEye, helping users spot trends or threat activity. Users can also compare alert logs for specific time periods to determine if specific trends are associated with a threat or are false positives.

Investigations and Reporting

ActiveEye includes robust *ad hoc* reporting capabilities that provide important information about active and historical threats. Users can share information outside of ActiveEye by downloading reports in .csv or .json format.

In addition to *ad hoc* reporting, ActiveEye can provide a daily email summary and monthly report. Daily email summaries can include alert counts, security cases opened or closed, saved queries that have new data, and detailed endpoint security statistics. If needed, ActiveEye can send one or more summary emails with different content for different groups. Monthly reports are available as a PDF download.

Security Advisories

ActiveEye also enables the SOC to share Security Advisories on active threats. These advisories guide security teams on how to take actions against threats and where to get more information.

Information Sharing

ActiveEye includes several other functions for sharing information. Automatic security alerts notify pre-defined contacts of incidents, based on incident priority. Other information-sharing functions include:

- **SOC Bulletins** - Instructions from your agency's personnel or the SOC that analysts reference when creating security cases. These can communicate short-term situations where a security case may not be required, such as during testing or maintenance windows.
- **Customer Notebook** - The SOC will use the Customer Notebook to document your agency's environment and any specific network implementation details assisting the SOC investigation of security cases.
- **Contact Procedures** - Escalation procedures and instructions on who to contact if an incident occurs. Contact procedures include instructions and procedures for specific security incident levels. The SOC and your agency's personnel will jointly manage contact procedures.

User Access

User access settings make it simple to add, update, and remove access to ActiveEye. Users may be given administrative access, allowing them to perform administrative tasks such as setting up new service connectors, resetting passwords, and setting up multi-factor authentication for other users.

4.3.2 ActiveEye Remote Security Sensors

ActiveEye Remote Security Sensors (AERSS) integrate the ActiveEye platform with network elements, enabling it to collect logs from syslog, as well as analyze network traffic over span port connections and scan elements for vulnerabilities.

4.3.3 Service Modules

One or more service modules can be integrated through the ActiveEye platform. These modules provide more information for ActiveEye to correlate, offering a clearer vision of events on your agency's network. In addition, modules enable security teams and analysts to more easily access and compare data from disparate systems.

4.3.3.1 Network Detection

The Network Detection service module automates the investigation of network traffic alerts and allows security teams to view those alerts in the context of other user activity. To enable this feature, the ActiveEye Intrusion Detection System (IDS) is deployed within Customer's network to perform real time signature and anomaly detection. The IDS analyzes traffic for signs of malicious activity in real time. In addition, the IDS performs packet level and flow level analysis, enabling network communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including activity over encrypted connections.

The Network Detection service is enabled by one or more ActiveEye Remote Security Sensors to perform traffic analysis.

4.3.3.2 Endpoint Detection and Response

If an attacker attempts to breach your existing security controls, it is critical to respond quickly. Integrating Endpoint Detection and Response (EDR) tools with the ActiveEye platform enables security analysts to respond to attacks and view threat intelligence in a single interface. Through the ActiveEye platform, analysts can isolate hosts, block files, allow files, and remove files.

See **Table 4-1.** Service Modules for subscription details.

4.3.4 Security Operations Center Monitoring and Support

ActiveEye MDR includes ongoing monitoring by Motorola Solutions SOC cybersecurity analysts to look for potential cybersecurity threats to connected networks, applications, and devices on a 24/7 basis. The SOC team operates from secure, redundant locations in the United States, and can securely operate at remote locations if necessary. Team members complete regular training on customer data management and privacy to protect sensitive customer data. Based on their broad security experience, the SOC's analysts will recommend security device configurations and implement playbooks to increase focus on the most critical threats.

If a threat investigation requires input from your agency's security team, the SOC will create a security case and follow defined escalation procedures for each priority level. ActiveEye will enable your agency's personnel to view security cases and event investigation history.

In the event of a potential incident, the SOC will use data available in ActiveEye and access your agency's system to determine the extent of malicious activity. If needed, the SOC will add more detection policies to your agency's service modules.

Section 5

Statement of Work – PremierOne MDR

In accordance with the terms and conditions of the Agreement, this Statement of Work (SOW), including all of its subsections and attachments, defines the principal activities and responsibilities of all parties for the delivery of Motorola Solutions ("Motorola") cybersecurity services as presented in this proposal to Port of Los Angeles (hereinafter referred to as "Customer").

5.1 Project Deployment

In order to establish initial expectations for deployment, Motorola will work with Customer to help you understand the impact of introducing a new solution and your preparedness for the implementation and support of PremierOne Managed Detection and Response.

Motorola Responsibilities

- Motorola will schedule a service kick-off meeting with the Customer and provide information-gathering documents to the customer within one week of contract signature. The kick-off meeting will be conducted remotely at the earliest mutually available opportunity.
- Motorola will provide detailed requirements regarding Customer infrastructure preparation actions within one week of the kick-off meeting.
- Motorola will provision tools in accordance with the requirements of this Service, and consistent with information gathered in earlier phases. Motorola will also provide detailed, required Customer deployment actions within one-week of the completion of all infrastructure readiness tasks.

Customer Responsibilities

- The Customer must attend the kick-off meeting and complete information gathering documents as quickly and accurately as possible.
- The Customer must accomplish all infrastructure preparation tasks as quickly as possible.
- The Customer must deploy tools, as applicable, in their environment, in accordance with provided requirements.

5.2 ActiveEye Platform

Motorola will provide 24/7 access to the ActiveEye platform. Motorola will notify Customer if access will be affected by scheduled maintenance.

Motorola Responsibilities

- Provide access to the ActiveEye portal for Customer and any identified, approved users. After initial deployment, Customer will have self-service access to add/remove/update user access as needed.
- Provide the services subscribed to, as noted in Table 4-1. Service.
- Make monthly services implementation and status reports available to Customer.

- Resolve platform issues and technical errors as documented by Customer.
- Retain security logs within ActiveEye. Security logs will be retained for the length of time designated by the long-term storage policy selected by Customer.

Customer Responsibilities

- Provide reasonable assistance to Motorola to perform the Service, as described in this SOW. This assistance includes, but is not limited to, technical assistance with issues that may require physical access to the devices affected by this Service, or virtual assistance with virtual environment issues that require administrative access to devices affected by this Service.
- Provide all technical, license, and service information requested in the implementation documents prior to the commencement of the Service.
- Perform all network and system integrations necessary for ActiveEye Service. This includes providing external connectivity for ActiveEye security components.
- Ensure network bandwidth of up to 40MB per host, per day.
- Install agents on in-scope systems and devices, as required.
- Configure all necessary components of Customer's infrastructure to integrate with ActiveEye.
- Provide the name, email, landline telephone numbers, and mobile telephone number for all shipping, installation, and security Points of Contact (POC)s.
- Manage user access to the ActiveEye portal, creating new user accounts when needed and removing a user's access when it is no longer required.

5.2.1 Endpoint Detection and Response

Motorola Responsibilities

- Provide ports and protocols to the Customer for the EDR solution.
- Deploy and maintain EDR agents to PremierOne host environment.
- Configure EDR solution to enable ActiveEye connection for event/alert collection and response actions.

Customer Responsibilities

- Deploy and maintain EDR agents to required customer-owned client workstations and handheld devices, as applicable.
- Configure networking infrastructure to allow EDR agents to communicate with centralized server components.
- Comply/consent with the terms of applicable licenses, privacy statements, or other third-party agreements to the extent third-party software or services are utilized or provided by/through Motorola Solutions, including applicable EDR solution provider's end user license agreements ("EULAs"), if any.
- Obtain any third-party consent required to enable Motorola to provide the monitoring service, if applicable.

5.2.2 Network Detection

ActiveEye Network Detection enables security teams to automate investigation of network alerts and view this activity in the context of other user activity.

Motorola Responsibilities

- Work with Customer to integrate ActiveEye Remote Security Sensor(s) containing the Network Intrusion Detection System into Customer's system.

Customer Responsibilities

- Configure networking infrastructure to allow ActiveEye Remote Security Sensor to communicate with ActiveEye as defined.
- Configure and maintain networking infrastructure physical and logical configuration to mirror (typically via a SPAN port on a switch) network traffic to the ActiveEye sensor.

5.2.3 Technical Support

ActiveEye Managed Detection & Response Technical Support provides Customer with a toll-free telephone number and email address for ActiveEye Managed Detection & Response support requests, available Monday to Friday from 8am to 7pm CST. Support requests are stored in a ticketing system for accountability and reporting.

Motorola Responsibilities

- Notify Customer of any scheduled maintenance or planned outages.
- Provide technical support, security control, and service improvements related to ActiveEye.

Customer Responsibilities

- Provide sufficient information to allow Motorola technical support agents to diagnose and resolve the issue.

Limitations and Exclusions

Technical support is limited to the implementation and use of the ActiveEye platform and does not include use or implementation of third-party components.

5.3 Security Operations Center Monitoring and Support

Motorola's Security Operations Center (SOC) will provide continuous 24x7 monitoring through automated tools and review by trained security analysts. Motorola will analyze events and notify Customer in accordance with **Table 5-2.** Notification Procedures.

Motorola will start monitoring the Service in accordance with Motorola processes and procedures after deployment, as described in Section 5.1 Project Deployment.

Customer will be able to open a support request for the SOC via a toll-free telephone number or email address, available 24/7. Support requests are stored in a ticketing system for accountability and reporting.

5.3.1 Ongoing Service Responsibilities

Motorola Responsibilities

If a probable security incident is detected, provide phone and email support to:

- Engage Customer's defined Incident Response Process
- Attempt to determine the root cause and extent of compromise using existing monitoring capabilities in place as part of the Service.
- Analysis and support to help Customer determine if Customer's corrective actions are effective.
- Continuous monitoring, in parallel with analysis, to support incident response.

Customer Responsibilities

- Provide Motorola with accurate and up-to-date information, including the name, email, landline telephone numbers, and mobile telephone numbers for all designated, authorized Customer escalation Points of Contact (POC).
- Provide a Network Map detailing Customer's network architecture for network(s) in scope for the Service, if available.
- Provide a timely response to SOC security incident tickets or investigation questions.
- Provide an established service window in which qualified IT personnel will be able to respond to major event escalations.
- Notify Motorola at least twenty-four (24) hours in advance of any scheduled maintenance, network administration activity, or system administration activity that would affect Motorola's ability to perform the Managed SOC Service, as described in this SOW.

5.3.2 Service Module Specific SOC Services

With this service, Motorola's SOC will provide specific services for ActiveEye platform service modules Customer is subscribed to. In addition, SOC services can be augmented by Advanced Threat Insights.

The following describes these security operations modules.

5.3.2.1 Managed Network Detection

Motorola's SOC will consult with Customer on the deployment of the Network Detection Service components.

The SOC will continually monitor and update the security policy of each sensor to tune out unnecessary alerting and flow monitoring so that the system is optimized to detect true malicious activity.

Motorola Responsibilities

- Optimize the policies and configurations to tune out noise and highlight potential threats.

Customer Responsibilities

- Initiate recommended response actions when active attacks are detected.

5.3.2.2 Managed Endpoint Detection and Response

Motorola's SOC will consult with Customer on the deployment of the Endpoint Detection and Response (EDR) solution. The SOC will advise, on an ongoing basis, what security policies should be updated to optimize threat detection.

The SOC will consult with Customer to define a response automation plan that outlines the scenarios where the SOC should take automatic response actions on systems within Customer environment. In cases outside the automatic response scenarios, the SOC will open Security Cases with Customer with recommended actions and await approval before taking actions.

The SOC will track suspicious files and processes in Customer environment to report threat trends on what new threats are being discovered vs. previously seen threats.

Motorola Responsibilities

- Provide recommendations on endpoint security policy and configuration to optimize threat identification.
- Maintain, with input from Customer, an automatic response plan for defined endpoint security scenarios or malware types.

