

AGREEMENT NO.

AGREEMENT BETWEEN
THE CITY OF LOS ANGELES AND
INTERNATIONAL BUSINESS MACHINES CORPORATION

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 INTERNATIONAL BUSINESS MACHINES CORPORATION, a New York corporation ("IBM" or "Consultant").

WHEREAS, City requires creation, implementation and operation of a Cyber Resilience Center that will receive, analyze, enrich and distribute cyber threat information with participating stakeholders in the Port of Los Angeles ("POLA") ecosystem; and

WHEREAS, Executive Director requires the professional, expert and technical services of Consultant on a temporary or occasional basis to assist the City in creation, implementation and operation of a fully expandable Cyber Resilience Center; and

WHEREAS, Consultant possesses extensive experience in dealing with creation, implementation and operating of a Cyber Resilience Center; and

WHEREAS, Consultant, by virtue of training and experience, is 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 ("Statement of Work" or "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 thirty (30) 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 thereof.

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 B.

B. The maximum payable under this Agreement, including reimbursable expenses (see Exhibit B), shall be Six Million Eight Hundred Thousand Dollars (\$6,800,000).

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 C) 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.

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

The Consultant shall defend, indemnify, and hold the City, its officers, employees, and agents harmless from and against any and all liability, loss expense (including reasonable attorney's fees), or claims for injury or damages on account of bodily injuries (including death) or damage to real property or tangible personal property for which Consultant is legally liable to that third party, and pay all costs, damages and attorney's fees that a court finally awards or that are included in a settlement approved by Consultant, provided that the City shall promptly notify Consultant in writing of the claim, and allow Consultant to control, and will cooperate with the Consultant in the defense and any related settlement negotiations that are caused by or result from the negligent or intentional acts or omissions of the Consultant, its officers, agents, or employees.

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) combined single limit for injury or claim. 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.

(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 One Million Dollars (\$1,000,000) 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 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.

(3) Workers' Compensation and Employer's Liability

Consultant shall certify that it is aware of 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) Technology Errors and Omissions Liability Insurance

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 all products and services of the insured, or by its employees, agents, or contractors, and include 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 Technology Errors and Omissions Liability Insurance in the amount of Five Million Dollars (\$5,000,000) per claim/aggregate including Notification Costs, 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 acceptance of the completed project by Board.

Each policy shall include a 10-days notice of cancellation for nonpayment of premium and a 30-days notice of cancellation for any other reasons may be submitted.

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.

Upon request by City, Consultant shall furnish a copy of the binder of insurance and/or a full certified policy for any insurance policy required herein. This obligation is intended to, and shall, survive the expiration or earlier termination of this Agreement.

(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

At least thirty (30) days 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. If Consultant neglects or fails to secure or maintain the insurance required above, Executive Director may, at his or her own option but without any obligation, obtain such insurance to protect City's interests. The cost of such insurance shall be deducted from the next payment due Consultant.

(6) Limits of Coverage

If Consultant maintains higher limits than the minimums required by this Agreement, City requires and shall be entitled to coverage for the higher limits maintained by Consultant. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to City.

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 thirty (30) 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.

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 D.

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 E.

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.

NOTE: 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, Los Angeles Business Assistance Virtual Network (LABAVN), at <http://www.labavn.org>.

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

If a third party asserts a claim against the City that a product that Consultant provides to the City under this Agreement infringes that party's patent or copyright, Consultant will defend the City against that claim at Consultant's expense and pay all costs, damages, and attorney's fees that a court finally awards against the City or that are included in a settlement approved by Consultant, provided that the City:

- (1) promptly notifies Consultant in writing of the claim;
- (2) allows Consultant to control, and cooperates with Consultant in, the defense and any related settlement negotiations; and
- (3) is and remains in compliance with the product's applicable license terms.

Contractor has no responsibility for claims based on Non Contractor Products, items not provided by Contractor, or any violation of law or third party rights caused by Content, or any Organization materials, designs, specifications, or use of a non-current version or release of a Contractor Product when an infringement claim could have been avoided by using a current version or release.

19. PROPRIETARY INFORMATION

A. Writings, as that term is defined in Section 250 of the California Evidence Code (including, without limitation, drawings, specifications, estimates, reports, records, reference material, data, charts, documents, renderings, computations, computer tapes or disks, submittals and other items of any type whatsoever, whether in the form of writing, figures or delineations), which are obtained, generated, compiled or derived in connection with this Agreement (collectively hereafter referred to as "property"), are owned by City as soon as they are developed, whether in draft or final form. City has the right to use or permit the use of property and any ideas or methods represented by such property for any purpose and at any time without compensation other than that provided in this Agreement. Consultant hereby warrants and represents that City at all times owns rights provided for in this section free and clear of all third-party claims whether presently existing or arising in the future, whether or not presently known. Consultant need not obtain for City the right to use any idea, design, method, material, equipment or other matter which is the subject of a valid patent, unless such patent is owned by Consultant or one of its employees, or its Subconsultant or the Subconsultant's employees, in which case such right shall be obtained without additional compensation. Whether or not Consultant's initial proposal or proposals made during this Agreement are accepted by City, it is agreed that all information of any nature whatsoever connected with the Scope of Work, regardless of the form of communication, which has been or may be given by Consultant, its Subconsultants or on either's behalf, whether prior or subsequent to this Agreement becoming effective, to the City, its boards, officers, agents or employees, is not given in confidence. Accordingly, City or its designees may use or disclose such information without liability of any kind, except as may arise under valid patents.

B. If research or development is furnished in connection with this Agreement and if, in the course of such research or development, patentable work product is produced by Consultant, its officers, agents, employees, or Subconsultants, the City shall have, without cost or expense to it, an irrevocable, non-exclusive royalty-free license to make and use, itself or by anyone on its behalf, such work product in connection with any activity now or hereafter engaged in or permitted by City. Upon City's request, Consultant, at its sole cost and expense, shall promptly furnish or obtain from the appropriate person a form of license satisfactory to the City. It is expressly understood and agreed that, as between City and Consultant, the referenced license shall arise for City's benefit immediately upon the production of the work product, and is not dependent on the written

license specified above. City may transfer such license to its successors in the operation or ownership of any real or personal property now or hereafter owned or operated by City.

C. City will own all intellectual property rights both created in the course of the contract and embodied in project materials, subject to a world-wide, non-exclusive, royalty-free, irrevocable license hereby granted to Consultant under any such intellectual property rights. For purposes of clarity, City's ownership of such intellectual property rights shall not include any copyrights, patents, moral rights, trademarks, trade dress, trade secrets, or any other intellectual property rights created outside of the contract, including but not limited to any such rights that preexist the contract.

20. CONSULTANT'S LIMITATION OF LIABILITY

A. Consultant's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by City up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the product or service that is the subject of the claim, regardless of the basis of the claim. Consultant will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings. These limitations apply collectively to Consultant, its affiliates, contractors, and suppliers.

B. The following amounts are not subject to the above cap: i) third party payments referred to in sections 9 and 18 above; and ii) damages that cannot be limited under applicable law.

21. EXCUSABLE DELAYS

Neither party shall be liable for its delay or failure to perform any obligation under and in accordance with this Contract, if the delay or failure arises out of fires, floods, earthquakes, epidemics, quarantine restrictions, other natural occurrences, strikes, lockouts (other than a lockout by the party or any of the party's Subcontractors), freight embargoes, terrorist acts, insurrections or other civil disturbances, or other similar events to those described above, but in each case the delay or failure to perform must be beyond the control and without any fault or negligence of the party delayed or failing to perform (these events are referred to in this provision as "Force Majeure Events"). In the event Contractor's delay or failure to perform arises out of a Force Majeure Event, Contractor agrees to use commercially reasonable best efforts to obtain the goods or services from other sources, and to otherwise mitigate the damages and reduce the delay caused by the Force Majeure Event.

22. 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 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.

23. 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, 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.

24. 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.

25. 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.

26. 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.

27. 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 F.

28. 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.

29. 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.

30. 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.**

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. EXHIBITS; ARTICLES

All exhibits 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.

37. 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

Dated: _____, 20__

By: _____
EUGENE D. SEROKA
Executive Director

Attest: _____
AMBER M. KLESGES
Board Secretary

INTERNATIONAL BUSINESS MACHINES CORPORATION

Dated: November 15, 2020

By: Christopher S Burns
Christopher S Burns Senior Security Services Sales Specialist
(Print/type name and title)

Attest: Robert Israel
Robert Israel Business Unit Executive, Security Services
(Print/type name and title)

APPROVED AS TO FORM AND LEGALITY

11/24, 2020
MICHAEL N. FEUER, City Attorney
JANNA B. SIDLEY, General Counsel

By: Brian A. Daluiso
BRIAN A. DALUISO, Deputy

BAD/ila (11/12/2020)
Attachments

Account #	_____	W.O. #	_____
Ctr/Div #	_____	Job Fac. #	_____
Proj/Prog #	_____		
Budget FY:		Amount:	
20/21		TBD	
21/22		TBD	
22/23		TBD	
TOTAL		\$6,800,000	

For Acct/Budget Div. Use Only:

Verified by: _____

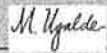

Verified Funds Available: _____

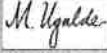

Date Approved: _____



Budget Information

Date: November 6, 2020

Contractor/Vendor Name: INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM)

Account #	54310	W.O. #	2555500
Ctr/Div #		Job Fac. #	1179
Proj/Prog #	640		
Budget FY:		Amount:	
20/21		\$912,941	
21/22		\$327,986	
22/23		\$454,735	
23/24		\$444,735	
TOTAL		\$2,140,397	
For Acct Div. Use Only:			
Verified by:	 <small>Digitally signed by Melody Ugaldes Date: 2020.11.09 13:13:00 -08'00'</small>		
Verified Funds Available:	 <small>Digitally signed by Frank Liu Date: 2020.11.09 14:38:59 -08'00'</small>		
Date Approved:	11/9/20		

Account #	55130	W.O. #	2555500
Ctr/Div #		Job Fac. #	1179
Proj/Prog #	640		
Budget FY:		Amount:	
20/21		\$0	
21/22		\$1,267,675	
22/23		\$0	
23/24		\$0	
TOTAL		\$1,267,675	
For Acct Div. Use Only:			
Verified by:	 <small>Digitally signed by Melody Ugaldes Date: 2020.11.09 13:13:14 -08'00'</small>		
Verified Funds Available:	 <small>Digitally signed by Frank Liu Date: 2020.11.09 14:37:22 -08'00'</small>		
Date Approved:	11/9/20		

Account #	55160	W.O. #	2555500
Ctr/Div #		Job Fac. #	1179
Proj/Prog #	640		
Budget FY:		Amount:	
20/21		\$0	
21/22		\$790,000	
22/23		\$0	
23/24		\$0	
TOTAL		\$790,000	
For Acct Div. Use Only:			
Verified by:	 <small>Digitally signed by Melody Ugaldes Date: 2020.11.09 13:13:27 -08'00'</small>		
Verified Funds Available:	 <small>Digitally signed by Frank Liu Date: 2020.11.09 14:36:33 -08'00'</small>		
Date Approved:	11/9/20		