Customer Responsibilities

- Initiate response actions on endpoint solutions when not defined as automatic actions or not available as remote actions on the EDR solution in use.

5.3.3 Event Response, Notification, and Tuning

Motorola will analyze events created and/or aggregated by the Service, assess their type, and notify Customer in accordance with the following table.

Table 5-1: Priority Level Definitions and Response Times

Incident Priority	Incident Definition	Response Time
Critical P1	Security incidents that have caused or are suspected to have caused significant and/or widespread damage to the functionality of the Customer's PremierOne system or information stored within it. Effort to recover from the incident may be significant. Examples: • Malware that is not quarantined by anti-virus • Evidence that a monitored component has communicated with suspected malicious actors.	Response provided **24 hours, 7 days** a week, including US Public Holidays.
High P2	Security incidents that have localized impact but are viewed as having the potential to become more serious if not quickly addressed. Effort to recover from the incident may be moderate to significant. Examples: • Malware that is quarantined by antivirus. • Multiple behaviors observed in the system that are consistent with known attacker techniques.	Response provided **24 hours, 7 days** a week, including US Public Holidays.

Medium P3	Security incidents that potentially indicate an attacker is performing reconnaissance or initial attempts at accessing the system. Effort to recover from the incident may be low to moderate. Examples include: • Suspected unauthorized attempts to log into user accounts. • Suspected unauthorized changes to system configurations, such as firewalls or user accounts. • Observed failures of security components. • Informational events. • User account creation or deletion. • Privilege change for existing accounts.	Response provided from 8:00a.m. to 5:00p.m. CST/CDT, Monday through Friday, excluding U.S. Public Holidays.
Low P4	These are typically service requests from the Customer.	Response provided from 8:00a.m. to 5:00p.m. CST/CDT, Monday through Friday, excluding U.S. Public Holidays.

5.3.3.1 Notification

Motorola will establish notification procedures with Customer, generally categorized in accordance with the following table.

Table 5-2. Notification Procedures

Notification Procedure	Details
Routine Notification Procedure	The means, addresses, format, and desired content (within the capabilities of the installed technology) for Events of Interest. These can be formatted for automated processing, e.g., by ticketing systems.
Urgent Notification Procedure	Additional, optional means and addresses for notifications of Events of Interest that require urgent notification. These usually include telephone notifications.

Motorola will notify Customer according to the escalation and contact procedures defined by Customer and Motorola during the implementation process.

5.3.3.2 Tuning

Motorola will assess certain events to be environmental noise, potentially addressable configuration issues in the environment, or false positives. Motorola may recommend these be addressed by Customer to preserve system and network resources.

Motorola will provide Customer with the ability to temporarily suppress alerts reaching ActiveEye, enabling a co-managed approach to tuning and suppressing events or alarms. The SOC may permanently suppress particular alerts and alarms if not necessary for actionable threat detection.

5.3.3.3 Tuning Period Exception

The tuning period is considered to be the first thirty (30) days after each service module has been confirmed properly deployed and configured and starts receiving data. During the tuning period, Motorola may make recommendations to Customer to adjust the configurations of their installed software so that Services can be effectively delivered. Service Availability will not be applicable during the tuning period and responses or notifications may not be delivered. However, Motorola will make best efforts to provide responses and notifications during this period.

Motorola may continue to recommend necessary tuning changes after this period, with no impact on Service Availability.

Motorola Solutions Responsibilities

- Motorola will monitor the service and check in-scope assets are properly forwarding logs or events and that system scans are functioning. Motorola will notify the customer of any exceptions. Motorola will begin monitoring any properly connected, in-scope sources after the tuning period.
- Motorola will conduct initial tuning of the events and alarms in the service, as well as set up initial reports (User Access, Administration Events, and Configuration Findings Reports).

Customer Responsibilities

- Customer must provide appropriate connectivity for all in-scope assets to the service and address any exceptions noted by Motorola. Failure to do so will delay completion of future phases and will prevent Motorola from monitoring those sources.
- Customer must deploy tools, as applicable, in their environment, in accordance with provided requirements. Customer must engage the SOC team in discussing the tuning approach and confirm the configurations requested.

5.3.4 Limitations and Exclusion

This Service excludes any incident response support actions outside those outlined within this SOW, such as those that require Motorola personnel to directly access Customer devices, travel, deploy new tools, or direct specific actions. These services may be obtained from Motorola through a separate proposal.

Section 6

Solution Description – Professional Services

Motorola Solutions, Inc. (Motorola) is pleased to present the proposed cybersecurity services for Port of Los Angeles (Customer).

The following cybersecurity services are included in our proposal:

- **Penetration Testing Service**
  - External Penetration Testing
  - Retesting
- **Cybersecurity Health Check**
  - ASTRO® Risk Assessment Package
    - Cyber Security Risk Assessment
    - Firewall Review
    - Physical Security Assessment
    - Vulnerability Scan
  - PremierOne Risk Assessment Standard
    - Cyber Security Risk Assessment
    - Firewall Review
    - Physical Security Assessment
    - Vulnerability Scan and Results Assessment
- **Incident Management and Response Preparedness Services**
  - ASTRO® Incident Response Package
    - Incident Response Plan Review and Development
    - Incident Response Tabletop Exercise
    - Incident Management Training
  - PremierOne CAD Incident Response Package
    - Incident Response Plan Review and Development
    - Incident Response Tabletop Exercise
    - Incident Management Training
- **Cybersecurity Tabletop Exercises**

6.1 Site Information

The following site information is included in the scope of our proposal:

Table 6-1: Customer Site Information

Quantity	Site / Location	Network Environment	Service Type
1	Organization Level	ASTRO	• Cyber Security Risk Assessment • Penetration Testing – External • Penetration Testing - Retesting • Vulnerability Scanning – Internal • Incident Management and Response Preparedness Services • Cybersecurity Tabletop Exercise
1	Core Site	ASTRO	• Physical Security Assessment • Firewall Review
1	DSR	ASTRO	• Physical Security Assessment • Firewall Review
2	Radio CEN	ASTRO	Physical Security Assessment
7	RF Site Locations	ASTRO	Physical Security Assessment
1	Dispatch Locations	ASTRO	Physical Security Assessment

Quantity	Site / Location	Network Environment	Service Type
1	Organization Level	PremierOne CAD	• Cyber Security Risk Assessment • Incident Management and Response Preparedness Services • Vulnerability Scanning and Results Assessment • Penetration Testing – External • Cybersecurity Tabletop Exercise
X	PSAP (Public Safety Answering Point)	PremierOne CAD	Physical Security Assessment
X	CAD Production System	PremierOne CAD	Firewall Review
X	Disaster Recovery	PremierOne CAD	• Physical Security Assessment • Firewall Review

Quantity	Site / Location	Network Environment	Service Type
1	Organization Level	CommandCentral Aware	• Penetration Testing – External • Penetration Testing – Retesting

Backhaul environments are not included in the scope of our proposal. RF Sites and Dispatch locations must be within 70 miles of the primary assessment location. The Risk Assessment scope will be one system core, as well as a backup site/location that is within 50 miles of the primary site.

Table 6-2: Services by Year

Year	Service	Description
1	Cybersecurity Health Check	• Cyber Security Risk Assessment • Firewall Review • Vulnerability Scanning – Internal • Physical Security Assessment
1	Penetration Testing	• External Penetration Test with Retesting
1	Incident Management and Response Preparedness Services	• Incident Response Plan Review and Development • Incident Response Tabletop Exercise • Incident Management Training
1	Cybersecurity Tabletop Exercise	• Ransomware
2+	Annual Cybersecurity Services	• External Penetration Test with Retesting • Cybersecurity Tabletop Exercises

6.2 Service Description

6.2.1 Penetration Testing Service

Information security follows a continuous cycle of design, deploy, test, and improve. Policies and guidelines, implementation processes and procedures, and testing form the basis for this process. While policies and procedures may be formalized and well-understood, breakdowns in processes or simple human error can lead to unknown vulnerabilities that can only be discovered through testing processes.

For information security, one of the best ways to accomplish these objectives is through a process referred to as penetration testing during which a security professional employs tools and techniques that both test configurations as well as simulate steps that could be taken by real-world attackers. Leveraging their technical knowledge of architecture, operating systems, and applications as well as publicly available or well-known information, these experts are often able to crack systems and networks—revealing important vulnerabilities within an infrastructure.

Motorola's experienced security team will utilize techniques and tools commonly used by attackers to attempt to exploit and show vulnerabilities within your network infrastructure and Motorola systems. This process goes beyond automated scanning and follows an approach as outlined in the Methodology section below.

6.2.1.1 External Penetration Testing

Motorola's External Penetration Testing simulates an external attempt to breach security using techniques and tools commonly used by attackers. This helps the Customer to determine which policies, processes, and technologies are effective under real conditions.

For this testing, Motorola experts combine their technical knowledge of architecture, operating systems, and applications with publicly available information to find security vulnerabilities in externally accessible infrastructure. The tests will follow a risk-based approach, with testers attempting to exploit

systems they suspect contain high-value information. Testing will also include "Targets of Opportunity" found in the Customer's network.

6.2.2 Cybersecurity Health Check

6.2.2.1 Cyber Security Risk Assessment

The Cyber Security Risk Assessment is a professional service to evaluate an existing information security program against best practices, as well as common frameworks. The Cyber Security Risk Assessment will support the investigation of already established policies, standards, procedures, practices, and technologies implemented by the Customer and align these practices with the chosen framework. The outcome of the assessment will allow Motorola to provide the Customer with an understanding of its state of compliance, provide insight into gaps that have been identified in the security program with respect to cyber best practices and benchmarks and provide remediation recommendations for the organization to improve upon.

Objectives

Customer is seeking assistance to evaluate if their security program meets prudent security guidelines, and is in compliance with common cyber requirements. This security review will provide Customer with visibility into how your existing IT Security standards stand up against best practices to:

- Identify cyber threats and gaps
- Determine areas of mis-alignment with common cyber frameworks such as CJIS, NIST CSF or ISO 27001
- Define and prioritize the risk associated with the gaps
- Offer specific advice on how to remediate the gaps

6.2.2.2 Vulnerability Scan and Results Assessment

Regular vulnerability scanning and analysis is a fundamental monitoring control in a comprehensive information security program. It provides an understanding of the degree to which the Customer's network infrastructure is well controlled and secure from public threats.

Objectives

Internal vulnerability scanning can include any combination of the following goals:

- Understand Customer's exposure to known vulnerabilities through Internet-facing systems.
- Understand Customer's exposure to internal server and/or system compromise through known vulnerabilities.
- Understand the effectiveness of Customer's patch management program.
- Understand the effectiveness of Customer's system hardening procedures.
- Meet independent third-party assessment requirements
- Assess and quantify existing vulnerabilities in tested systems and provide remediation strategies.
- Establish a baseline of the network for future vulnerability assessments.

For each issue discovered during vulnerability scanning, Motorola provides detailed vulnerability and remediation information to assist with planning Customer's next steps to address the issues discovered. This includes:

- Definitions of the risk severity levels and potential consequences posed by a vulnerability.
- Recommended procedures for remediating each vulnerability. These are provided in Motorola's easy-to-use Vulnerability Assessment Detail Analyzer provided in a Microsoft Excel format. This Analyzer can be used to perform additional data analysis and gain additional insight into the environment.

6.2.2.3 Firewall Review

Review firewall configuration files in order to determine whether there are any misconfigurations or security weaknesses that would allow traffic from external sources to bypass security restrictions and enter the network, as well as whether traffic is allowed to leave the network undetected.

Checks performed include authentication services and settings, time synchronization, message logging, network interfaces, etc.

6.2.2.4 Physical Security Assessment

Locating gaps in facility security and determining what risks are associated with them requires specialized training that can be expensive to maintain on staff. Motorola can provide an evaluation by a facility security expert, giving the benefit of expert assessment without the costs of recruiting and retaining personnel. Motorola's expert assesses the efficacy of security controls and procedures, and provides a report outlining potential security risks and ways to mitigate them.