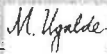

Account #	54310	W.O. #	
Ctr/Div #	0640	Job Fac. #	
Proj/Prog #	000		
Budget FY:		Amount:	
20/21		\$0	
21/22		\$600,445	
22/23		\$1,200,890	
23/24		\$800,593	
TOTAL		\$2,601,928	
For Acct Div. Use Only:			
Verified by:	 <small>Digitally signed by Melody Ugaldes Date: 2020.11.09 13:13:44 -08'00'</small>		
Verified Funds Available:	 <small>Digitally signed by Frank Liu Date: 2020.11.09 14:36:45 -08'00'</small>		
Date Approved:	11/9/20		

EXHIBIT A

Information Technology

Port of Los Angeles Cyber Resilience Center

STATEMENT OF WORK



October 20, 2020

PROJECT DESCRIPTION

1 Project Goals and Objectives

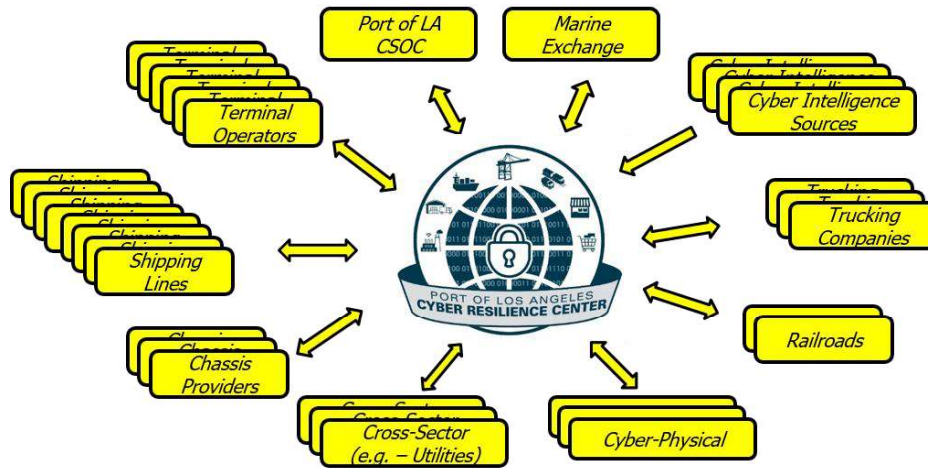
ITD is seeking a turn-key Port of Los Angeles Cyber Resilience Center (CRC) solution, including design, installation, operation, maintenance and support services. The CRC will be a first-of-its-kind solution that will help to reduce the port-wide risk of a cyber incident that could disrupt the flow of cargo at the Port of Los Angeles.

The CRC will enable key stakeholders from the Port of Los Angeles ecosystem to share cyber threat indicators and defensive measures with each other as a means to reduce the impacts of a cyber incident experienced by one of the Port's stakeholders to disrupt multiple operations within the Port of Los Angeles. In addition to defensive measures, the CRC will serve as an information resource stakeholders may use to help restore operations following an attack. The CRC will receive, analyze and share information to and from direct stakeholders (e.g. – cargo handlers, tenants) and cross-sector stakeholders (e.g. – providers of essential services to direct stakeholders) who choose to become members of the CRC.

CRC objectives include:

- Provide both automated and manual information sharing among participating stakeholders.
- Improve the quality, quantity and speed of available analysis of ecosystem cyber risks.
- Create new collaboration with stakeholders to increase cyber resilience.
- Provide a new source of information to stakeholders which could allow them to improve their cyber security posture.

The CRC will also serve as the critical first step to implement the technical foundation upon which other Port of Los Angeles technological innovations can be better protected. The CRC will be different than the scope and function of the Port's existing Cyber Security Operations Center (CSOC). The CRC will be a "system of systems" that connects to the CSOC and stakeholder cyber security systems (see diagram below), but will not duplicate or replace them, nor will the CRC be intrusive, disruptive or burdensome to stakeholder systems. Stakeholders will have the control to decide if, and how, to use information from the CRC.



A solution such as this does not exist today. Therefore, the Port of Los Angeles invites an innovative and effective CRC solution to achieve the Port's objectives.

2 Project Scope of Work

The Port of Los Angeles seeks a contractor to furnish resources, processes and technologies for a turn-key CRC solution. All aspects of the CRC work shall employ a collaborative approach with participating stakeholders. The requirements below provide the framework and minimum requirements of the system.

The CRC project scope of work shall include the following elements: 1) governance, 2) design, 3) data sharing agreements, 4) installation, 5) stakeholder onboarding, 6) operations, 7) warranty, maintenance and support, 8) project closeout.

1) GOVERNANCE

1.1 The contractor shall establish a collaborative governance structure that includes an Executive Steering Committee and a Technical Committee (collectively "Governance Committees"). Both Governance Committees shall consist of select stakeholder representatives.

1.2 The contractor shall establish protocols for both Governance Committees, including roles, responsibilities, policies, procedures, communications, etc., for collaborative and effective governance.

1.3 The contractor shall assist with the facilitation of both Governance Committees for the duration of the agreement.

2) DESIGN

2.1 General Design

2.1.1 The contractor shall design the CRC solution in collaboration with participating stakeholders.

- 2.1.2 The CRC shall be a closed information solution. Data will be received from participating stakeholders and from external cyber intelligence sources. However, data will be distributed only to participating stakeholders. Data will not be distributed outside of the CRC.
- 2.1.3 The CRC platform shall enable Port of Los Angeles stakeholders to automatically and manually exchange cyber threat intelligence to increase the collective knowledge base of known threat actors, activity, and malware.
- 2.1.4 The CRC shall be compliant with relevant state, federal and international laws and regulations.
- 2.1.5 The CRC platform shall be based on, and compliant with the National Institute of Standards and Technology (“NIST”) Special Publication 800-150, Guide to Cyber Threat Information Sharing.
- 2.1.6 The CRC platform shall be capable of data sharing via an API, sensor and/or STIX/TAXII protocol.
- 2.1.7 The CRC will be a system of systems, and shall not replace any cyber security operations of participating stakeholders.
- 2.1.8 The CRC shall not be invasive or disruptive to existing systems of participating stakeholders.
- 2.1.9 The CRC shall not include stakeholder proprietary information.
- 2.1.10 The CRC shall not identify or expose stakeholder cyber vulnerabilities.
- 2.1.11 The CRC shall not be burdensome to stakeholder staff.
- 2.1.12 The CRC shall have a minimum availability of 99.9%, with fail-over and redundancy of critical components.
- 2.1.13 The CRC shall have a hot standby disaster recovery solution.
- 2.1.14 The CRC platform shall have tools and capabilities for authorization, authentication, and accounting.
- 2.1.15 Data at rest and in motion shall be encrypted with latest cryptographic standards.
- 2.1.16 The CRC solution shall be flexible and scalable to be able to meet future needs.
- 2.1.17 The CRC website(s) shall be hosted under designated domain(s) of the Port of Los Angeles.
- 2.1.18 Contractor may be required to travel to stakeholder and other locations. Travel expenses to be reimbursed shall be in accordance with City of Los Angeles travel policy, found in Section 1.8 of the City Controller’s Manual

<http://inside.controlpanel.la/sites/default/files/inline-files/Controller%20Manual%20%283%29.pdf>).

2.1.19 On-premise, cloud, managed security services provider, or hybrid solutions will be considered.

2.2 Data Collection And Integration

2.2.1 Data elements required to meet the CRC objectives shall be identified in collaboration with stakeholders.

2.2.2 The CRC shall receive, normalize, aggregate and integrate data received from different stakeholder sources and from external cyber intelligence sources. Data source platforms and formats are expected to be different.

2.2.3 The CRC shall be able to effectively ingest data from multiple sources without failure due to overload or saturation.

2.2.4 The CRC must be capable of storage of data allowing for a minimum of 90 days retrieval. Data retention time shall be configurable.

2.2.5 Data From Stakeholders:

- Data elements that stakeholders agree to share shall be automatically transmitted from stakeholder systems to the CRC.
- A secure data collection portal shall be created and available for stakeholders to manually share additional data with the CRC.
- Data shall be transmitted from the source system to the CRC in real-time such that source data are available in the CRC at the same time as in the source system.

2.2.6 Data From External Threat Intelligence Sources:

- In addition to stakeholder data, the CRC shall be able to receive data from multiple external cyber intelligence sources.
- Contractor shall provide proposed intelligence consumption processes for the intake of external intelligence data for analysis, classification and integration into CRC operations.
- Contractor's proposal shall include up to ten recommended external threat intelligence sources that are appropriate for their solution. This can include pre-subscribed services, paid and free subscriptions, technology vendor intelligence, native capability and other sources.

2.3 Analysis

2.3.1 The CRC shall perform data analytics, data correlation, categorization and enrichment of threat indicators utilizing the latest security technologies.

- 2.3.2 The CRC should process data such that it may be used by participating stakeholders to help them classify, identify, and disseminate indicators of compromise and other selectors for blacklisting within firewalls, servers, appliances and tools.
- 2.3.3 The CRC shall include only data that is related to the maritime transportation industry, including secondary transportation sectors such as trucking and rail serving the Port of Los Angeles.
- 2.3.4 The CRC shall incorporate machine learning and artificial intelligence capabilities.

2.4 Data To Stakeholders

- 2.4.1 The CRC data shall be distributed only to the participating stakeholders.
- 2.4.2 The CRC data shall provide actionable maritime cyber security information to stakeholders that may be used as an early detection and warning of cyber threats that may help to improve cyber defenses.
- 2.4.3 The CRC shall also be an information resource to assist with cyber information for incident recovery assistance, as may be appropriate to participating stakeholders.
- 2.4.4 Data shared with stakeholders shall not be automatically ingested by stakeholder systems. Each stakeholder will have the control to decide whether to use the CRC provided data, or not, as appropriate to their operations.
- 2.4.5 Data shared with stakeholders shall be anonymized so as not to disclose the stakeholder that originally provided the information.
- 2.4.6 The CRC shall not simply pass through irrelevant or redundant data that creates “noise” and burden for stakeholders.

2.5 Visualization

2.5.1 At the CRC Facility

- The CRC shall provide visibility into the cyber posture of the Port’s ecosystem.
- The CRC shall include real-time graphical static & dynamic displays and dashboards that present threat data for situational awareness, including global trends and maritime business sector displays.
- The contractor shall preconfigure a minimum of three dashboards for likely incident scenarios.
- A Cyber Alert Indicator (similar to MS-ISAC Cyber Alert Level Indicator) for the Port of Los Angeles ecosystem shall be developed and displayed

on the dashboard. The Cyber Alert Indicator shall show the current level of cyber risk in the POLA ecosystem based on Traffic Light Protocol.

- Contractor's proposal shall include proposed examples of dashboard views.

2.5.2 For Stakeholders

- The CRC shall enable participating stakeholders to observe threat data in various dashboard models through a secure portal. Visualization for stakeholders shall include their own data and anonymized data that other stakeholders agree to share.
- The CRC shall incorporate role-based access controls, and security into the design of the platform. The CRC shall have the capability to provide separate views for stakeholders and system administrators depending upon the data and their roles.
- The CRC data shall be able to be displayed with existing stakeholder dashboards, desktops/laptops, tablets and/or smartphones.
- The CRC data shall be accessible to participating stakeholders at any time and from anywhere securely with an internet connection.
- The CRC shall communicate (e.g. alerts, notifications, updates, etc.) to participating stakeholders in real-time.
- Contractor's proposal shall include proposed examples of stakeholder views.