6.2.3 Incident Management and Response Preparedness Services

The reality of security incidents, breaches, and data loss have become all too familiar to a growing number of organizations across all industries. Information security incident management programs are required to help institutions respond to information security incidents that compromise the confidentiality, availability, and integrity of an institution's information technology resources and data. In most cases, failure to plan for handling information security incidents can jeopardize the organization's ability to effectively detect, contain, and respond to costly and time-consuming cybersecurity events.

To help our customers prepare and plan for cybersecurity events, Motorola delivers Incident Management and Response Preparedness services. These services deliver support with incident handling development and testing. The services are designed to help document and exercise the processes need to reduce the impact resulting from cybersecurity events and intrusions within the customer's environment.

6.2.3.1 Incident Response Plan Review and Development

An Incident Response (IR) Plan is a set of written instructions for detecting, responding to, and limiting the effects of an information security breach/event. The Incident Response Plan Review and Development effort will support the Customer in defining, developing, implementing, and testing the procedures required to follow when a security event occurs based on the most common and recent threats in the Customer's industry. By identifying the various stakeholders, documenting their roles throughout an Incident Management and Response process, the Customer will be able to Prepare,

Detect, Analyze, Contain, Eradicate, Recover, and move forward with Post-Incident Activity which is necessary before and after a security incident.

6.2.3.2 Incident Response Tabletop Exercise

A Cybersecurity Incident Response Tabletop Exercise provides scenario(s), which are presented in timed release of information, to specific participants in a discussion format to determine the Customer's ability to perform response and recovery decision-making related to a cybersecurity event. During the Cybersecurity Incident Response Tabletop Exercise, the participants will respond according to what they would 'normally' do given the scenario and subsequent events. As the scenario unfolds the Customer will discuss the response needed to determine courses of action. The format of the Cybersecurity Incident Response Tabletop Exercise is strictly discussion-based and limited to participants in the venue – no actions are taken on live systems. A facilitator will guide the discussion and prompt participants' additional actions or comments via thought-provoking questions designed to achieve the exercise objectives.

6.2.3.3 Incident Management Training

During a cybersecurity incident, a trained multi-disciplinary team is required to confront the threats to data and loss of system availability. An incident response and management team is composed of both technical and non-technical resources that must work together seamlessly to accomplish a common outcome. Incident Management Training is a series of courses that provide an overview of Incident Management topics such as: The Incident Response Lifecycle; Notifications and Escalation; Classification and Severity; Cyber Insurance Basics; Involving Third Parties Judiciously; Regulatory Requirements for Reporting; and Incident Response Team Roles and Responsibilities.

6.2.4 Cybersecurity Table-Top Exercise

A tabletop exercise is a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator guides the discussion by presenting a scenario and asking questions based on the scenario.

Motorola's tabletop exercise offering is designed to evaluate the customer's ability to effectively respond to, and recover from, a ransomware event where an attacker encrypts the organization's data and demands payment to restore access. While the exercise tests the customer's knowledge and execution of their IR Plan in response to the ransomware scenario, it also looks at how the organization coordinates and communicates with the Motorola SOC team providing MDR support to the customer. During the exercise, participants will respond according to what they would 'normally' do given the scenario and subsequent events. As the scenario unfolds, the customer will discuss the response needed to determine courses of action.

The tabletop exercise will be limited to the participants in the venue – no actions are taken on live systems. The exercise facilitator will serve as the Motorola SOC Team providing MDR support and prompt participant actions or comments via questions designed to achieve the exercise objectives. The desired end-state is a validated IR Plan, the identification of any gaps in the process (e.g., training, supporting documentation, coordination/communication requirements, etc.), and customer familiarization with the SOC and its MDR capabilities before a real-world incident occurs.

Section 7

Statement of Work – Professional Services

In accordance with the terms and conditions of the Agreement, this Statement of Work (SOW), including all of its subsections and attachments, defines the principal activities and responsibilities of all parties for the delivery of Motorola Solutions, Inc. (Motorola) Cybersecurity services as presented in this proposal to Port of Los Angeles (Customer).

7.1 Penetration Testing Service

Penetration Testing services are described in the subsections below.

7.1.1 Methodology

Penetration Testing follows a three-step methodology of:

- Reconnaissance
- Enumeration
- Fingerprinting, Exploit Selection (and where appropriate Exploitation / Compromise)

Step One: Reconnaissance

This phase uses public sources of information such as Google searching, public web sites, Wiki and Blog communities, domain naming and registration information, and other information to determine as much information about potential targets as possible. This information is then integrated with any information provided by the Customer to build as complete a picture as possible about the target systems and network.

Step Two: Enumeration

During the enumeration phase, the tester actively tries to confirm or expand the information he has regarding the system. This can involve additional tools that actively attempt to map networks, systems, and configuration settings.

Step Three: Fingerprinting, Exploit Selection (and Compromise)

Once active and passive information gathering is complete, testers begin to narrow in on potential attack paths. During the fingerprinting phase, testers gather additional detailed information about a specific target. This can include an operating system or software versions, allowed encryption methods, and other specific information that leads to identifying a weakness or vulnerability and selecting the appropriate exploit technique to leverage that vulnerability. During testing, it may be sufficient to identify vulnerabilities and use a limited exploit to confirm their existence. However, whether for proof or confirmation, many times exploits will be leveraged to gain access and show system weaknesses. Motorola follows a "Do No Harm" approach to testing and will not conduct tests or exploits that would purposely take down a system or cause other operational harm to a system or data.

7.1.1.1 External Penetration Testing

External penetration testing applies these techniques to Internet-facing systems where "external" refers to tests performed from outside the organization's infrastructure. These tests target the following types of systems and services:

- Firewalls
- External Routers
- Web Servers – typically at the operating system and web server levels. Dynamic web applications are penetration tested by a comprehensive web application penetration testing approach outside the scope of a standard external penetration test unless requested.
- Domain Name Service Servers (DNS)
- Remote Access (VPN's, SSL VPN's, etc.)
- Secure encrypted connections (site-to-site or B2B VPN's)
- Email Systems
- File Transfer Servers

Scope of Activity

- Reconnaissance, Enumeration, Exploitation & Remediation Recommendations
- Up to 50 live IP addresses tested

Service Deliverables are described in Section 7.1.2.

7.1.2 Service Deliverables

The following service deliverables will be provided by Motorola:

Table 7-1: Service Deliverables

Deliverable	Description
Electronic Reports	After the assessment is complete, Motorola will provide Customer with a formal report that contains: **Executive Summary:** This is a concise summary of the findings and associated recommendations targeted to a non-technical, executive audience. **Operational Findings Matrix and Action Plan:** A findings matrix summarizing items that Motorola determines to pose a risk to the Customer along with risk ratings and remediation recommendations. Technical overview of critical and high level findings from the assessment.
Draft Review Conference Call or Presentation	A formal conference call debriefing based on the draft report before marking the report as final. Customer participants will be able to have interim question-and-answer conversations with the testers regarding their findings as well.

7.2 Cybersecurity Health Check

The following Risk Assessment services are described in the subsections below.

- Cyber Security Risk Assessment
  - Security Program Review
- Vulnerability Scan
- Firewall Review
- Physical Security Assessment

7.2.1 Cyber Security Risk Assessment

The project consists of the following tasks:

- Introduction Call, Planning and Setup
- Assessment Initiation: Discovery, Key Risks, Control and Program Assessment
- Draft NIST CSF Security Program Risk Assessment and DHS CPG scorecard creation
- Draft Report Review and Final Report Delivery

Step One: Introduction Call, Planning, and Setup

Motorola will collaborate with the Customer's Primary Point of Contact (POC) to define the timing, confirm scope, and speak through any related details related to interview scheduling with key stakeholders, relevant security program documents, coordination of project status meeting and milestone schedule, travel, and/or escalation protocol required for the kick-off of the project.

Assessment Initiation: Discovery, Key Risks, Control Assessment

Once Motorola completes the Introduction Call, Planning, and Setup phase and upon the arrival of the agreed upon assessment date(s), Motorola will conduct the Cyber Security Risk Assessment based on the following methodology and tasks:

Step Two: Discovery

Motorola will conduct a series of remote and/or onsite interviews to understand the elements by which the Customer's cybersecurity efforts will be measured against, along with identifying the Customer's in-scope framework categories and subcategories. Through the interviews with key Customer staff, Motorola will determine the Customer's cybersecurity compliance as they relate to safeguarding or disseminating data and maintaining the availability of systems against the best practices and industry leading frameworks. Motorola will evaluate compliance with the following security disciplines:

- Asset Management
- Governance
- Remote Access
- Risk Management
- Supply Chain Management
- Identity Management and Access Control
- Awareness and Training

- Data Security and Encryption
- Maintenance
- Protective Technology
- Detection and Security Monitoring
- Incident Response, Analysis, and Recovery
- Remote Access
- Business Continuity and Disaster Recovery

Key Risks

NIST's Special Publication 800 Series provides guidance for supervision and administration of an enterprise Information Security Management System. Motorola methodology includes a systematic orientation to the threat environment facing Customer's industry as well as Customer's specific business and operating environment. Motorola will determine key risk areas based on vulnerabilities, likely threats, potential impacts as identified through document reviews, interviews, and industry best practices.

Control Assessment

Upon identifying the key risks for the Customer with respect to compliance and best practices, Motorola will perform a control analysis to determine the current profile of cybersecurity maturity with NIST, ISO, and other industry framework requirements and create a list of Information Security Management System program and policy gaps. Motorola will then determine the target profile based on the desired level of risk mitigation and risk appetite and outline the needed investments and rebalancing efforts to meet the target profile required to satisfy compliance with regulatory requirements and cyber industry leading practices.

Step Three: Draft NIST CSF Security Program Risk Assessment Report Creation

Motorola will document the results of the Risk Assessment findings, gaps, and recommendations in a written Portable Document Format (PDF) formatted report and make reasonable efforts to prioritize issues via the most pressing threats, risk areas and gaps.

Upon the completion of the Draft Report, Motorola will perform the following tasks with the Customer:

- Provide the Customer with the Draft Report for their review and analysis. During this time, Motorola will also coordinate a Draft Report Review session with the relevant stakeholders over the phone and/or internet conferencing methods.
- Review the report and findings with the Customer and discuss recommendations for mitigating the relevant risks with the Customer
- Upon completion of the Draft Report Review, Motorola will make final modifications to the report that are brought up by the Customer and deliver the Final Report back to the Customer POC to complete the project.

7.2.1.1 Scope of Activity

Motorola understands the scope of this engagement to be:

Activity or Focus	Description
Cyber Security Risk Assessment	Up to fifteen (15) interviews of Customer staff knowledgeable in information security, technology management. All Information protection and security documentation such as: – Policies, Procedures, Guidelines, Baselines, and / or Standards – Previous audits, assessments and / or regulatory reviews Environment(s) in scope: See Section 6.1 for site listing.

7.2.2 Vulnerability Scan

7.2.2.1 Methodology

Motorola's Vulnerability Assessment Methodology uses a signature-based test-and-evaluate process that leverages input from industry vulnerability databases including but not limited to the Common Vulnerabilities and Exposures (CVE) database, Microsoft vulnerabilities, and Bugtraq. Motorola personnel performed this Vulnerability Scanning analysis with the use of automated vulnerability scanning systems and where appropriate applied manual validation techniques, experienced security analysis, and/or follow up discussions to gain additional information.

The data gathered is then aggregated and placed in the Vulnerability Assessment Detail Analyzer for further review with Customer.

7.2.2.2 Scope of Activity

- Scan of the internal IP range of up to 1,500 active internal IPs. IP addresses will be reconfirmed with Customer prior to the beginning of the effort.
- Any Critical findings are informally communicated within 24 hours of discovery.

7.2.3 Firewall Review

Motorola will review the Customer's firewall configuration files to provide the following services:

- Determine whether there are any misconfigurations or security weaknesses that would allow traffic from external sources to bypass security restrictions and enter the network, as well as whether traffic is allowed to leave the network undetected.
- Perform industry best practice validations such as authentication services and settings, time synchronization, message logging, network interfaces, etc.
- Provide a report that includes an analysis of the findings, best practice comparison and recommendations, as well as recommendations of configuration changes for any weaknesses or misconfigurations.

The configuration file can be reviewed offline so no disruption to normal network activities would occur.

7.2.4 Physical Security Assessment

The assessment will evaluate Customer's physical safeguards. Motorola's expert will travel to Customer's location to assess the efficacy of security controls and procedures.

7.2.4.1 Requirements & Objectives

The following scope is included within this service offering:

- Physical Security:
  - Site Security Architecture Assessment
  - Perimeter Access Controls Assessment
- Sensitive Information Handling:
  - Internal sensitive information handling assessment

7.2.4.2 Service Deliverables

After performing the assessment, the expert will provide a report outlining potential security risks and recommending changes to mitigate them.

7.2.5 Service Deliverables

The following service deliverables will be provided by Motorola:

Table 7-2: Service Deliverables

Deliverable	Description
Electronic Reports	After the assessment is complete, Motorola will provide Customer with a formal report that contains: **Executive Summary:** This is a concise summary of the findings and associated recommendations targeted to a non-technical, executive audience. **Technical Summary:** – Identify several strong security practices currently in place supporting Customer's security program. – Provide areas for improvement based on determined security risks currently facing Customer and its information security program with respect to the CSF requirements. – Identify potential gaps between the in-scope Customer's operating environment and the NIST CSF requirements. – Provide a DHS Cross-Sector Cybersecurity Performance Goal scorecard that displays where organizations are lacking in conformance to the CPGs. – Provide a control rating using the scoring methodology based on observations generated in interviews, and policies and documentation received and reviewed. – Provide additional recommendations and remediation guidance for each control in NIST CSF categories and subcategories which will assist Customer management in reaching compliance.

Deliverable	Description
Draft Review Conference Call or Presentation	A formal conference call debriefing based on the draft report before marking the report as final. Customer participants will be able to have interim question-and-answer conversations with the testers regarding their findings as well.

7.3 Incident Management and Response Preparedness Services

7.3.1 Incident Response Plan Review and Development

7.3.1.1 Methodology

Motorola will use industry best practices to help develop and enhance the Customer's Incident Response Plan. The Incident Response Plan will support the customer with the following phases of a cybersecurity incident as outlined by NIST 800-61r2:

Preparation

The Preparation phase documents, outlines, and explains Customer's Incident Response team's roles and responsibilities, including establishing the underlying security policy which will guide the development of the Customer's Incident Response Plan.

Detection and Analysis

The Detection and Analysis phase of the Incident Response Plan involves monitoring, detecting, alerting, and reporting on security events. This includes identifying known, unknown, and suspect threats—those that appear malicious in nature, but not enough data is available at the time of discovery to decide either way. Criteria will also be established for the categorization of incidents as well as an escalation matrix for incidents to be reported.

Containment, Eradication, and Recovery

The Containment, Eradication and Recovery phase is used to help with triaging, containing, and neutralizing the security threats by isolating, shutting down, or otherwise "disconnecting" infected systems from your network to prevent the spread of the cyber-attack.

Additionally, incident response operations will include eliminating the threats which led to the security incident and bring affected production systems back online carefully, to prevent additional attacks.

Lessons Learned

The purpose of the Lessons Learned phase is to complete documentation that could not be prepared during the response process and investigate the incident further to identify its full scope, how it was contained and eradicated, what was done to recover the attacked systems, areas where the response team was effective, and areas that require improvement.

7.3.1.2 Scope of Activity

Motorola understands the scope of this engagement to be:

- Determine the current state of the existing Customer Incident Response plans and procedures and review internal Customer objectives for the plan with the Customer's Incident Response lead.
- Assist the Customer's Incident Response lead in developing and coordinating across Customer's business units (Cyber) Security Incident Severity Classification guidance to address Customer business operations and response priorities.
- Develop a workflow that establishes key steps and considerations for a response along with highlighting key decision points for escalation and response team expansion.
- Compile or update appropriate written response procedures for addressing a range of cyber incidents or attacks, to include initial actions upon detection, notification of key staff, external reporting, escalation procedures, handling public messaging, legal and regulatory considerations, and identification of internal and external expertise to leverage during an incident response. Motorola will document the resulting plan in a form approved by Customer's Incident Response lead, to include both restricted prescriptive form (i.e., limited distribution and used during an incident) and unrestricted informational form (i.e., identifies response framework and guidance for use with auditors and other non-operational uses).
- Determine and coordinate linkages to other Incident Response-related plans and procedures, such as corporate communications plan(s) and higher-level business continuity plans and procedures.
- Develop a glossary of industry-standard or best-practice Incident Response terms for use in instructing and educating the Customer staff.
- Instruct and educate the Customer Incident Response lead on best practices for incident response to build confidence in and advocacy for the resulting Incident Response plan.
- Assist the Customer Incident Response lead in gaining approval for the final Incident Response plan with appropriate Customer business units and security leadership.
- Instruct and educate the Customer security team and appropriate business units on the final approved Incident Response plan; Motorola proposes to do this via an on-site training event, via webinar, or a combination of the two activities.

7.3.1.3 Service Deliverables

Motorola will work with the Customer to prepare an Incident Response Plan. The document will include the following details:

Electronic Documents

- Customer Incident Response Plan
  - Preparation
  - Detection and Analysis
  - Containment, Eradication, and Recovery
  - Post-Incident Activity
- The Incident Response Plan may document the following items:
  - Purpose of the Plan

  - Scope and Exceptions
  - Inputs and Starting Events
  - Outputs and Completion of Events (Evidence)
  - Procedures
  - Authorities
  - Definitions
  - Links to Related Policies
  - Links to Related Procedures
  - Relevant Regulations
  - Enforcement
  - Revision and Review History
  - IT and Data Security Incident Severity Classification
  - Security Incident Response Team Roster and Contact Information
  - Additional External Contacts (Law Enforcement, Key Security Vendors, Stakeholders)
- Prioritized Incident Response Recommendations for any IR actions that are not currently planned, accounted for and/or addressed by Customer

Draft Review Conference Call or Presentation

- A formal conference call debriefing based on the draft plan before marking the plan "final".
- Customer will be able to have interim question-and-answer conversations with Motorola regarding the Incident Response Plan.

7.3.2 Incident Management Training

7.3.2.1 Methodology

Discovery

Motorola will work with Customer's team to find out key elements of your organization including your current model of incident response and management, internal and external stakeholders, and incident response team structure.

Motorola will find out more about Customer's goals and objectives for the training and what key takeaways are critical for employees to get from the training experience.

Customization and Creation

Our team will create and customize training to your specific needs and culture as well as ensure it fits your educational objectives.

Training Delivery

Training will be delivered by an in-person experience or live by a remote virtual conference software.

7.3.2.2 Scope of Activity

Motorola will conduct group training sessions with stakeholders to ensure all team members are well versed in the plan document(s), understand their roles and are knowledgeable of expected actions in a real-world event. Training sessions can certainly be recorded for replay as needed.

7.3.2.3 Service Deliverables

Motorola will provide Customer with the following deliverables:

- Trainings will be conducted on-site.
- Training topics are up to forty-five (45) minutes of content each, with up to ten (10) minutes of questions and discussion.
- Customer may select up to two (2) training topics from the list below:
  - Incident Management Overview
  - Incident Management and Response Lifecycle
  - Incident Response Team Roles and Responsibilities
  - Incident Classification, Severity, and Notification
  - Regulatory Reporting Requirements for Incidents
  - Incident Response Plan Walkthrough and Refresher
- Up to three (3) training sessions for each course can be offered to ensure maximum participation.

7.3.3 Incident Response Tabletop Exercise

As part of the Incident Response Tabletop Exercise, Motorola will help plan, conduct, and facilitate a four (4) to six (6) hour tabletop exercise to walk through the Customer Incident Response (IR) plan with applicable Customer business units. The selection of which Customer business units participate will be at the discretion of the Customer CISO or Incident Response lead, and we will develop appropriate scenarios to address the appropriate elements of the Incident Response plan and level of involvement for each group. The plan walk-through will be conducted on the basis of scenarios designed to elicit discussion around key elements of the Incident Response plan. While the walk-through will focus on indoctrination to the plan, it will also provide opportunities to verify key assumptions in the plan.

7.3.3.1 Methodology

Motorola leverages lessons learned from years of experience using planning and execution practices based on the Homeland Security Exercise and Evaluation Program (HSEEP), a national standard for exercises, and our own objectives-based contingency planning and risk assessment methodology.

Our proposed process includes the following five key activities:

Identifying Exercise Objectives

Motorola will review Customer's participating stakeholders and gather background data on the information security and cybersecurity skill level of the staff, the current security capabilities of the organization, identify key threat scenarios, and response and coordination processes that may/may not be established. Motorola may conduct interviews or review documentation as part of this activity.

Motorola will work with the Customer and exercise participants to draft, coordinate, and approve the scenario(s) and exercise objectives.

Developing and Design of the Exercise

Motorola will design the scenario(s) based on the information gathered from the interviews with the participating cooperatives and coordinate it with the Customer's exercise stakeholders. A collaborative process between the stakeholders to identify key concerns and response actions will then be used as a foundation for the exercise

Exercise

Motorola will facilitate a tabletop exercise over the agreed upon timeframe involving stakeholders identified with the Customer. Motorola personnel will act as facilitator, controller, and scribe for the exercise, ensuring the exercise meets established objectives, and documents key observations of participants.

After-Action Report

Motorola will conduct a facilitated debrief immediately upon completion of the exercise to solicit observations, gaps, and comments from all participants. Key observations and areas for further examination will be identified and recommended. Motorola will use these observations to provide an out brief presentation detailing the exercise, key takeaways, and recommendations to make any revisions to the scenario(s) included in the exercise and leverage lessons learned for the Customer to consider for future enhancements for their Incident Management and Response efforts.

7.3.3.2 Scope of Activity

Motorola will develop two (2) incident scenarios to use as the basis for walking through the plan with assembled Customer staff and leadership. Scenario products will be presented for approval by the Customer's assigned project leader.

- Motorola will facilitate the cybersecurity tabletop exercises.
- Motorola will coordinate the exercise timeline, define scope of the exercise and its key objectives, conduct, and steer the Incident Response Tabletop Exercise.
- Motorola facilitator will document observations and recommendations based on gaps in the plan or procedures identified during discussions.

7.3.3.3 Service Deliverables

Motorola will provide Customer with the following for the Incident Response Tabletop Exercise:

- Tabletop Exercise Facilitation.
- Final Presentation in PDF format which will include after action review, observations gap analysis, and recommendations.

7.4 Cybersecurity Tabletop Exercise

7.4.1 Cybersecurity Tabletop Exercise

As part of the Cybersecurity Incident Response Tabletop Exercise, Motorola will help plan, conduct, and facilitate a four (4) to six (6) hour tabletop exercise to walk through the Customer Incident Response (IR) plan with applicable Customer business units. The selection of which Customer business units participate will be at the discretion of the Customer CISO or Incident Response lead, and we will develop appropriate scenarios to address the appropriate elements of the Incident Response plan and level of involvement for each group. The plan walk-through will be conducted on the basis of scenarios designed to elicit discussion around key elements of the Incident Response plan. While the walk-through will focus on indoctrination to the plan, it will also provide opportunities to verify key assumptions in the plan.

7.4.1.1 Methodology

Motorola leverages lessons learned from years of experience using planning and execution practices based on the Homeland Security Exercise and Evaluation Program (HSEEP), a national standard for exercises, and our own objectives-based contingency planning and risk assessment methodology.