2.6 CRC Facility

2.6.1 Primary Facility Location

- Contractor shall build a physical CRC facility that will be the location from which CRC operations will be conducted. This facility will be used as the on-site CRC work location for an on-premise, cloud, managed security services provider, or hybrid solution.
- The CRC facility will be located in a Harbor Department building located at 300 Water Street, Wilmington, CA 90744. The dimensions of the room are 15 ft 8 in x 10 ft 4 in, with 9 feet high ceilings (See Attachment 4). The video monitors should be along the 10 ft 4 inch wall. Contractor can assume that sufficient power, lighting and HVAC exists in the room.
- Equipment racks, if any, may be installed in an adjacent, separate room.
- The CRC shall be completely independent from the Harbor Department's Information Technology infrastructure.

- The CRC facility shall include all necessary components including, but not limited to, the following:
 - Furniture, hardware, software, supplies;
 - Four console work stations/consoles for CRC operations staff/analysts;
 - Two independent Internet Service Provider (ISP) connections from different providers, minimum 1 gbps per ISP, during the Operations phase (contractor may use POLA guest internet connection during development phase);
 - Voice telephone lines, with redundancy, which function like a dispatch call center where incoming calls are sent to the same number;
 - Video wall, with minimum 6 monitors and a video wall controller;
 - Multimedia video and audio system;
 - Video teleconference system;
 - Smartboard and whiteboard;
 - Back-up power for critical components; and
 - Other facility components to meet the CRC objectives.
- Secure badge access control to enter the CRC facility will be provided by the Harbor Department.
- Contractor's proposal shall include a sketch of the proposed CRC facility layout.
- Contractor's proposal shall include all proposed network diagrams (low level and high level), and technical related documentation.

2.6.2 Alternate Facility Location

- The CRC shall be designed such that if the CRC Primary Location is not available, then an Alternate Location with an internet connection can be used to stand up the CRC and resume operations.
- Note: The Alternate Facility Location requirement is for the design only. The contractor will not build the Alternate Facility Location.

2.7 CRC Operations Manual

- 2.7.1 The contractor shall prepare an organized and succinct Operations Manual that describes how the CRC will operate. The Operations Manual shall be based on a Cyber Resilience Framework to achieve the CRC objectives.

This shall include, but is not limited to, the CRC sharing cyber threat indicators and defensive measures, and the CRC serving as an operations center where stakeholders can get information during an incident in the ecosystem.

- 2.7.2 The Operations Manual shall include, but is not limited to, CRC policies, procedures, roles, responsibilities, staffing levels, work shifts and contact information.
- 2.7.3 The Operations Manual shall include, but is not limited to, visuals of processes, data collection, integration and distribution flows.
- 2.7.4 The Operations Manual shall include, but is not limited to, visualization, descriptions, and uses of CRC facility dashboards.
- 2.7.5 The Operations Manual shall define and identify typical use cases and threat scenarios that may be submitted to the CRC, including how they should be handled.
- 2.7.6 The Operations Manual shall define minimum technical requirements for stakeholders to connect to the CRC.
- 2.7.7 The Operations Manual shall define how outages due to scheduled maintenance and other CRC disruptions will be handled, including protocols to notify stakeholders and back-up procedures.

3) DATA SHARING AGREEMENTS

- 3.1 Based on the CRC Design, the Contractor shall develop and write a uniform/standardized data sharing agreement to be entered into by each CRC participating stakeholder.
- 3.2 The data sharing agreement shall be based on the National Institute of Standards and Technology (NIST) information sharing guidelines (NIST SP 800-150) or similar.
- 3.3 Data sharing agreements shall be reviewed and approved by the Harbor Department Executive Director.
- 3.4 The Contractor shall be responsible for obtaining each participating stakeholder's approval to enter into the data sharing agreement.

4) CRC INSTALLATION

- 4.1 Upon receiving a Notice-to-Proceed with the CRC installation from the Executive Director of the Harbor Department, the contractor shall procure and install the CRC per the Design within the location selected by the Harbor Department. Contractor shall not incur expenses for the installation (e.g. hardware, software, construction, etc.) until after a Notice-to-Proceed has been issued.
- 4.2 Contractor shall be responsible for required permits, if any.

4.3 In addition to the installation of the CRC, the contractor shall also perform the following:

- Run all necessary cables between components and properly label all ports and wall plates with cable and connector information;
- Integrate all new equipment with existing equipment and infrastructure, as applicable; and
- Verify that all equipment is operational.

5) STAKEHOLDER ON-BOARDING

5.1 Contractor shall on-board stakeholders in coordination with stakeholder availability and in accordance with the CRC Design (Section 2) and Data Sharing Agreements (Section 3).

5.2 Contractor shall be responsible for all technical aspects of connecting the stakeholder systems to the CRC platform.

5.3 Contractor shall provide training to stakeholders, including but not limited to, use of the CRC platform, use of dashboards, use of data and available reports. Training shall also include communications and interactions between stakeholders and CRC Operations.

5.4 Contractor shall develop on-boarding documentation and provide documentation to stakeholders. This documentation shall be detailed and organized such that it can later be used as a stakeholder operations manual or reference guide.

5.5 Contractor may be required to travel to stakeholder and other locations. Travel expenses to be reimbursed shall be in accordance with City of Los Angeles travel policy.

6) OPERATIONS

6.1 The CRC shall be operated 24 hours per day, 7 days per week (24x7).

6.2 The contractor shall conduct operations in accordance with the CRC Operations Manual. The CRC Operations Manual shall be periodically reviewed and updated with new information and when changes are made.

6.3 The CRC shall achieve International Organization for Standardization/International Electrotechnical Commission 27001 (ISO 27001) certification within 6 months of going live and continue to maintain the certification for the duration of the contract.

6.4 Contractor shall provide feedback and recommendations for continuous improvement of the CRC.

6.5 Contractor staff that operate the CRC:

- 6.5.1 The lead person operating the CRC must possess and maintain a Certified Information Systems Security Professional (CISSP) certification. Alternate

certifications/experience in lieu of the CISSP may be considered. Additional industry certifications (e.g. GCIH, GCIA, GMON, GICSP, GRID, etc.) that are relevant to the role are recommended.

6.5.2 All staff must have excellent communication and customer service skills.

6.5.3 All staff must meet security requirements, including criminal and drug background checks.

6.5.4 All staff shall be subject to review and approval by the Harbor Department, at the proposal stage and during the term of the agreement if staffing changes are proposed by the contractor.

6.6 Operations Tools

6.6.1 An automated service management tool shall be used to manage and track inquiries and work orders.

6.6.2 Automated technical tool(s) shall be used to monitor and manage the CRC and connections to stakeholders to confirm proper operations. The tool(s) shall monitor the entire CRC environment and up to the demarcation point with the participating stakeholders.

6.7 On-Going Training

6.7.1 Contractor shall provide annual refresher CRC training for all participating stakeholder staff that interface with the CRC. This annual training shall also include tabletop exercises.

6.7.2 Contractor shall provide annual general cyber security awareness training that participating stakeholders may use for their end users, as appropriate for their company's cyber program.

6.8 Reports

6.8.1 CRC shall generate and distribute periodic reports for situational awareness and preventive operations.

6.8.2 CRC shall create and provide sanitized post-incident reports with lessons learned.

6.8.3 CRC shall provide ad-hoc reports as needed.

7) WARRANTY, MAINTENANCE AND SUPPORT

7.1 Warranty, maintenance and support shall be provided for everything provided under the agreement, for the duration of the agreement. This shall include, but is not limited to, hardware, software, services, licenses, updates, and 3rd party items.

8) CLOSEOUT

8.1 Ownership of the complete functioning CRC, including all intellectual property, software source code and documentation developed under this contract, shall be assigned by contractor to the Harbor Department at the conclusion of the contract.

For intellectual property, software source code and documentation that are not developed under this contract, the contractor shall transfer the rights to continue to use them to the Harbor Department at the conclusion of the contract; this may include, but not be limited to, transfer of subscriptions, licenses and third-party agreements.

8.2 The Harbor Department shall have full ownership rights to continue to operate and develop the CRC with its own staff or with another contractor.

8.3 All data shall be given to the Harbor Department. No copies of the data shall be retained by the contractor.

8.4 All CRC access/login credentials shall be given to the Harbor Department.

8.5 Contractor shall transition the CRC operations to the Harbor Department or designee so there is no disruption in services. This shall include knowledge transfer to the Harbor Department staff or a new contractor.

8.6 The contractor shall provide a final report that includes technical details at the time of closeout, including detailed configuration documents, security protocols, details of the developed API/STIX/TAXII protocols, process flow documents, data maps, details of analytical tools and displays, and general user documents.

9) SCHEDULE

The Harbor Department's desired schedule is presented below. However, proposers may include in their proposal an alternate schedule to achieve the CRC requirements.

1. Governance, Design and Data Sharing Agreements: Within 4 months of contract award:
 - Executive Steering and Technical Committees shall be established and in operation.
 - Design of the CRC completed.
 - Data sharing agreements should be signed with the first group of participating stakeholders (up to 20). The initial group of stakeholders will be determined during project planning.
2. Installation And On-Boarding Of First Group Of Stakeholders (up to 20): Within 6 months after the Harbor Department issues the Notice-to-Proceed (NTP) for the CRC installation:
 - CRC should be installed.
 - First group of participating stakeholders should be on-boarded.

3. On-Boarding 10 Additional Stakeholders (Total Of 30): Within 6 months after completion of Installation:
 - Data sharing agreements should be entered into with ten more stakeholders, for a total of thirty stakeholders on-boarded.
4. On-Boarding 10 Additional Stakeholders (Total Of 40): Within 12 months after completion of Installation:
 - Data sharing agreements should be established with ten more stakeholders, for a total of forty stakeholders on-boarded.
5. On-Boarding 10 Additional Stakeholders (Total Of 50): Within 18 months after completion of Installation:
 - Data sharing agreements should be established with ten more stakeholders, for a total of fifty stakeholders.
6. On-Boarding 10 Additional Stakeholders (Total Of 60): Within 24 months after completion of Installation:
 - Data sharing agreements should be established with ten more stakeholders, for a total of sixty stakeholders.
7. On-Boarding Additional Stakeholders (Total Of Up To 100, if the original 3-year contract is extended for two additional years for a total duration of five years): Within 48 months after completion of installation:
 - Data sharing agreements should be established with additional stakeholders, for a total of up to one hundred stakeholders (if agreement is 5 years).
8. ISO 27001 Certification: Within 6 months after CRC is in operation:
 - CRC should achieve ISO 27001 certification. This certification shall be maintained for the duration of the agreement.
9. On-Going Operations, Maintenance, and Enhancements:
 - Shall be provided from the completion of the CRC installation until the end of the agreement.