Our proposed process includes the following five key activities:

Identifying Exercise Objectives

Motorola will review Customer's participating stakeholders and gather background data on the information security and cybersecurity skill level of the staff, the current security capabilities of the organization, identify key threat scenarios, and response and coordination processes that may/may not be established. Motorola may conduct interviews or review documentation as part of this activity. Motorola will work with the Customer and exercise participants to draft, coordinate, and approve the scenario(s) and exercise objectives.

Developing and Design of the Exercise

Motorola will design the scenario(s) based on the information gathered from the interviews with the participating cooperatives and coordinate it with the Customer's exercise stakeholders. A collaborative process between the stakeholders to identify key concerns and response actions will then be used as a foundation for the exercise

Exercise

Motorola will facilitate a tabletop exercise over the agreed upon time involving stakeholders identified with the Customer. Motorola personnel will act as facilitator, controller, and scribe for the exercise, ensuring the exercise meets established objectives, and documents key observations of participants.

After-Action Report

Motorola will conduct a facilitated debrief immediately upon completion of the exercise to solicit observations, gaps, and comments from all participants. Key observations and areas for further examination will be identified and recommended. Motorola will use these observations to provide an out brief presentation detailing the exercise, key takeaways, and recommendations to make any revisions to the scenario(s) included in the exercise and leverage lessons learned for the Customer to consider for future enhancements for their Incident Management and Response efforts.

7.4.1.2 Scope of Activity

Motorola will develop two (2) incident scenarios to use as the basis for walking through the plan with assembled Customer staff and leadership. Scenario products will be presented for approval by the Customer's assigned project leader, at a minimum. It is encouraged that Customer suggests or select scenarios. Some common scenarios are listed below (this is not an exhaustive list):

- Ransomware
- Exploitation of a vulnerability or service
- Data Loss
- Equipment loss (theft, natural disaster)
- Insider Threat
- Malware
- Web Application attacks (ex: Cross-Site Scripting)
- Phishing
- Physical security breaches
- Loss of availability of a critical system (due to disaster or other event)
- Vendor/Supplier compromise

To facilitate the cybersecurity tabletop exercise, Motorola will coordinate the exercise timeline, define scope of the exercise and its key objectives, conduct, and steer the Cybersecurity Incident Response Tabletop Exercise. Motorola facilitator will document observations and recommendations based on gaps in the plan or procedures identified during discussions.

7.4.1.3 Service Deliverables

Motorola will provide Customer with the following for the Cybersecurity Incident Response Tabletop Exercise:

- Tabletop Exercise Facilitation.
- Final Presentation in PDF format which will include after action review, observations gap analysis, and recommendations.

Motorola will provide Customer with a comprehensive report providing details of the observations made during the exercise. Motorola will also provide a remediation plan which highlights opportunities for improvement. This includes two scenarios, onsite delivery, and two 3-hour sessions (recommended one executive and one technical).

7.5 Coordination & Assumptions

Coordination & Engagement Planning Call

Motorola recognizes the value and necessity of effective communication and ongoing collaboration with our customers throughout the life of an engagement. To ensure engagements get started off on the right track, Motorola has found it beneficial to begin with a structured engagement planning meeting,

typically by conference call. During the planning call, Motorola will facilitate a discussion of the following topics along with other engagement-specific items:

- Introduce key engagement participants.
- Establish communication protocols.
- Review scope of services and expected timelines for the delivery of services.
- Review communication, notification, and issue-escalation expectations and procedures.
- Determine the frequency of method of project status meetings (i.e., in-person, conference call, online meeting, etc.).
- Discuss other Customer requests and rules of engagement.
- Discuss the involvement of the Customer's staff in the project for knowledge transfer and security.
- Review the deliverables required at completion of the project, the designated recipient, and the manner in which Motorola will forward those deliverables.

Roles, Responsibilities, & Assumptions

Motorola used the following assumptions during development of this SOW. Any changes to these assumptions may affect the price and schedule commitments.

- Customer will assign a knowledgeable single point of contact for all issues that require escalation/resolution.
- Customer will provide Motorola access to the Customer's place of business, technical information, and facilities necessary to execute this engagement.
- Customer will ensure that appropriate personnel are available to meet with Motorola, as necessary, and provide timely response to all requests for information, revisions, and resources.
- The Motorola professional working day is eight and a half hours, including reasonable time for meals. Motorola understands that occasions arise during engagements that require a longer or shorter working day. Motorola will perform the work between 8:30am and 5:00pm (Customer's local time). After-hours and weekend must be explicitly identified in the Statement of Work or be otherwise specifically agreed to in writing by the parties. Motorola will request approval from Customer for any dates and times in which work will be performed.
- Motorola will always attempt to be flexible to meet Customer needs and will not extend engagements to our detriment when such delays result from the Customer's inability to reasonably meet stated prerequisites agreed to prior to an engagement, nor when delays result from Customer personnel not being reasonably available to provide required support.

7.6 Estimated Project Timeline

Milestones & Deliverables	Proposed Timeline
Penetration Testing Service – External Penetration Testing – Retesting **Cybersecurity Health Check** – Cyber Security Risk Assessment – Vulnerability Scan and Results Assessment – Firewall Review – Physical Security Assessment **Cybersecurity Tabletop Exercise** – Cybersecurity Incident Response – Ransomware	Begin based on Customer authorization
Phase 1 – Information Exchange Motorola and Customer will set specific assessment & deliverable dates, review information on infrastructure required for assessment, and exchange contact information.	Week One
Phase 2 – Active Assessment Active assessment will take place based on agreed to schedule.	Weeks Two, Three
Phase 3 – Report Writing & QA Draft reports written and QA of reports performed prior to delivery to Customer.	Weeks Four, Five
Phase 4 – Draft Reports Delivered Draft report delivered to Customer. Reviewed by Customer prior to Draft Report review call.	Week Six, Seven
Phase 5 – Draft Report Review & Final Report Delivered Motorola and Customer discuss findings, recommendations, and review reports. Motorola will make any required adjustments to the draft report and return to Customer as a final report.	Week Eight

Milestones & Deliverables	Proposed Timeline
Incident Management and Response – Incident Response Plan Review and Development – Cybersecurity Incident Response Tabletop Exercise – Incident Management Training	Begin based on Customer authorization
Phase 1 – Information Gathering Motorola and Customer will determine Customer expectations and Incident Response scope by Identifying risks, regulatory, contractual, industry and other requirements. Motorola will assess Customer's current state of incident response, including security policies, procedures, and practices.	Week One

Milestones & Deliverables	Proposed Timeline
Motorola will interview key stakeholders during the information gathering phase.	
Phase 2 – Develop Incident Response Plan Motorola will document response procedures for addressing a range of cyber incidents or attacks. **Develop Exercise Plan, Incident Management Training** Conduct in-brief at Customer location to baseline expectations of participants exercise and training.	Weeks Two, Three
Phase 3 – Exercise Execution During the exercise and training, Motorola will facilitate and control two to three Incident Response scenarios.	Weeks Four, Five
Phase 4 – Draft and Final Review Motorola will provide a draft plan to client for review. Upon approval of draft, Motorola will provide final copy of Incident Response Plan.	Week Six

7.7 Responsibilities

Motorola Responsibilities

- **Project Lead.** Motorola will assign a project lead to oversee the engagement, interface with Customer's project management team and provide project status as needed during the assessment.
- **Experienced and Senior Security Professional.** Motorola will provide one Cybersecurity subject matter expert who will:
  - Conduct a kick-off meeting with Customer to identify the scope of the assessment.
  - Conduct the elements of the in-scope activities with the assistance of Customer's technical point of contact.
  - Conduct an off-site analysis of the data collected and generate the final report.
  - Create a final summary presentation of the results and conduct a review of the assessment results with the Customer.
  - Motorola will provide one (1) PDF electronic copy of the presentation to the Customer.
- **Recommended Assessment Sites/Locations.** All site locations must be within a 70-mile radius or additional charges will be assessed. Motorola resources will perform a physical inspection and technical evaluation on the number of sites listed in Table 6-1: Customer Site Information.
  - Motorola may perform inspections and technical evaluations of additional sites if they can be completed within the time allotted for the in-scope site visit.
- **Deliverables.** Motorola will provide the following deliverables as an output of the in-scope activity:
  - **Cybersecurity assessment report and accompanying presentation** - The report and accompanying presentation outlines the findings of the cybersecurity assessment and provides an overview of the cybersecurity risk posture.

- **Single Report** – Motorola will provide one (1) comprehensive cybersecurity risk assessment report for assessments included in the statement of work for this proposal.

Customer Responsibilities

- **Confirmation of Scope.** Customer will receive and must acknowledge in writing the Cybersecurity Professional Service Statement of Work provided by Motorola prior to initiating the service.
- **Kickoff Support**. Customer will participate in the kickoff meeting, which identifies the scope of the assessment.
- **Contacts.** Customer will appoint at least one (1) primary contact, including a project manager, and one (1) technical point of contact that are trained and knowledgeable of the project objectives to assist Motorola's project lead and Motorola's security engineer and answer any technical or business process questions. Customer's partners, consultants or any third parties involved in the project shall likewise provide access to their resources, and shall not restrict access by Motorola to Customer resources.
- **Reasonable Access to Resources.** Customer will provide reasonable access to necessary resources as requested by the project manager, including access to the applicable facilities, network equipment and systems. Where access directly by the Motorola security engineer is not permissible, Customer must provide the necessary technical expertise to acquire the necessary data or information for Motorola.
- **Reasonable Access to Information.** Customer will provide Motorola with reasonable access to any information necessary to facilitate the project. Such requests may include site plans, facility layout, network topography or other documentation. Where access directly by the Motorola engineer is not permissible, customer must provide the necessary technical expertise to acquire the necessary data or information for Motorola.
- **Site Conditions.** Customer will ensure that all work sites it provides will be safe, secure, and in compliance with all applicable industry and Occupational Safety and Health Administration (OSHA) standards (or relevant national governance body equivalent).
- **Customer Review.** Customer will review project documentation as it is received to provide feedback for appropriate and timely discussions and changes.
- **On-Site Services.** Customer and Motorola will agree on the dates and times associated with Motorola's on-site activities. Customer will provide the necessary access and resources, as described above, throughout those periods.
- **Access to Workspace, Telephone and Internet.** Customer will provide access to workspace, telephone and Internet connectivity to Motorola during the project. This access will be used solely for purposes of project execution.
- **Physical Access on-Site.** Customer will provide any escort, badges, security personnel, labor resources or other necessary assistance to enable Motorola's access to required work areas on site. Customer is responsible for all costs associated with availability and use of these resources.
- **Third-Party Equipment, Software and Services.** Unless specifically provided by Motorola's service delivery team described herein, Customer is responsible for all third-party services, equipment and software associated with this service.
- **Project Changes.** Customer will communicate schedule changes for tasks or phase events to the Motorola project lead. Customer understands such changes may lead to additional costs for which Customer will be responsible.

Section 8

Limitations and Clarifications

Motorola's ASTRO MDR service does not include services to perform physical containment and/or remediation of confirmed security incidents, remote or onsite. The Customer may choose to purchase additional Incident Response professional services to assist in the creation of and/or completion of a Customer's Incident Response Plan.

Motorola's scope of services does not include responsibilities relating to active protection of customer data, including its transmission to Motorola, recovery of data available through the products or services, or remediation or responsibilities relating to the loss of data, ransomware, or hacking.

8.1.1 Service Limitations

Cybersecurity services are inherently limited and will not guarantee that the Customer's system will be error-free or immune to security breaches as a result of any or all of the services described in this SOW. Motorola does not warrant or guarantee that this service will identify all cybersecurity incidents that occur in the Customer's system. Services and deliverables are limited by, among other things, the evolving and often malicious nature of cyber threats, conduct/attacks, as well as the complexity/disparity and evolving nature of Customer computer system environments, including supply chains, integrated software, services, and devices. To the extent we do offer recommendations in connection with the services, unless otherwise stated in the Statement of Work, our recommendations are necessarily subjective, may or may not be correct, and may be based on our assumptions relating to the relative risks, priorities, costs and benefits that we assume apply to you.