Port of Los Angeles

CYBER RESILIENCE CENTER

By:

ALANA MUNTZ

IBM Client Executive

alana.muntz@ibm.com

310-882-0695





[This Page Intentionally Left Blank]



Table of Contents

Executive Summary..... 5

Port of Los Angeles Goals for Cyber Resilience Center 5

Proposed Solution for the Port of Los Angeles..... 6

 IBM Cloud Pak for Security (CP4S)..... 6

 Methodology..... 8

 Applications 9

 Dashboards 11

 Professional Security Services 11

 Cyber Intelligence Services 12

Firm Qualifications, Experience and References..... 14

 Reference: Los Angeles Cyber Lab..... 14

 References for Alliance Partner, Trustar: IT-ISAC and RH-ISAC..... 15

 Reference: University of Southern California Keck Medical 15

Project Organization, Personnel and Staffing..... 17

Project Personnel and Staffing..... 17

 Security Analyst 17

 Incident Commander Resume 18

 Project Manager – IT Security Services PMO 19

 Product Partner: Trustar 20

Project Organization..... 21

 Implementation plan by phase..... 21

 Transition 21

Project Approach and Work Plan (Scope of Work)..... 23

Governance..... 23

 Guiding Principles 23

 CRC Governance Scope & Operating Model 23

 CRC Governance Communications 24

 CRC Governance Meetings 24

 Strategy and Oversight 25

 Operational Governance 26

 Stakeholder Cyber Intelligence Governance 27

 Cyber Intelligence 28

 CP4S / TruStar Engineering 29

 Operations Scrum 29

Cloud Pak for Security System Design 30

 IBM Responsibilities for System Design 30

IBM IRIS Cyber Intelligence Services 33

 Methodology..... 34

 Enterprise Intelligence Management 34

 Analysis-(Analysts)..... 35



Cyber Resilience Center Facility..... 37
 Scope 38
 Disaster Recovery 40
 CRC Installation 41

Data sharing agreements..... 41
 CRC Stakeholder Onboarding 42
 Operations 42
 Data Sharing with Stakeholders 43
 Warranty 43
 Closeout 43

RFP Requirements Matrix..... 44

Project Management..... 52

Schedule..... 53

Sample Reports 54

Cost 55
 Port of LA Cyber Resilience Center RFP Pricing Table Error! Bookmark not defined.

Business Enterprise Programs and Contract Administrative Requirements.... 56

Executive Summary



The Information Technology Division (ITD) is seeking a turn-key Port of Los Angeles (PoLA) Cyber Resilience Center (CRC) solution, including design, installation, operation, maintenance and support services. The CRC will be a first-of-its-kind solution that will help to reduce the port-wide risk of a cyber incident that could disrupt the flow of cargo at the Port of Los Angeles. IBM recognizes that ITD and the Port of Los Angeles faces an unprecedented set of pressures and our services and solutions will identify these threats with prompt and effective analysis, notification and escalation.

IBM understands that the CRC will serve as the critical first step to implement the technical foundation upon which other Port of Los Angeles technological innovations can be better protected. The CRC will be different than the scope and function of the Port's existing Cyber Security Operations Center (CSOC). The CRC will be a "system of systems" that connects to the CSOC and stakeholder cyber security systems (see diagram below), but will not duplicate or replace them, nor will the CRC be intrusive, disruptive or burdensome to stakeholder systems. Stakeholders will have the control to decide if, and how, to use information from the CRC.

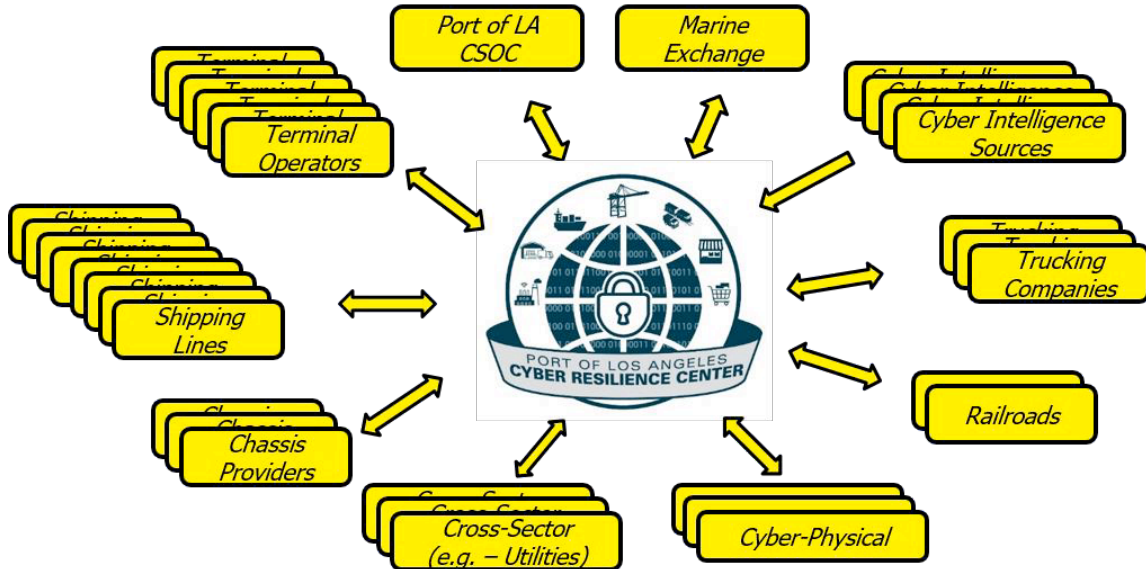
Port of Los Angeles Goals for Cyber Resilience Center

IBM will deliver a turn-key solution that will enable the CRC, and its key stakeholders from the Port of Los Angeles ecosystem, to share cyber threat indicators and defensive measures with each other as a means to reduce the impacts of a cyber incident experienced by one of the Port's stakeholders to disrupt multiple operations within the Port of Los Angeles. In addition to defensive measures, the CRC will serve as an information resource that stakeholders may use to help restore operations following an attack. The CRC will receive, analyze and share information to and from direct stakeholders (e.g. – cargo handlers, tenants) and cross-sector stakeholders (e.g. – providers of essential services to direct stakeholders) who choose to become members of the CRC.

CRC objectives include:

- Provide both automated and manual information sharing among participating stakeholders.

- Improve the quality, quantity and speed of available analysis of ecosystem cyber risks.
- Create new collaboration with stakeholders to increase cyber resilience.
- Provide a new source of information to stakeholders which could allow them to improve their cyber security posture.



Proposed Solution for the Port of Los Angeles

IBM Cloud Pak for Security (CP4S)

IBM’s Cloud Pak for Security is compliant with ISO 27001 and the National Institute of Standards and Technology (“NIST”) Special Publication 800-150, Guide to Cyber Threat Information Sharing. The CP4S platform is specifically designed to quickly integrate your existing security tools and intelligence sources while generating deeper insights into threats across hybrid, multi-cloud environments. Based on an infrastructure-independent common operating environment, Cloud Pak for Security can be installed and run wherever you need it. It can connect disparate data sources to uncover hidden threats and help make better, risk-based decisions, while leaving the data where it resides. REQ 1

By using open standards and IBM innovations such as STIX Shifter, Cloud Pak for Security can securely access both IBM and third-party tools to search for threat indicators across your environment whether cloud or on premises. The resulting insights are presented in a unified interface that enables the Port of Los Angeles to design orchestrated workflows which yield faster, more decisive incident resolution.


Cloud Pak for Security is comprised of containerized software pre-integrated with Red Hat OpenShift, the industry’s most comprehensive enterprise Kubernetes platform. This integration improves Cloud Pak for Security return on investment (ROI) by enabling on premises, public cloud, and private cloud deployment.





Component containerization benefits include increased reliability, scalability, uptime, and decreased infrastructure management effort.

<p><i>Run anywhere</i></p> <h2 style="text-align: center;">Connect openly</h2> <ul style="list-style-type: none"> - Run on premises, private cloud, or public cloud - Increase and shift investment as needed - Reduce vendor lock-in - Promote interoperability 	<p><i>Gain security insights</i></p> <h2 style="text-align: center;">Connect data</h2> <ul style="list-style-type: none"> - Uncover your hidden threats - Make better risk-based decisions - Leave your data where it is - Get more out of your investments 	<p><i>Take action faster</i></p> <h2 style="text-align: center;">Connect workflows</h2> <ul style="list-style-type: none"> - Respond faster as a team and business - Orchestrate across security use cases - Reduce your integration costs - Extend your team's capabilities
--	---	--

With IBM Cloud Pak for Security, be better connected to be better prepared

	<p>Create various cybersecurity dashboards for analysts, managers, and CISOs</p>	<p>Create various security dashboards based on a common framework and custom dashboards from a library of Threat Intelligence Insight widgets.</p> <p>Gain more insight as analysts can drill into their own dashboard views including details on specific threats and risks. REQ 2</p>
 <p>IBM Security Data Explorer</p>	<p>Streamline investigations with federated search</p>	<p>Provides federated search across multiple tools and environments, massively simplifying investigations.</p> <p>Supports a single, unified interface and workflow to investigate threats and indicators of compromise into user selected data sources.</p> <p>Track, append, and create security cases from a native, platform case management system.</p>



 <p>IBM Security Threat Intelligence Insights</p>	<p>Investigate threats and indicators of compromise (IOCs) across multiple sources</p>	<p>Delivers unique, actionable, and timely threat intelligence.</p> <p>Provides identification and prioritization based on organizational profile and environmental telemetry.</p> <p>Reduces noise in security operations while prioritizing incidents and threat reports.</p>
 <p>Security Orchestration, Automation and Response (SOAR)</p>	<p>Respond faster to security incidents with automation</p>	<p>Respond faster to security incidents from a unified interface that connects your existing security and IT tools.</p> <p>Automation—150 integrations available for immediate use providing threat enrichment and remediation.</p> <p>Leverage orchestration and automation to accelerate your incident response and improve your overall security operations.</p> <p>If needed, tap into IBM Security Services for a range of capabilities from on-demand consulting services to custom development.</p>

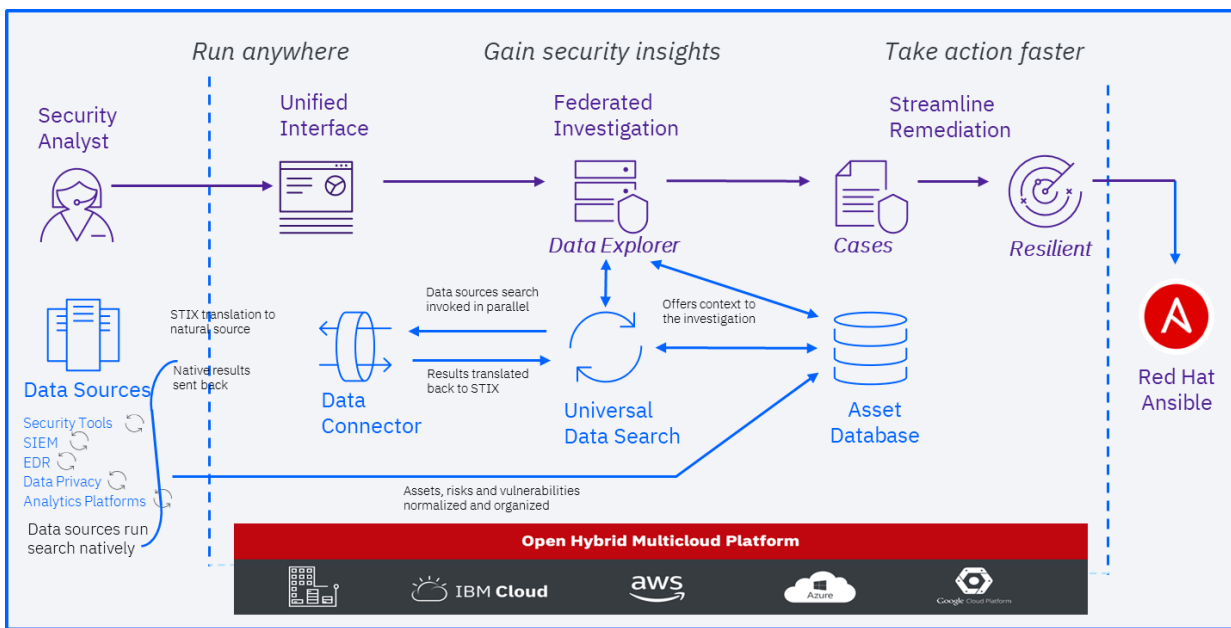
Methodology

Cloud Pak for Security connects security-related data sources, from different tools such as your Security Information and Event Management (CP4S/TRUSTAR), Endpoint Detection and Response (EDR), data lakes, and more. It fuses data from a variety of sources and provides access across all of them. Consolidated insight is then delivered back to the connected security applications to yield further enrichment. Orchestrated workflows for incident response automate manual and repetitive tasks. CRC will be able to productively collaborate and respond faster by working together based on all available data.