8.1.2 Processing of Customer Data in the United States and/or other Locations

Customer understands and agrees that data obtained, accessed, or utilized in the performance of the services may be transmitted to, accessed, monitored, and/or otherwise processed by Motorola in the U.S. and/or other Motorola operations globally. Customer consents to and authorizes all such processing and agrees to provide, obtain, or post any necessary approvals, consents, or notices that may be necessary to comply with applicable law.

8.1.3 Customer and Third-Party Information

Customer understands and agrees that Motorola may obtain, use and/or create and use, anonymized, aggregated and/or generalized Customer Data, such as data relating to actual and potential security threats and vulnerabilities, for its lawful business purposes, including improving its services and sharing and leveraging such information for the benefit of Customer, other customers, and other interested parties. For avoidance of doubt, so long as not specifically identifying the Customer, Customer Data shall not include, and Motorola shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, third party threat vectors and IP addresses (i.e., so long as not defined as personal information under applicable law), file hash information, domain names, malware signatures and information, information obtained from third party sources, indicators of

compromise, and tactics, techniques, and procedures used, learned or developed in the course of providing Services, which data shall be deemed Service Use Data (i.e., Motorola data).

8.1.4 Third-Party Software and Service Providers, including Resale

Motorola may use, engage, license, resell, interface with or otherwise utilize the products or services of third-party processors or sub-processors and other third-party software, hardware, or services providers (such as, for example, third-party endpoint detection and response providers). Such processors and sub-processors may engage additional sub-processors to process personal data and other Customer Data. Customer understands and agrees that the use of such third-party products and services, including as it relates to any processing or sub-processing of data, is subject to each respective third-party's own terms, licenses, End User License Agreements (EULA), privacy statements, data processing agreements and/or other applicable terms. Such third-party providers and terms may include the following, if applicable, or as otherwise made available publicly, through performance, or upon request.

Motorola disclaims any and all responsibility for any and all loss or costs of any kind associated with security events. Motorola disclaims any responsibility for customer use or implementation of any recommendations provided in connection with the services. Implementation of recommendations does not ensure or guarantee the security of the systems and operations evaluated.

Section 9

Proposal Pricing

9.1 Pricing Summary

Motorola pricing is based on the services and solution presented in Section 2. The addition or deletion of any component(s) may subject the total solution price to modifications.

Description	
ASTRO® 25 Managed Detection and Response	$180,313.69
ActiveEye Managed Detection and Response supporting PremierOne and CC Environment	$85,605.72
Cybersecurity Professional Services	$316,480.00
Customer Loyalty Discount for signing by December 13, 2024	-$124,434.00
Sales Tax	$3,312.08
Year 1 Total	**$461,277.49**

Initial Subscription Period after Year 1:

Description					
	ASTRO MDR	**PremierOne MDR**	**Professional Services**	**Total**	***Not to Exceed**
Initial Subscription Period - Year 2	$87,352.18	$73,763.03	$130,790.40	$291,905.61	$312,039.01
Initial Subscription Period - Year 3	$90,846.27	$76,713.55	$136,022.03	$303,581.85	$324,832.58

*The not to exceed amount is calculated in accordance with the Inflation Adjustment prevision outlined in section 9.2 to account for inflation adjustment (if applicable).

The Total Contract Value of this proposal is: NOT TO EXCEED $1,098,149.08.

9.2 Payment Schedule & Terms

Period of Performance

The initial MDR subscription period of the contract will extend three (3) years, from the Commencement Date of Service, defined as the date of the last signature on the agreement, or not later than thirty (30) days after Motorola provides the Customer with necessary hardware or software.

Professional Services will begin approximately three (3) months after contract execution and are contingent upon completion of any related equipment/installation configuration. The project will follow the general schedule shown in Section 7.6.

Term

The Term of the contract begins on the Commencement Date of Service and remains in effect until the expiration of the initial period so specified.

Billing

Upon acceptance of this proposal by the Customer, Motorola will invoice the Customer for all service fees in advance for the full Year 1 amount according to the Pricing table in Section 9.1.

Thereafter, Motorola will invoice the Customer annually, in advance for (a) the Services to be performed (as applicable); and (b) any other charges incurred as agreed upon between the parties during the term of the subscription.

Customer will make payments to Motorola within thirty (30) days after receipt of each invoice. Customer will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a United States financial institution.

Inflation Adjustment. For multi-year agreements, at the end of the first year of the Agreement and each year thereafter, a CPI percentage change calculation shall be performed using the U.S. Department of Labor, Consumer Price Index, all Items, Unadjusted Urban Areas (CPI-U). Should the annual inflation rate increase greater than 3% during the previous year, Motorola shall have the right to increase all future maintenance prices by the CPI increase amount exceeding 3%. All items, not seasonally adjusted shall be used as the measure of CPI for this price adjustment. Measurement will take place once the annual average for the new year has been posted by the Bureau of Labor Statistics. The adjustment rate shall not exceed 7% for any adjustment period. For purposes of illustration, if in year 5 the CPI reported an increase of 11%, Motorola may increase the Year 6 price by 7% (11%-3% base, but not to exceed 7%).

Customer affirms they have signatory authority to execute this contract. The contract price, Not to Exceed $1,098,149.08, is fully committed and identified, including all subsequent years of contracted services, if applicable, subject to SECTION 4 – Termination Due to Non-Appropriation of Funds. The Customer will pay all invoices as received from Motorola and any changes in scope will be subject to the change order process as described in this Agreement.

Motorola acknowledges the Customer may require the issuance(s) of a purchase order or notice to proceed as part of the Customer's procurement process. However, Customer agrees that the issuance or non-issuance of a purchase order or notice to proceed does not preclude the Customer from its contractual obligations as defined in this Agreement.

Tax

Unless otherwise noted, this proposal excludes sales tax or other applicable taxes (such as Goods and Services Tax, Value Added Tax and other taxes of a similar nature). Any tax the customer is subject to will be added to invoices.

9.3 Invoicing and Shipping Addresses

Invoices will be sent to Customer at the following address:	
Name:	
Address:	
Phone:	
Email:	
Address of Ultimate Destination for Equipment to be Delivered to Customer:	

Name:	
Address:	
Equipment Shipped to Customer at the following address:	
Name:	
Address:	
Phone:	

Section 10

Contractual Documentation

PRODUCTS AND SERVICES AGREEMENT

This Products and Services Agreement (this "**Agreement**") is entered into between **Motorola Solutions Inc.**, ("**Seller**" or "**Motorola**") and the entity set forth in section I(b) ("**Customer**") as of the date last signed below ("Effective Date"). Seller and Customer will each be referred to herein as a "**Party**" and collectively as the "**Parties**".

I. Seller and Customer Information

(a)	Seller	Motorola Solutions, Inc.
(b)	Customer	Name: Port of Los Angeles Address: 425 South Palos Verdes Street San Pedro, CA 90731 Contact: Captain Daniel R. Cobos

II. Transaction Details

(a)	Proposal	Proposal No.: 24-175548 Date: July 8, 2024 Motorola will provide Customer with the products and services set forth in the proposal dated above (the "Proposal"), a copy of which is attached hereto and incorporated herein.
(b)	Pricing	Pricing for products and services being purchased by Customer is set forth in the Proposal.
(c)	Terms and Conditions	The Parties acknowledge and agree that the terms of the Motorola Customer Agreement ("MCA"), including all applicable addenda, are incorporated herein and shall apply to the products and services provided to Customer as set forth in the Proposal. A copy of the MCA is available upon request.

III. Entire Agreement

This Agreement, including the Proposal and any terms and conditions referenced herein, constitutes the entire agreement of the Parties regarding the subject matter of the Agreement and supersedes all previous agreements, proposals, and understandings, whether written or oral, relating to this subject matter. This Agreement may be executed in multiple counterparts, and shall have the same legal force and effect as if the Parties had executed it as a single document. The Parties may sign in writing, or by electronic signature, including by email. An electronic signature, or a facsimile copy or computer image, such as a PDF or tiff image, of a signature, shall be treated as and shall have the same effect as an original signature. In addition, an electronic signature, a true and correct facsimile copy or computer image of this Agreement shall be treated as and shall have the same effect as an original signed copy of this document. This Agreement may be amended or modified only by a written instrument signed by authorized representatives of both Parties. The preprinted terms and conditions found on any Customer purchase or purchase order, acknowledgment or other form will not be considered an amendment or modification of this Agreement, even if a representative of each Party signs that document, and the terms of this Agreement will take precedence.

CUSTOMER:	MOTOROLA SOLUTIONS INC.
By:_____	By:_____
Print Name:_____	Print Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

MONTHLY SUBCONSULTANT MONITORING REPORT

Instructions: Please indicate the SBE/VSBE/MBE/WBE/OBE/DBE participation levels achieved for the month of _____covered by the referenced contract number.

Contract No. | Division | Contractor Administrator

Contractor | *Group | Contract Title/Project

Contract Amount | Start Date | End Date

Total Amount Invoiced to Date

SBE Mandated Participation Percentage | SBE | VSBE

Proposed Subcontractor Percentage | MBE | WBE | OBE | DVBE

				PROPOSED		ACTUALS		
	Name of Subcontractor	Type of Work Performed	Group SBE/VSBE/MBE/WBE/OBE/DVBE	Original Proposed Amount	Original Proposed Percentage	Amount Paid to Date	Amount Paid to Date Percentage	Contract Amount Percentage
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

Directions:

Original Proposed Percentage: Original Proposed Percentage of Total Contract Amount

Amount Paid to Date Percentage: Percentage of Total Amount Invoiced to Date

Contract Amount Percentage: Percentage Paid to Date of Total Contract Amount

EXHIBIT B

* Group = (SBE/VSBE/MBE/WBE/OBE/DVBE/DBE)

EXHIBIT C - AFFIRMATIVE ACTION PROGRAM PROVISIONS

Sec. 10.8.4 Affirmative Action Program Provisions.

Every non-construction and construction Contract with, or on behalf of, the City of Los Angeles for which the consideration is $25,000 or more shall contain the following provisions which shall be designated as the AFFIRMATIVE ACTION PROGRAM provisions of such Contract:

A. During the performance of a City Contract, the Contractor certifies and represents that the Contractor and each Subcontractor hereunder will adhere to an Affirmative Action Program to ensure that in its employment practices, persons are employed and employees are treated equally and without regard to or because of race, color, religion, national origin, ancestry, sex, sexual orientation, age, disability, marital status, domestic partner status or medical condition.

1. This section applies to work or services performed or materials manufactured or assembled in the United States.

2. Nothing in this section shall require or prohibit the establishment of new classifications of employees in any given craft, work or service category.

3. The Contractor shall post a copy of Paragraph A., hereof, in conspicuous places at its place of business available to employees and applicants for employment.

B. The Contractor shall, in all solicitations or advertisements for employees placed, by or on behalf of, the Contractor, state that all qualified applicants will receive consideration for employment without regard to their race, color, religion, national origin, ancestry, sex, sexual orientation, age, disability, marital status, domestic partner status or medical condition.

C. At the request of the Awarding Authority or the DAA, the Contractor shall certify on an electronic or hard copy form to be supplied, that the Contractor has not discriminated in the performance of City Contracts against any employee or applicant for employment on the basis or because of race, color, religion, national origin, ancestry, sex, sexual orientation, age, disability, marital status, domestic partner status or medical condition.

D. The Contractor shall permit access to, and may be required to provide certified copies of, all of its records pertaining to employment and to its employment practices by the Awarding Authority or the DAA for the purpose of investigation to ascertain compliance with the Affirmative Action Program provisions of City Contracts and, upon request, to provide evidence that it has or will comply therewith.