IBM Cloud Pak for Security provides a state-of-the-art foundation for an integrated ITD and CRC, moving from uncoordinated processes using disparate point products to a coordinated and integrated response. With a focus on fostering interoperability, it enhances the value of your existing tools as an integration platform. Rather than demanding a central data store that requires data ingestion, Cloud Pak for Security **federates data** to provide unified visibility into security insights and events across integrated tools in your environment. This allows Port of Los Angeles to preserve existing investments and empowers your security teams to deal with the complexity of the heterogeneous IT landscape as well as the range of heterogenous IT security tools deployed.

Through the OASIS Open Cybersecurity Alliance, IBM has forged partnerships with dozens of companies to promote interoperability and help reduce vendor lock-in across the security community through co-developed open source technologies. Cloud Pak for Security **builds on open standards** and can run on various platforms, including on premises environments, private clouds, and public Infrastructure as a Service (IaaS) infrastructures such as IBM Cloud, Amazon Web Services (AWS), and Microsoft® Azure.

It connects to solutions from the most relevant vendors in cybersecurity, such as Splunk, Tenable, Carbon Black, Elastic, BigFix, AWS, and Microsoft Azure via a unified, modern interface. Security data is accessed through an integration layer and open source technology so relevant findings can be further analyzed from one place.



Supports a seamless workflow across your security team and tools

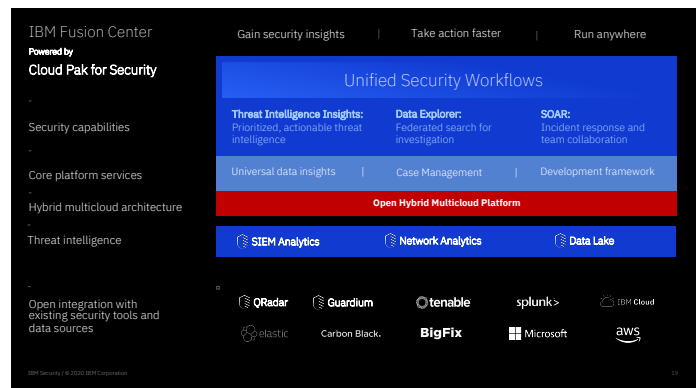
Applications

IBM Cloud Pak for Security applications:

IBM Security Data Explorer: Data Explorer enables federated search and investigation across your hybrid, multi-cloud environment in a single interface and workflow. Data Explorer enables users to perform investigations and threat hunts in a timely manner without requiring duplication of data.

IBM Security Threat Intelligence

Insights: Threat Intelligence Insights delivers unique, actionable, and timely threat intelligence. Identification and prioritization are based on PoLA's organizational profile and environmental telemetry. Once you detect a threat, you can seamlessly





investigate the threat details and indicators of compromise (IOCs) across multiple sources, and remediate cyberthreats all from a single console dashboard by leveraging the applications on IBM Cloud Pak for Security. Threat Intelligence Insights maximizes security analyst workflow by:

- Reducing noise in security operations
- Prioritizing incidents and threat reports
- Effectively correlating global threat intelligence with the contextualized local environment

We use human intelligence to add context to machine-generated data. The IBM X-Force® Incident Response and Intelligence Services (IRIS) Premium Threat Intelligence Reports provide the latest threat intelligence indicators of compromise to block threat campaigns, malware, threat groups, and industry specific threats based on in-depth analysis by the elite IBM team of threat researchers working on incident response investigations. REQ 3

IBM Resilient® Security Orchestration, Automation and Response (SOAR):

SOAR empowers security teams to more effectively and efficiently resolve security incidents. It is available as a stand-alone virtual appliance or as an integrated application in Cloud Pak for Security, either option requires a license. Additionally, it provides the following benefits:

Codifies incident response plans into dynamic playbooks to enable incident response consistency and guide investigation and remediations actions.

Maximizes security investments by easily integrating with other security and IT tools. This includes Red Hat Ansible Automation as well as more than 150 validated and community apps through the IBM Security App Exchange, an ecosystem that helps you extend the capabilities of IBM Security solutions with a host of ready-to-install Business Partner apps and add-ons.

Enables collaboration across your organization, equipping various PoLA stakeholders with the information they need to fulfill their roles and tasks as part of an incident response effort.

Provides data privacy breach reporting assistance, adding tasks associated to relevant regulations, in the event of a public data breach. Your privacy and security teams can leverage more than 170 global, state, and industry-specific regulations, including California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and many more. REQ 4

Case Management: Case Management for Cloud Pak for Security provides PoLA with the ability to track, manage, and manually resolve cybersecurity incidents. With Case Management, your security and IT teams can collaborate across your organization to rapidly and successfully respond to incidents. Case Management is a

subset of the Orchestration and Automation application and is available without an extra license on Cloud Pak for Security. REQ 5

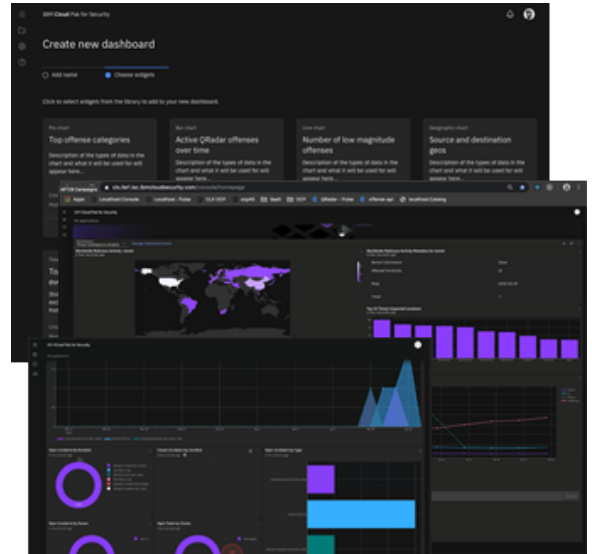
Dashboards

Organizations often struggle to obtain clear threat and risk insights from their hybrid multi-cloud security infrastructure. Cloud Pak for Security provides a simple and flexible framework for the creation of various dashboard visualizations that will allow PoLA to:

Enable users to get a sense of your organization's security posture as well as drill down to **understand the contributing factors**. REQ 6

Develop various **security dashboards based on a common framework**. Development teams can rapidly deliver special-purpose dashboards with information coming from Cloud Pak for Security apps and data services.

Create **custom dashboards from a library of widgets and data sources**. Analysts can build their own dashboard canvases and fill in with visualizations of their security data.



Drill into **dashboard views for more insights**. Analysts can drill into high-level dashboard views to get details on specific threats and risks. REQ 7

Professional Security Services

IBM offers a variety of professional services ranging from onboarding to connector development to support services to help Cloud Pak for Security enhance PoLA's security program:

Expert-on-demand services: Your security environment is unique and complex. IBM can provide consultancy services around industry best practice recommendations on threat operations, orchestration, and automation. We will work with CRC to develop a maturity model for threat operations, orchestration, and automation, tailored to your environment.

Quick Start Services: Cloud Pak for Security is most valuable to CRC when your use cases and processes are defined. To help you get the most out of your investment, IBM offers Quick Start Services that help in the deployment of Cloud Pak for Security. We pair your technical team with IBM experts to answer your deployment questions. Cloud Pak for Security comes with pre-built connectors to many cloud and security products. We can assist with configuring and customizing

these solutions for your environment and provide guidance on creating federated search queries.

Strategy and operational services: This service builds upon Quick Start Services and provides additional service options. In addition to configuring and customizing connectors and creating federated search queries to assist with your threat investigation, IBM can help you with streamlining remediation and adopting industry-standard incident response best practices. As part of the SOAR capabilities on the platform, we can help you develop custom playbooks and help automate security incident response. We also offer an optional design thinking workshop to understand your organizational priorities and tune orchestration and automation actions aligned to your business priorities.

Operations Manuals: IBM will provide an organized and succinct Operations Manual that describes how the CRC will operate. IBM utilizes the Cyber Resilience Framework and this will be the basis of the manual. This will include all the policies, procedures, roles, responsibilities, staffing levels, work shifts and contact information. IBM will provide visuals of the processes, data collection, integration and distribution flows along with the uses of CRC facility dashboards. The Operations Manual shall define and identify typical use cases and threat scenarios that may be submitted to the CRC along with the minimal technical requirements for stakeholders to connect to the CRC. The Operations Manual shall describe how planned outages occur due to scheduled maintenance and other CRC disruptions will be handled including protocols to notify stakeholders and back-up procedures.

REQ 8

Connector development services: While there are several connectors already supported by Cloud Pak for Security platform, your organization may be using a product or data source that may not have a connector available at launch. IBM can work with you to develop connectors to these data sources to leverage the full power of Cloud Pak for Security across all your tools.

Cyber Intelligence Services

IBM's innovative cyber intelligence sources are managed by X-Force IRIS Threat Intelligence Solutions. Our method includes a bespoke threat intelligence management platform powered by TruSTAR and comprehensive membership guidelines. X-Force IRIS Threat Intelligence Solutions includes data governance and role-based access control (RBAC) best practices. As a threat intelligence platform member, Cyber Resilience Center (CRC) stakeholders receives value-driven content and a custom experience. X-Force IRIS Enterprise Intelligence Management extends platform access and allows you to exchange data within your organization, with IBM, and other permissioned intelligence sharing enclaves and communities.

A core component of the proposed threat intelligence solution is a robust Premier Threat Intelligence knowledgebase. Centralized knowledge acts as the hub of a cyberthreat intelligence wheel; absorbing, analyzing, classifying, authenticating,



anonymizing, and redistributing threat intelligence from our global threat intelligence and operational network. IBM Security proposes to support the client's mission to automatically exchange threat intelligence information with businesses, government agencies, and other third parties.