E. The failure of any Contractor to comply with the Affirmative Action Program provisions of City Contracts may be deemed to be a material breach of a City Contract. The failure shall only be established upon a finding to that effect by the Awarding

Authority, on the basis of its own investigation or that of the DAA. No finding shall be made except upon a full and fair hearing after notice and an opportunity to be heard has been given to the Contractor.

F. Upon a finding duly made that the Contractor has breached the Affirmative Action Program provisions of a City Contract, the Contract may be forthwith cancelled, terminated or suspended, in whole or in part, by the Awarding Authority, and all monies due or to become due hereunder may be forwarded to and retained by the City of Los Angeles. In addition thereto, the breach may be the basis for a determination by the Awarding Authority or the Board of Public Works that the Contractor is a non-responsible bidder or proposer pursuant to the provisions of Section 10.40 of this Code. In the event of such determination, the Contractor shall be disqualified from being awarded a contract with the City of Los Angeles for a period of two years, or until he or she shall establish and carry out a program in conformance with the provisions hereof.

G. In the event of a finding by the Fair Employment and Housing Commission of the State of California, or the Board of Public Works of the City of Los Angeles, or any court of competent jurisdiction, that the Contractor has been guilty of a willful violation of the California Fair Employment and Housing Act, or the Affirmative Action Program provisions of a City Contract, there may be deducted from the amount payable to the Contractor by the City of Los Angeles under the contract, a penalty of ten dollars for each person for each calendar day on which the person was discriminated against in violation of the provisions of a City Contract.

H. Notwithstanding any other provisions of a City Contract, the City of Los Angeles shall have any and all other remedies at law or in equity for any breach hereof.

I. The Public Works Board of Commissioners shall promulgate rules and regulations through the DAA and provide to the Awarding Authorities electronic and hard copy forms for the implementation of the Affirmative Action Program provisions of City contracts, and rules and regulations and forms shall, so far as practicable, be similar to those adopted in applicable Federal Executive Orders. No other rules, regulations or forms may be used by an Awarding Authority of the City to accomplish this contract compliance program.

J. Nothing contained in City Contracts shall be construed in any manner so as to require or permit any act which is prohibited by law.

K. By affixing its signature to a Contract that is subject to this article, the Contractor shall agree to adhere to the provisions in this article for the duration of the Contract. The Awarding Authority may also require Contractors and suppliers to take part in a pre-registration, pre-bid, pre-proposal, or pre-award conference in order to develop, improve or implement a qualifying Affirmative Action Program.

1. The Contractor certifies and agrees to immediately implement good faith effort measures to recruit and employ minority, women and other potential employees in

a non-discriminatory manner including, but not limited to, the following actions as appropriate and available to the Contractor's field of work. The Contractor shall:

(a) Recruit and make efforts to obtain employees through:

(i) Advertising employment opportunities in minority and other community news media or other publications.

(ii) Notifying minority, women and other community organizations of employment opportunities.

(iii) Maintaining contact with schools with diverse populations of students to notify them of employment opportunities.

(iv) Encouraging existing employees, including minorities and women, to refer their friends and relatives.

(v) Promoting after school and vacation employment opportunities for minority, women and other youth.

(vi) Validating all job specifications, selection requirements, tests, etc.

(vii) Maintaining a file of the names and addresses of each worker referred to the Contractor and what action was taken concerning the worker.

(viii) Notifying the appropriate Awarding Authority and the DAA in writing when a union, with whom the Contractor has a collective bargaining agreement, has failed to refer a minority, woman or other worker.

(b) Continually evaluate personnel practices to assure that hiring, upgrading, promotions, transfers, demotions and layoffs are made in a non-discriminatory manner so as to achieve and maintain a diverse work force.

(c) Utilize training programs and assist minority, women and other employees in locating, qualifying for and engaging in the training programs to enhance their skills and advancement.

(d) Secure cooperation or compliance from the labor referral agency to the Contractor's contractual Affirmative Action Program obligations.

(e) Establish a person at the management level of the Contractor to be the Equal Employment Practices officer. Such individual shall have the authority to disseminate and enforce the Contractor's Equal Employment and Affirmative Action Program policies.

(f) Maintain records as are necessary to determine compliance with Equal Employment Practices and Affirmative Action Program obligations and make the records available to City, State and Federal authorities upon request.

(g) Establish written company policies, rules and procedures which shall be encompassed in a company-wide Affirmative Action Program for all its operations and Contracts. The policies shall be provided to all employees, Subcontractors, vendors, unions and all others with whom the Contractor may become involved in fulfilling any of its Contracts.

(h) Document its good faith efforts to correct any deficiencies when problems are experienced by the Contractor in complying with its obligations pursuant to this article. The Contractor shall state:

(i) What steps were taken, how and on what date.

(ii) To whom those efforts were directed.

(iii) The responses received, from whom and when.

(iv) What other steps were taken or will be taken to comply and when.

(v) Why the Contractor has been or will be unable to comply.

2. Every contract of $25,000 or more which may provide construction, demolition, renovation, conservation or major maintenance of any kind shall also comply with the requirements of Section 10.13 of the Los Angeles Administrative Code.

L. The Affirmative Action Program required to be submitted hereunder and the pre-registration, pre-bid, pre-proposal or pre-award conference which may be required by the Awarding Authority shall, without limitation as to the subject or nature of employment activity, be concerned with such employment practices as:

1. Apprenticeship where approved programs are functioning, and other on-the-job training for non-apprenticeable occupations;

2. Classroom preparation for the job when not apprenticeable;

3. Pre-apprenticeship education and preparation;

4. Upgrading training and opportunities;

5. Encouraging the use of Contractors, Subcontractors and suppliers of all racial and ethnic groups; provided, however, that any contract subject to this ordinance shall require the Contractor, Subcontractor or supplier to provide not less than the prevailing wage, working conditions and practices generally observed in private industries in the Contractor's, Subcontractor's or supplier's geographical area for such work;

6. The entry of qualified women, minority and all other journeymen into the industry; and

7. The provision of needed supplies or job conditions to permit persons with disabilities to be employed, and minimize the impact of any disability.

M. Any adjustments which may be made in the Contractor's work force to achieve the requirements of the City's Affirmative Action Program in purchasing and construction shall be accomplished by either an increase in the size of the work force or replacement of those employees who leave the work force by reason of resignation, retirement or death and not by termination, layoff, demotion or change in grade.

N. This ordinance shall not confer upon the City of Los Angeles or any Agency, Board or Commission thereof any power not otherwise provided by law to determine the legality of any existing collective bargaining agreement and shall have application only to discriminatory employment practices by Contractors engaged in the performance of City Contracts.

O. All Contractors subject to the provisions of this article shall include a similar provision in all subcontracts awarded for work to be performed under the Contract with the City and shall impose the same obligations including, but not limited to, filing and reporting obligations, on the Subcontractors as are applicable to the Contractor. Failure of the Contractor to comply with this requirement or to obtain the compliance of its Subcontractors with all such obligations shall subject the Contractor to the imposition of any and all sanctions allowed by law, including, but not limited to, termination of the Contractor's Contract with the City.

EXHIBIT D

(1) SMALL/VERY SMALL BUSINESS ENTERPRISE PROGRAM

(2) LOCAL BUSINESS PREFERENCE PROGRAM

(1) SMALL/VERY SMALL BUSINESS ENTERPRISE PROGRAM:

The Harbor Department is committed to creating an environment that provides all individuals and businesses open access to the business opportunities available at the Harbor Department in a manner that reflects the diversity of the City of Los Angeles. The Harbor Department's Small Business Enterprise (SBE) Program was created to provide additional opportunities for small businesses to participate in professional service and construction contracts. An overall Department goal of 25% SBE participation, including 5% Very Small Business Enterprise (VSBE) participation, has been established for the Program. The specific goal or requirement for each contract opportunity may be higher or lower based on the scope of work.

It is the policy of the Harbor Department to solicit participation in the performance of all service contracts by all individuals and businesses, including, but not limited to, SBEs, VSBEs, women-owned business enterprises (WBEs), minority-owned business enterprises (MBEs), and disabled veteran business enterprises (DVBEs). The SBE Program allows the Harbor Department to target small business participation, including MBEs, WBEs, and DVBEs, more effectively. It is the intent of the Harbor Department to make it easier for small businesses to participate in contracts by providing education and assistance on how to do business with the City, and ensuring that payments to small businesses are processed in a timely manner. **In order to ensure the highest participation of SBE/VSBE/MBE/WBE/DVBEs, all proposers shall utilize the City's contracts management and opportunities database, the Los Angeles Business Assistance Virtual Network (LABAVN), at http://www.labavn.org, to outreach to potential subconsultants.**

The Harbor Department defines a SBE as an independently owned and operated business that is not dominant in its field and meets criteria set forth by the Small Business Administration in Title 13, Code of Federal Regulations, Part 121. Go to www.sba.gov for more information. The Harbor Department defines a VSBE based on the State of California's Micro-business definition which is 1) a small business that has average annual gross receipts of $3,500,000 or less within the previous three years, or (2) a small business manufacturer with 25 or fewer employees.

The SBE Program is a results-oriented program, requiring consultants who receive contracts from the Harbor Department to perform outreach and utilize certified small businesses. **Based on the work to be performed, it has been determined that the percentage of small business participation will be 0 %, including 0% VSBE participation**. The North American Industry Classification System (NAICS) Code for the scope of services is 541511. This NAICS Code is the industry code that corresponds to at least 51% of the scope of services and will be used to determine the size standard for SBE participation of the Prime Consultant. The maximum SBE size standard for this NAICS Code is $34 million.

Consultant shall be responsible for determining the SBE status of its subconsultants for purposes of meeting the small business requirement. Subconsultants must qualify as an SBE based on the type of services that they will be performing under the Agreement. All business participation will be determined by the percentage of the total amount of compensation under the agreement paid to SBEs. The Consultant shall not substitute an SBE firm without obtaining prior approval of the City. A request for substitution must be based upon demonstrated good cause. If substitution is permitted, Consultant shall endeavor to make an in-kind substitution for the substituted SBE.

Consultant shall complete, sign, and submit as part of the executed agreement the attached Affidavit and Consultant Description Form. The Affidavit and Consultant Description Form, when signed, will signify the Consultant's intent to comply with the SBE requirement. All SBE/VSBE firms must be certified by the time proposals are due to receive credit. In addition all consultants and subconsultants must be registered on the LABAVN by the time proposals are due.

(2) LOCAL BUSINESS PREFERENCE PROGRAM:

The Harbor Department is committed to maximizing opportunities for local and regional businesses, as well as encouraging local and regional businesses to locate and operate within the Southern California region. It is the policy of the Harbor Department to support an increase in local and regional jobs. The Harbor Department's Local Business Preference Program (LBPP) aims to benefit the Southern California region by increasing jobs and expenditures within the local and regional private sector.

Consultants who qualify as a Local Business Enterprise (LBE) will receive an 8% preference on any proposal for services valued in excess of $150,000. The preference will be applied by adding 8% of the total possible evaluation points to the Consultant's score. Consultants who do not qualify as a LBE may receive a maximum 5% preference for identifying and utilizing LBE subconsultants. Consultants may receive 1% preference, up to a maximum of 5%, for every 10% of or portion thereof, of work that is subcontracted to a LBE. LBE subconsultant preferences will be determined by the percentage of the total amount of compensation proposed under the Agreement.

The Harbor Department defines a LBE as:

(a) A business headquartered within Los Angeles, Orange, Riverside, San Bernardino, or Ventura Counties. Headquartered shall mean that the business physically conducts and manages all of its operations from a location in the above-named counties; or

(b) A business that has at least 50 full-time employees, or 25 full-time employees for specialty marine contracting firms, working in Los Angeles, Orange, Riverside, San Bernardino, or Ventura Counties.

In order for Harbor Department staff to determine the appropriate LBE preference, Consultant shall complete, sign, notarize (where applicable) and submit the attached Affidavit and Consultant Description Form. The Affidavit and Consultant Description Form will signify the LBE status of the Consultant and subconsultants.