X-Force IRIS offers Threat Intelligence Solutions in a cloud environment having application website operations, backend data enclaves, plus threat intelligence feed aggregation that integrates directly with Cloud Pak for Security (CP4S) dashboards.

IBM's intelligence sources aggregates both open and closed intel sources, integrates with security workflow applications (Cloud Pak for Security [CP4S], Security Operations and Response [SOAR], Case Management, and delivers bi-directional communication for intel and systems improvement updates, and a secure threat intelligence sharing capability for both internal and external use.

We curate our threat intelligence from real world IBM Security Incident Response Investigations, IBM Managed Security Services operations, IBM Security Research, and both open and closed sources. We deliver consulting and management services to benchmark and roadmap client threat intelligence capabilities and programs.

Our intelligence sources will provide PoLA CRC with:

X-Force IRIS Threat Intelligence sources that can help the CRC operationalize, automate, and optimize your threat intelligence management programs. You can exchange threat information between stakeholders and make intelligence sharing more efficient and secure. X-Force IRIS Threat Intelligence Sources provide: High-quality, prioritized, human readable, **actionable intelligence** for both detection and response capabilities from both common and unique sources.

A partnership with highly respected **intelligence experts** that can design, build, deliver, and operate an automated cyberthreat intelligence services and solutions.

The means to aggregate, operationalize, and share **threat information** within an organization and industry peers in near real-time.

The opportunity for **integration of threat intelligence** into security workflow applications via pre-built Application Program Interface (APIs).



Firm Qualifications, Experience and References

Organization	Contact	Title	Phone No.
Los Angeles Cyber Lab	Chris Covino	Policy Director for Cybersecurity	213-534-7372
IT-ISAC	Scott Algeier	Executive Director	703-385-4969
RH-ISAC	Tommy McDowell	Executive Director	720-309-9958
USC Keck Medical	Christian AbouJoude	Chief Technical Officer	323-865-7970

Reference: Los Angeles Cyber Lab

The Client: Home to approximately 20 million people in its metropolitan area, this major American city aims to enable businesses, government agencies, and other third parties to automatically exchange threat intelligence information, as a result of its newly created information sharing and analysis organization.

The Requirement: The client was looking to partner with a leader that could design, build, deliver and operate a cyber threat platform, which provides accurate and up-to-the minute cyber threat data from both common and unique sources.

IBM Security and TruSTAR partnership deliver value via Amazon Web

Services: The IBM Security X-Force IRIS Threat Intelligence team has fast become known for its ability to create new cyber threat intelligence and add insight to existing threat information. With its winning formula focused on Trust and Technology, the IBM Security team partnered with enterprise intelligence management provider, TruSTAR to deliver the cloud-architected solution on Amazon Web Services.

Many organizations struggle with creating threat intelligence for various reasons – trust, availability, and integration with other sources – and then converting the information into meaningful and actionable tactics. However, the IBM Security X-Force IRIS Threat Intelligence team creates new threat intelligence for IBM Security every day, using commercial data sources for malware, surface web, dark web and open data sources from IBM’s Threat Intelligence Liaison program. The team has also built a practice around relationships with global CERTs, other country government entities, private industry, US government entities and special interest groups.

- 34 Private Industry
- 30 US Government entities
- 16 Other Country Government entities, originating from G20 and NATO
- 14 Global CERTs

- 7 Special Interest Groups

To bring this capability to the client, the team relied on TruSTAR to use the Amazon Web Services architecture to deconstruct a monolithic threat intelligence exchange into elemental micro-services. TruSTAR has the ability to scale critical functions of their exchange and provide resiliency and reliability. The AWS technology stack used by TruSTAR includes a variety of AWS products, such as AWS EC2 and S3.

The solution impact:

With the possibility of mounting cyber threats to several densely populated areas, many municipalities across the world face a growing need for insightful information to act and react to real-time dangers.

The combined capabilities of IBM's Threat Intelligence team, along with TruSTAR's platform within the AWS Cloud presented the client with innovation required to quickly and flexibly centralize threat intelligence data, which is designed to protect the citizens and businesses within the metropolitan area. Using the AWS platform, TruSTAR is helping to bring the client collaborative threat intelligence, ensuring data governance, and quickly provisioning the cloud architecture to meet the client's needs to deal with critical cyber threat.

References for Alliance Partner, TruSTAR: IT-ISAC and RH-ISAC

As a leader in intelligence management and fusion, TruSTAR provides a robust platform for ISAC/ISAO's, such as RH-ISAC and IT-ISAC, to facilitate, manage and share threat intelligence with member organizations. TruSTAR understands the greater value of both RH-ISAC and IT-ISAC and supports their missions to provide an ecosystem for the retail and hospitality industries as well as customer-facing companies to share intelligence and best practices - all to build better security through collaboration. Since early 2017, TruSTAR has forged an integrated partnership with RH-ISAC and IT-ISAC, presenting unique, valuable benefits to their members which include centralized, secure platform to share threat intelligence, one-to-one onboarding plus training webinars, monthly account and member activity/usage reports, white glove support covering 24x7 response, and inter-ISAC and enterprise introductions to encourage cross-industry intel sharing and strategic discussions.

Reference: University of Southern California Keck Medical

The Client: The **Keck Hospital of USC**, formerly **USC University Hospital**, is a private teaching hospital of the University of Southern California (USC). The Hospital is part of the USC Keck School of Medicine. They are located on the USC Health Sciences Campus. USC Keck Medical is dedicated to promoting health, preventing and curing disease, advancing biomedical research and educating tomorrow's physicians and scientists.



The Requirement: The client was looking to partner with a leader that could design, build, deliver and operate a Managed Security Information Event Management solution, that could operate 24 hours a day 365 days a year. This solution helps to alert USC Keck Medical of security offenses that could effect their network.

The proposed team does not include former Commissioner, officers or employees of the Harbor Department.

Project Organization, Personnel and Staffing

Project Personnel and Staffing

Security Analyst

Name Withheld

Contact withheld

INSIGHTFUL, SENIOR CYBER SECURITY ANALYST Implementing Mitigation Strategies through Risk Management

Mitigates possible attacks on network infrastructure based on intrusion detection system alerts, open source research, and deep dive of packet analysis to determine the best possible recourse for blocking, intercepting, or resetting known for zero day threats.

Superb analytical skills, matched with effective communication. Excel in fast-paced environment and exceed goals. Express strategies and solution with others and come up with new approach and renewed energy to tackle any network threat challenge.

Areas of expertise includes: Digital Forensics and Incident Response (DFIR) | Security Analysis & Consulting | Threat and Vulnerability Management (TVM) | Cloud technologies | Secret Clearance |

Technical Skills: Deep packet analysis, QRadar, basic malware analysis, Splunk, intrusion analysis, intrusion detection systems, network troubleshooting/configuration, IT Service management Experience, familiarity with system log information, ArcSight, TCP/IP troubleshooting, understanding of common network services (web, mail, DNS, authentication), knowledge of host based firewalls, HIDS/IDS

Programming Skills: Academic knowledge of C++ and Java. Familiar with security related/scripting languages like Perl. Experience with UNIX, Linux, Windows Operating Systems

PROFESSIONAL EXPERIENCE

IBM, Austin, TX

2014 - present

Senior Cyber Threat Analyst and Cyber Incident Response Team (CIRST)

Pro-actively identify suspicious and malicious network activity. Monitor Security information and event management (SIEM) platform, investigate complex security incidents, and provide forensic and monitoring capabilities.

- Manage Advanced Persistent Threat (APT) white and black list in SIEM, disseminating to appropriate operators for tool policy and setting updates in security tools.
- Create cyber threat intelligence reports, using Open Source Intelligence (OSINT), with actionable metrics and indicators of compromise, keeping senior management abreast on latest threats.
- Triage and resolve advanced vector attacks, such as ransomware and persistent malware, through triage and open and track tickets for remediation of issues found during incident or vulnerability.
- Develop security operation center (SOC) runbooks, ensuring SOC's controls and procedures operating effectively relative to predicted effectiveness of mitigation.
- Provide management oversight for identification, triage and response of events or incidents of apparent security breaches over private and public cloud environments.
- Deliver tuning recommendations of policy in security control tools to administrators, based on findings during investigations and threat information reviews.

NAVAL INFORMATION OPERATIONS COMMAND, San Antonio, TX

2011 - 2014

Senior Cyber Analyst

Oversaw and provided leadership for initiatives concerning overall security of organization, including consulting with law enforcement, NSA customers, and partners on security matters.

- Planned and coordinated Continuity of Operations Planning (COOP) exercises, ensuring mission readiness and refining policies and procedures, which increased efficiency within the SOC.
- Monitored security threats, via SIEM, analyzing network packets, acting as focal point for security investigation, and directing full investigation with recommended course of action.
- Produced detailed incident reports and technical briefs with metrics for management, administrators, and end-users used, determining better processes and quicker mitigation of alarms.
- Conducted log analysis across a diverse ecosystem of technology to locate root cause of incidents.

Incident Commander Resume

IBM Incident Commander - Name Removed

Contact Removed

PROFESSIONAL SUMMARY

U.S. Marine Corps Veteran with over 22 years of Security Operations leadership experience that includes employing Encase Cyber Security, Network Access Control Net – FTK/Witness Investigator and Informer; ArcSight 6 Console, Logger and Express; Fire Eye Email Protection, Fire Eye Web Protection, En Circle, Jump Server, Blue Coat, Snort, ASA Firewall, SCCM, Splunk, and Sourcefire. Meticulous and dedicated professional with experience abiding by Security Operations Guideline protocols NIST, US Cert, and FISMA Framework.

CERTIFICATIONS

- North American Electric Reliability Corporation (NERC)
- Federal Energy Regulation Commission (FERC)
- CISSP

EDUCATION

- Walden University: **PhD, Security Management – 2017**
- Strayer University: **MBA, Information Security Management – 2009**
- Strayer University: **BA, Business Management – 2008**

SECURITY TOOLS/SKILLS

- | | | | |
|----------------|----------------|-----------------------|--------------------------------|
| ▪ NBT Scan | ▪ Splunk SIEM | ▪ HP Logger | ▪ Web Sense |
| ▪ Metasploit | ▪ QRadar | ▪ EnCase Enterprise | ▪ Protection |
| ▪ CORE Impact | ▪ Source Fire | ▪ HP ArcSight Console | ▪ Symantec Endpoint |
| ▪ Cylance | ▪ Checkpoint | ▪ Fire Eye Web | ▪ Protection |
| ▪ Splunk 6.4 | ▪ McAfee | Protection | ▪ Net Witness Investigator FTK |
| ▪ Palo Alto | ▪ Nessus | ▪ Fire Eye Email | ▪ rapid 7 |
| ▪ ASA Firewall | ▪ Carbon black | ▪ TCP Dump | ▪ Blue Coat |
| | ▪ Tanium | ▪ log rhythm | ▪ Qualys |

PROFESSIONAL EXPERIENCE

Security Engineer hands On Manager- June 2018-Present

IBM (Client)

Used Intrusion Detection/Prevention Systems daily, perform in-depth as a Blue Team/Red Team expert and point man for the SOC analyst/ vulnerabilities team conducting incident response, event, and threat intelligence for the corporate enterprise

- Experience with multiple attack vectors such as: Malware, Trojans, Exploit Kits, Ransomware and Phishing, and Botnet.
- Reviewed logs and vulnerabilities utilizing CIRATS (Compliance Issue Risk and APAR Tracking, 48 Reports, and I oversee 3 locations. Build many SOC's from ground zero until go live.
- Maintained the Intrusion detection system and monitoring all events and traffic
- Performed Computer Security Incident Response activities for a large organization, coordinates with other government agencies to record and report incidents.
- Monitored and analyze Intrusion Detection Systems (IDS) to identify security issues for remediation.
- Analyzed malware behavior, network infection patterns and security incidents in defense of U.S.
- Analyzed approximately 10 classified network security intelligence reports daily.
- Specialized in network centric analysis utilizing a variety of tools and techniques such as Network Security Monitoring, log analysis, and more.
- Monitored, detected, and analyzed network traffic for malicious activity and provide reports.
- Used net-witness to analyze PCAPs



Project Manager – IT Security Services PMO

Name Withheld

EXECUTIVE SUMMARY:

A charismatic results-oriented Agile PMO and Monitoring/Compliance Program Manager with 13 years+ of experience in Strategic Project/Program/Portfolio Management; consultation/supporting international customers with industry focus of Electronics, Telecom, E-Commerce, FIN, Sales/ MRKG, Semiconductor, IT, US Federal & Healthcare (Clinical). Have a successful record of accomplishments in SW Dev/Testing, IT Infrastructure, IT Security, SaaS, Mergers Acquisitions & Divestitures on RUP, ITIL, SOX, CMM/CMMI, TMMI, Agile/Scrum, COBIT, PMI Frameworks. A team player; always giving extra mile to achieve goals/objectives & results/benefits. Extremely passionate about driving org's towards excellence, enterprise effectiveness through promoting change & improving processes.

KEY SKILLS:

Project/Program/Portfolio Management (PMO):

- Global PMO Setup/Management/Support and Governance/Process Institutionalization
- Project, Program and Portfolio Management, Strategic Alignment, Continuous Delivery, Onsite/Offshore Model
- Stakeholders, Budget, Business Value/Benefits Management
- Organizational Change, Enterprise Risk Management and Data Loss Prevention
- IT Service Management, Enterprise Process/SOX Compliance Audits and Scorecards

Compliance/Monitoring:

- Support Information Security Operations Center (ISOC) by assessing/monitoring/defending information systems; web sites, applications, databases, data centers and servers, networks, desktops and other endpoints
- Support managing incidents ensuring they are properly identified, analyzed, communicated, actioned, investigated and reporting.
- Support monitoring apps to identify a possible attacks or events and determines if it is a real, threat or incident.
- Support Enterprise Security Information & Event management (SIEM) S/m for NW discovery, vulnerability, governance risk & compliance (GRC), monitoring, application & DB scanners, intrusion detection/prevention, log management, NW behavior & firewalls
- Support process compliance, score carding, reporting org level data to the senior management

Technical:

- Microsoft Project Server 2013 (EPM/MPP/PWA), and Microsoft Technologies (SharePoint, .NET, Exchange)
- SDLC (Agile/Scrum, Waterfall, RUP), SW Testing (STLC, WinRunner, Microsoft Stress, Astra Load, HP QC, QTP)
- VB, ASP, HTML, Java, Java Script/Beans, CGI (w/C & Perl), JDBC, Servlets, UNIX/LINUX, C++, PHP, CSS, XML, RSS
- ITOnline, VSS, LiveLink, JIRA, GIT, UCM, Databases (Oracle, MySQL, PL/pgSQL), Mural, Slack, Trello
- IT Infra. (Data Center, Networking, Identity and Access), BC/DR/Information Security and RiskManagement

Clients:

1. Pharmacy Retailing Industry, The Drugstore Chain
- 2.
3. Government Department, The City Department of IT & Telecomm.
- 4.
5. Electronics, Semiconductors and Home Appliances Industry
6. Higher Education Industry
- Global Food and Beverage Distribution industry

CERTIFICATIONS	TRAININGS	COMMUNITY GIVING
<ul style="list-style-type: none"> ➤ Certified Scrum Master (CSM) ➤ Prog. Man. (George Washington University, School of Business) ➤ IBM Security Essentials ➤ Certified Software Quality Analyst (CSQA) ➤ Project Man Professional (WIP renewal) 	<ul style="list-style-type: none"> ➤ Citizens Police Academy – Class 34, Fall 2018 ➤ IBM Cloud Top Gun Boot camp/Course – Introduction to Selling Cloud Software and Services Cognitive Patterns ➤ Artificial Intelligence (AI) – aarago.co ➤ Medical (AHM 540) and Healthcare Management (AHM 250) ➤ Intermediate Concepts of SEI CMMI DEV 	<ul style="list-style-type: none"> ➤ Board Commissioner – for Williamson County Emergency Services District (ESD) # 9, TX USA ➤ Board Director – for Home Owners Association (HOA) ➤ Member of – Agile Austin University (U), and ParksideHOA Communications Committee



Product Partner: Trustar

Head of Customer Success: 15+ Years of Account Management / Sales Experience, Collaborating with Engineering, Marketing, and Service Departments, 3+ Years of SaaS Account Management / Sales Maintaining Relationships with Channel Partners (VAR). Responsible for leading the direction and overall strategy of Customer Success program OKRs. Handles all CS program accounts.

Account Manager: 7+ years experience in cyber, fraud, abuse, and data center account support. Responsible for managing the success of individual accounts as key lead and point of contact. Handles a specific 10-15 accounts at any given time.

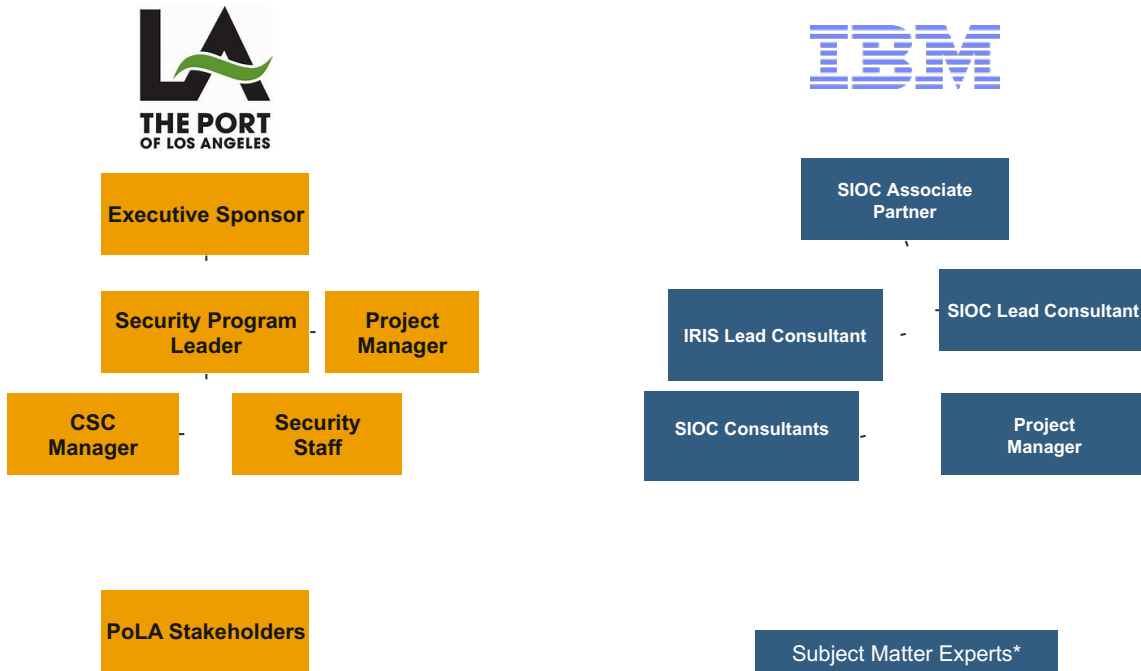
Technical Account Manager: Software / Machine Learning, 10+ years in engineering related fields for US government. Responsible for partnering with Account Manager to ensure implementation of technical resources, integrations, and workflow inputs are completed. Handles a specific 10-15 accounts at any given time.

Product Support Manager: 4+ years as Enterprise Customer Support and Enterprise Product Specialist. Responsible for all issues relating to product / technical requests, partnering with Account Manager to ensure all support tickets are completed to adhere to SLAs. Handles 20-25 accounts at any given time.



Project Organization

Transformation Resources



Implementation plan by phase

PHASE 1: Program Initiation and Planning	PHASE 2: CRC CP4S / TruStar System Design	PHASE 3: Implementation	PHASE 4: Integration and Transition	PHASE 5: Ongoing Operational Support
<ul style="list-style-type: none"> Program Kickoff and Initial Data Collection Requirements Definition and Planning Session Stakeholders Use Case Validation Workshop Architecture and Intelligence Sources Workshop 	<ul style="list-style-type: none"> Detailed Process and Data Gathering Detailed Functional and Non-Functional Requirements Gathering Macro Architecture Design (Logical) Micro System Design (Physical) Design Review 	<ul style="list-style-type: none"> Configure CP4S Configure TruStar Intelligence Collection Deploy and Test Use Cases Perform Any Custom Development and Integration Test, Tune, and Optimize CP4S / TruStar 	<ul style="list-style-type: none"> Staged Transition to Operational Support Metrics Report, Communication Plan, Runbook, and Resilient Playbook Definition Readiness Assessment and Simulated Operations 	<ul style="list-style-type: none"> Real Time Event Monitoring Notification Report generation, review, and analysis CP4S System Management CP4S System Change Requests X-Force Investigation Analysis Resilient Orchestration
<ul style="list-style-type: none"> Initial Project Plan 	<ul style="list-style-type: none"> Macro and Micro Design (DRAFT) 	<ul style="list-style-type: none"> Operational SIEM 	<ul style="list-style-type: none"> Macro and Micro Design Comm. Plan and Runbook Support 	<ul style="list-style-type: none"> Regular Reporting XF-IRIS Reports Quarterly Advisory Service

Transition

Introduction

IBM is committed to providing PoLA with an efficient and smooth Transition of Services, performed with thoughtful planning and methodologies which have been tested and proven through hundreds of transition projects. The main objectives of our transition approach are to accelerate cost saving for PoLA, continue maintaining or improving the quality of the business processes, minimize risks to ongoing operations, and execute efficient and effective Knowledge

Transfer.

Critical Success Factors for Transition

Based on our extensive experience, we have identified the following critical success factors, which we have incorporated into our Transition approach for PoLA:

- A dedicated transition team from IBM and PoLA who will collaborate / work together from the identification through the completion of the transition activities;
- A joint IBM and PoLA transition plan that addresses the needs of internal and external stakeholders and includes change management and communication activities;
- Upfront agreement on transition plans and process changes;
- A strong and collaborative approach to Knowledge Transfer from PoLA to IBM;
- Early identification and testing of connectivity and environments between IBM and PoLA;
- Proactive Change Management planning; and
- Formal joint sign-off before physical transition to the IBM Service Delivery Centers.