In the event of Consultant's noncompliance during the performance of the Agreement, Consultant shall be considered in material breach of contract. In addition to any other remedy available to City under this Agreement or by operation of law, the City may withhold invoice payments to Consultant until noncompliance is corrected, and assess the costs of City's audit of books and records of Consultant and its subconsultants. In the event the Consultant falsifies or misrepresents information contained in any form or other willful noncompliance as determined by City, City may disqualify the Consultant from participation in City contracts for a period of up to five (5) years.

AFFIDAVIT OF COMPANY STATUS

"The undersigned declares under penalty of perjury pursuant to the laws of the State of California that the following information and information contained on **the attached Consultant Description Form** is true and correct and includes all material information necessary to identify and explain the operations of

Motorola Solutions, Inc.

Name of Firm

as well as the ownership and location thereof. Further, the undersigned agrees to provide complete and accurate information regarding ownership in the named firm, and all of its domestic and foreign affiliates, any proposed changes of the ownership and to permit the audit and examination of firm ownership documents, and the ownership documents of all of its domestic and foreign affiliates, in association with this agreement."

(1) **Small/Very Small Business Enterprise Program:** Please indicate the ownership of your company. Please check all that apply. At least one box must be checked:

☐ SBE ☐ VSBE ☐ MBE ☐ WBE ☐ DVBE ☒ OBE

- A Small Business Enterprise (SBE) is an independently owned and operated business that is not dominant in its field and meets criteria set forth by the Small Business Administration in Title 13, Code of Federal Regulations, Part 121.
- A Very Small Business Enterprise (VSBE) is 1) a small business that has average annual gross receipts of $3,500,000 or less within the previous three years, or (2) a small business manufacturer with 25 or fewer employees.
- A Minority Business Enterprise (MBE) is defined as a business in which a minority owns and controls at least 51% of the business. A Woman Business (WBE) is defined as a business in which a woman owns and controls at least 51% of the business. For the purpose of this project, a minority includes:
  - (1) Black (all persons having origins in any of the Black African racial groups not of Hispanic origin);
  - (2) Hispanic (all persons of Mexican, Puerto Rican, Cuban, Central or South American or other Spanish Culture or origin, regardless of race);
  - (3) Asian and Pacific Islander (all persons having origins in any of the original peoples of the Far East, Southeast Asia, The Indian Subcontinent, or the Pacific Islands); and
  - (4) American Indian or Alaskan Native (all persons having origins in any of the original peoples of North America and maintaining identifiable tribal affiliations through membership and participation or community identification).
- A Disabled Veteran Business Enterprise (DVBE) is defined as a business in which a disabled veteran owns at least 51% of the business, and the daily business operations are managed and controlled by one or more disabled veterans.
- An OBE (Other Business Enterprise) is any enterprise that is neither an SBE, VSBE, MBE, WBE, or DVBE.

(2) **Local Business Preference Program:** Please indicate the Local Business Enterprise status of your company. Only one box must be checked:

☐ LBE ☒ Non-LBE

- A Local Business Enterprise (LBE) is: (a) a business headquartered within Los Angeles, Orange, Riverside, San Bernardino, or Ventura Counties; or (b) a business that has at least 50 full-time employees, or 25 full-time employees for specialty marine contracting firms, working in Los Angeles, Orange, Riverside, San Bernardino, or Ventura Counties. "Headquartered" shall mean that the business physically conducts and manages all of its operations from a location in the above-named counties.
- A Non-LBE is any business that does not meet the definition of a LBE.

Signature: Kenneth Senkel Title: Commercial Counsel

Printed Name: ~~Kenneth Senkel~~ Date Signed: July 12, 2024

Consultant Description Form

PRIME CONSULTANT:

Contract Title: Cybersecurity Managed Detection & Response and Professional Services

Business Name: Motorola Solutions, Inc. LABAVN ID#: 2406

Award Total: $ $1,177,786.87

Owner's Ethnicity: n/a Gender n/a Group: SBE VSBE MBE WBE DVBE OBE (Circle all that apply)

Local Business Enterprise: YES_____NO__x__(Check only one)

Primary NAICS Code: 541519 Average Three Year Gross Revenue: $ 27.25 B

Address: 500 W. Monroe Street,

City/State/Zip: Chicago, IL 60661

County: Cook

Telephone: (847 576-5000 FAX: ( )

Contact Person/Title: Michael Conrey - Account Manager

Email Address: michael.conrey1@motorolasolutions.com

SUBCONSULTANT:

Business Name: _____ LABAVN ID#: _____

Award Total: (% or $): _____

Services to be provided: _____

Owner's Ethnicity: _____Gender _____Group: SBE VSBE MBE WBE DVBE OBE (Circle all that apply)

Local Business Enterprise: YES_____NO_____(Check only one)

Primary NAICS Code: _____ Average Three Year Gross Revenue: $_____

Address: _____

City/State/Zip: _____

County: _____

Telephone: ( ) _____ FAX: ( ) _____

Contact Person/Title: _____

Email Address: _____

SUBCONSULTANT:

Business Name: _____ LABAVN ID#: _____

Award Total: (% or $): _____

Services to be provided: _____

Owner's Ethnicity: _____Gender _____Group: SBE VSBE MBE WBE DVBE OBE (Circle all that apply)

Local Business Enterprise: YES_____NO_____(Check only one)

Primary NAICS Code: _____ Average Three Year Gross Revenue: $_____

Address: _____

City/State/Zip: _____

County: _____

Telephone: ( ) _____ FAX: ( ) _____

Contact Person/Title: _____

Email address: _____

Consultant Description Form

SUBCONSULTANT:

Business Name: _____ LABAVN ID#: _____

Award Total: (% or $): _____

Services to be provided: _____

Owner's Ethnicity: _____Gender _____Group: SBE VSBE MBE WBE DVBE OBE (Circle all that apply)

Local Business Enterprise: YES_____NO_____(Check only one)

Primary NAICS Code: _____ Average Three Year Gross Revenue: $_____

Address: _____

City/State/Zip: _____

County: _____

Telephone: ( ) _____ FAX: ( ) _____

Contact Person/Title: _____

Email Address: _____

SUBCONSULTANT:

Business Name: _____ LABAVN ID#: _____

Award Total: (% or $): _____

Services to be provided: _____

Owner's Ethnicity: _____Gender _____Group: SBE VSBE MBE WBE DVBE OBE (Circle all that apply)

Local Business Enterprise: YES_____NO_____(Check only one)

Primary NAICS Code: _____ Average Three Year Gross Revenue: $_____

Address: _____

City/State/Zip: _____

County: _____

Telephone: ( ) _____ FAX: ( ) _____

Contact Person/Title: _____

Email Address: _____

SUBCONSULTANT:

Business Name: _____ LABAVN ID#: _____

Award Total: (% or $): _____

Services to be provided: _____

Owner's Ethnicity: _____Gender _____Group: SBE VSBE MBE WBE DVBE OBE (Circle all that apply)

Local Business Enterprise: YES_____NO_____(Check only one)

Primary NAICS Code: _____ Average Three Year Gross Revenue: $_____

Address: _____

City/State/Zip: _____

County: _____

Telephone: ( ) _____ FAX: ( ) _____

Contact Person/Title: _____

Email address: _____

EXHIBIT E

Sec. 10.8.2.1. Equal Benefits Ordinance.

Discrimination in the provision of employee benefits between employees with domestic partners and employees with spouses results in unequal pay for equal work. Los Angeles law prohibits entities doing business with the City from discriminating in employment practices based on marital status and/or sexual orientation. The City's departments and contracting agents are required to place in all City contracts a provision that the company choosing to do business with the City agrees to comply with the City's nondiscrimination laws.

It is the City's intent, through the contracting practices outlined in this Ordinance, to assure that those companies wanting to do business with the City will equalize the total compensation between similarly situated employees with spouses and with domestic partners. The provisions of this Ordinance are designed to ensure that the City's contractors will maintain a competitive advantage in recruiting and retaining capable employees, thereby improving the quality of the goods and services the City and its people receive, and ensuring protection of the City's property.

(c) Equal Benefits Requirements.

(1) No Awarding Authority of the City shall execute or amend any Contract with any Contractor that discriminates in the provision of Benefits between employees with spouses and employees with Domestic Partners, between spouses of employees and Domestic Partners of employees, and between dependents and family members of spouses and dependents and family members of Domestic Partners.

(2) A Contractor must permit access to, and upon request, must provide certified copies of all of its records pertaining to its Benefits policies and its employment policies and practices to the DAA, for the purpose of investigation or to ascertain compliance with the Equal Benefits Ordinance.

(3) A Contractor must post a copy of the following statement in conspicuous places at its place of business available to employees and applicants for employment: "During the performance of a Contract with the City of Los Angeles, the Contractor will provide equal benefits to its employees with spouses and its employees with domestic partners." The posted statement must also include a City contact telephone number which will be provided each Contractor when the Contract is executed.

(4) A Contractor must not set up or use its contracting entity for the purpose of evading the requirements imposed by the Equal Benefits Ordinance.

(d) Other Options for Compliance. Provided that the Contractor does not discriminate in the provision of Benefits, a Contractor may also comply with the Equal Benefits Ordinance in the following ways:

(1) A Contractor may provide an employee with the Cash Equivalent only if the DAA determines that either:

a. The Contractor has made a reasonable, yet unsuccessful effort to provide Equal Benefits; or

b. Under the circumstances, it would be unreasonable to require the Contractor to provide Benefits to the Domestic Partner (or spouse, if applicable).

(2) Allow each employee to designate a legally domiciled member of the employee's household as being eligible for spousal equivalent Benefits.

(3) Provide Benefits neither to employees' spouses nor to employees' Domestic Partners.

(e) Applicability.

(1) Unless otherwise exempt, a Contractor is subject to and shall comply with all applicable provisions of the Equal Benefits Ordinance.

(2) The requirements of the Equal Benefits Ordinance shall apply to a Contractor's operations as follows:

a. A Contractor's operations located within the City limits, regardless of whether there are employees at those locations performing work on the Contract.

b. A Contractor's operations on real property located outside of the City limits if the property is owned by the City or the City has a right to occupy the property, and if the Contractor's presence at or on that property is connected to a Contract with the City.

c. The Contractor's employees located elsewhere in the United States but outside of the City limits if those employees are performing work on the City Contract.

(3) The requirements of the Equal Benefits Ordinance do not apply to collective bargaining agreements ("CBA") in effect prior to January 1, 2000. The Contractor must agree to propose to its union that the requirements of the Equal Benefits Ordinance be incorporated into its CBA upon amendment, extension, or other modification of a CBA occurring after January 1, 2000.

(f) Mandatory Contract Provisions Pertaining to Equal Benefits. Unless otherwise exempted, every Contract shall contain language that obligates the Contractor to comply with the applicable provisions of the Equal Benefits Ordinance. The language shall include provisions for the following:

(1) During the performance of the Contract, the Contractor certifies and represents that the Contractor will comply with the Equal Benefits Ordinance.

(2) The failure of the Contractor to comply with the Equal Benefits Ordinance will be deemed to be a material breach of the Contract by the Awarding Authority.

(3) If the Contractor fails to comply with the Equal Benefits Ordinance the Awarding Authority may cancel, terminate or suspend the Contract, in whole or in part, and all monies due or to become due under the Contract may be retained by the City. The City may also pursue any and all other remedies at law or in equity for any breach.

(4) Failure to comply with the Equal Benefits Ordinance may be used as evidence against the Contractor in actions taken pursuant to the provisions of Los Angeles Administrative Code Section 10.40, et seq., Contractor Responsibility Ordinance.

(5) If the DAA determines that a Contractor has set up or used its Contracting entity for the purpose of evading the intent of the Equal Benefits Ordinance, the Awarding Authority may terminate the Contract on behalf of the City. Violation of this provision may be used as evidence against the Contractor in actions taken pursuant to the provisions of Los Angeles Administrative Code Section 10.40, et seq., Contractor Responsibility Ordinance.