Highlights of IBM's Transition approach for PoLA

The IBM approach is customized for each workstream but utilizes common overall methodology and Project Management structure. Highlights of the common approach are outlined below:

Collaborative Planning and Data Gathering: Each workstream will quickly assemble its transition team after contract signature and initiate a detailed and collaborative transition planning session with PoLA counterparts. IBM will also bring in the process experts early on to initiate process design workshops and business requirements gathering for the implementation of new tools;

Cross Workstream Team: Along with specialized workstream transition teams, IBM will have a cross workstream team that will facilitate frequent communication and interaction between workstreams, as well as leverage lessons learnt across workstreams. The IBM cross workstream team will also include Change Management experts who will work closely with PoLA staff to support appropriate and timely communication to affected organizations and promote change readiness.

Disclaimer

This document depicts an overview of a typical Transition Plan that IBM has successfully delivered in several similar programs around the world and it is not intended to be comprehensive and / or exhaustive.

During the first weeks of the program, IBM will gather specific points and needs from PoLA in order to develop a comprehensive and sound Transition Plan for each workstream.

Project Approach and Work Plan (Scope of Work)

As the primary contractor, IBM will deliver to the Port of Los Angeles the required resources, processes and technologies for a turn-key CRC solution. All aspects of the CRC work shall employ a collaborative approach with participating stakeholders. The requirements below provide the framework and minimum requirements of the system.

The CRC project scope of work shall include the following elements:

- Governance
- Design data sharing agreements
- Installation
- Stakeholder onboarding
- Operations
- Warranty
- Maintenance and support
- Project closeout

Governance

This section describes the Governance Program for the Port of Los Angeles Cyber Resilience Center (CRC). The purpose of the Governance Program is to describe the specific roles and responsibilities of the program and its stakeholders, focusing primarily on authority level and decision-making structure.

Guiding Principles

The primary function of the CRC Governance Program is to define and implement a structure which provides visibility, management, and administration for all levels of the CRC. The governance program will provide oversight, regularly review performance, and identify adjustments to ensure achievement of the planned CRC objectives. The owners, stakeholders, and participants of the CRC Governance Program are charged with ensuring that the CRC; REQ 9

- Is operating within predefined performance targets and measurements.
- Addresses and tracks key risk indicators and compliance requirements.
- Manages resource capacity and matures capabilities.
- Maintains proper resources (people, systems, funding, authority, etc).
- Sustains a connection to the overall PoLA security strategies.

CRC Governance Scope & Operating Model

PoLA's CRC is tasked with the identification, investigation, and oversight over cyber events within PoLA's stakeholders. Scope for the CRC includes proactive intelligence analysis of both internal and external sources, monitoring of potential security event activity and initiating escalation and alerting to specified stakeholders for the duration of the agreement. REQ 10

In order to understand the integration required and define the scope for the CRC Governance Program, the CRC Operations Model will include an organizational and data flow model of the steady state operations of the CRC. It will provide an operational representation of the complexity of the major functions of the CRC and their relationships and interactions with stakeholders. Please note that relationships and interactions between groups are not strictly limited to the arrows shown in the diagram. Other exchanges are expected, however the relationships are intended for the teams interact with each other, and evolve as the threat landscape evolves.

CRC Governance Communications



CRC Governance Meetings

The goal of the governance meetings is to review status/progress of approved CRC operational priorities and provide support to address priority issues, determine which new priorities should be implemented next, and potentially approve necessary resources (funding and staff) for the initiative.

The table below provides a high-level list of the required CRC Governance Program meetings and a short description of key topics for each. The remainder of this section provides a detailed description including the audience, ownership and the purpose of each meeting.

Note: the section table for each meeting is listed under the meeting title.

Meeting	Key Topics	Frequency
Executive Information Technical Committee	<ul style="list-style-type: none"> Updates to and from the Security teams Oversight/Input from committee on tactical moves/decisions Ad Hoc measurements may be presented related to tactical decisions 	Quarterly
ITD Security Leadership	<ul style="list-style-type: none"> Security Program Maturity Security Risks and Mitigation 	Monthly
PoLA CRC Leadership	<ul style="list-style-type: none"> Team & leadership updates Intelligence sharing (IoC's, New Threats, Trending) Lessons learned 	Monthly
CP4S / IRIS TruStar (CRC Focus)	<ul style="list-style-type: none"> Technical Review 	Monthly
Use Case Governance	<ul style="list-style-type: none"> Review Use Case Strategy against business risk and compliance requirements Review Use Case Activity Tracker and CP4S change recommendations from Use Case Development team Stakeholder Management 	Monthly



CRC Oversight	<ul style="list-style-type: none"> • Key Risk/Performance Indicators (KRI/KPI) • Security Posture (NIST, Kill Chain, Intel Analysis) • Operations Mgmt.(Efficiency/Capacity) 	Monthly
CP4S Development	<ul style="list-style-type: none"> • Review rules that have been identified for possible changes or tuning associated with SOC capacity and SOC procedural runbooks • Review and prioritize use cases and rules that will be proposed to the Use Case Governance team for addition during next development cycle • Update the Use Case Tracker for submittal to Use Case Governance team 	Bi-weekly
CRC Management & Showcase	<ul style="list-style-type: none"> • Progress Updates 	Bi-weekly
CRC Planning	<ul style="list-style-type: none"> • Goals and expectations setting • Workload and staff commitment planning 	Bi-weekly
CP4S / TruStar Intel Tuning	<ul style="list-style-type: none"> • Use Case/ review • CP4S / TruStar rule tuning 	Weekly
Daily Status Updates	<ul style="list-style-type: none"> • Daily updates • Identifying blockers 	Daily

Strategy and Oversight

Title:	Strategy and Oversight Steering Committee
Description:	The Executive Oversight and Steering Committee provides the highest level of oversight for the operational performance of PoLA. The committee is comprised of key executive stakeholders from across PoLA ensuring proper representation and prioritization of PoLA activities. The committee meets on a regular schedule (quarterly) to review PoLA’s security posture and PoLA performance against assigned key risk indicators (KRIs). REQ 11
Decisions / Actions:	There are no standing decisions or actions this committee will undertake, however, based upon the information provided in the session and corresponding discussions may result in assignments or adjustments. Those activities will be captured by the meeting facilitator and will be responsible for reporting status back to the key stakeholders, if required, during the next committee meeting or agreed upon method.



Key Topics and Metrics	<ol style="list-style-type: none"> 1. Review of Risk and Security Posture 2. Key Risk Indicators 3. PoLA metrics by Service and Maturity Indicators 4. Considerations and Recommendations
Session Output:	Meeting minutes
Key Stakeholders:	Designated by CISO
Owner / Facilitator:	CIO
Contributors:	PoLA Director, PoLA Manager, CSIRT Manager, PoLA Operations Manager
Frequency:	Quarterly
Duration:	60-90 minutes

Operational Governance

Title:	Operational Governance
Description:	The Operational Governance Committee is responsible for the coordination of key service and functional areas. The committee’s intention is to review and improve the performance of the PoLA and its interactions across PoLA. REQ 12
Decisions / Actions:	There are no standing decisions or actions this committee will undertake, however, based upon the information provided in the session and corresponding discussions may result in assignments or adjustments. Those activities will be captured by the meeting facilitator and will be responsible for reporting status back to the key stakeholders, if required, during the next committee meeting or agreed upon method.
Key Topics and Metrics	Key Risk Indicators (KRIs) View by Department / Areas PoLA Capabilities / Maturity Security Posture (NIST, Kill Chain, Intel Analysis) Operations Management (Efficiency / Capacity)
Session Output:	Meeting minutes
Owner / Facilitator:	PoLA Security Manager



Key Stakeholders:	PoLA CISO, PoLA Manager, Project Manager
Contributors:	PoLA Operations Manager, Threat Intelligence analyst, Threat Response Analyst
Frequency:	Monthly
Duration:	60 minutes

Stakeholder Cyber Intelligence Governance

Title:	CTI Governance, Intake, and Prioritization
Description:	<p>The CTI Governance meeting is responsible for setting the development roadmap for use cases to be handled by the PoLA. This forum will review in-production use cases and suggested requests from both PoLA and Intelligence Analysts within the PoLA organization. Use cases will be assessed based upon their impact to the business, compliance requirements etc. The PoLA will provide the operational capacity, feasibility, and level of effort for each proposed use case.</p> <p>After review of proposed and requested use cases, the CTI Use Case Governance meeting will adjust the current use case development roadmap, if required, to reflect decisions made in this session. Actions may include adding new and modifying or removing existing use cases.</p>
Decisions / Actions:	<p>The primary function of the Use Case Governance meeting is to determine the optimal development roadmap of use cases for the PoLA. Stakeholders in this session are required to weigh the impacts of any additions and changes to the use case roadmap.</p> <p>The meeting owner will document decisions and update the PoLA Use Case Framework and Roadmap accordingly.</p>
Key Topics and Metrics	<ol style="list-style-type: none"> 1. Use Case Intake and Prioritization 2. Use Case Roadmap 3. Procedural Playbook
Session Output:	Meeting Minutes, Use Case Framework, and Roadmap Update



Owner / Facilitator:	PoLA Security Manager
Key Stakeholders:	PoLA CISO, CSIRT Manager, PoLA Operations Manager, Threat Intelligence analyst, Use case engineer, Threat Response Analyst
Contributors:	Threat Triage Analyst, Threat monitoring Analyst, PoLA Admin
Frequency:	Monthly / Scheduled as Required
Duration:	60 min

Cyber Intelligence

Title:	Threat Intelligence Cadence
Description:	The PoLA Threat Intelligence Cadence session will review and monitor the overall security posture for PoLA. Individual intelligence feeds, hunting assignments, and security controls will be included in the review.
Decisions / Actions:	There are no standing decisions or actions assigned to the Threat Intelligence Cadence, however based upon the information provided in the session and corresponding discussions may result in analyst assignments or procedural adjustments.
Key Topics and Metrics	<ol style="list-style-type: none"> 1. Security Posture (NIST, Kill Chain, Intel Analysis) 2. Consolidated Intelligence reports and Use Case recommendations 3. PoLA Playbook
Session Output:	Revised analyst assignments, updated PoLA Playbook
Owner / Facilitator:	PoLA Security Manager
Key Stakeholders:	PoLA Operations Manager, Threat Intelligence analyst, Threat Response Analyst
Contributors:	Threat Triage Analyst, Threat monitoring Analyst, PoLA Admin
Frequency:	Weekly
Duration:	60 min



CP4S / TruStar Engineering

Title:	CP4S/TRUSTAR Engineering Cadence
Description:	The CP4S/TRUSTAR Engineering cadence session will review the status of the CP4S/TRUSTAR environments including health, availability, and capacity. Additionally, the status of log sources, current and in-development will be reviewed to ensure proper handling.
Decisions / Actions:	There are no standing decisions or actions assigned to the CP4S/TRUSTAR Cadence, however, based upon the information provided in the session and corresponding discussions may result in analyst assignments or procedural adjustments.
Key Topics and Metrics	<ol style="list-style-type: none"> 1. Availability 2. Capacity 3. Maintenance and Projects 4. CP4S/TRUSTAR Rules 5. Stakeholder CTI Management
Session Output:	CP4S/TRUSTAR environment adjustments, Engineer assignments
Owner / Facilitator:	PoLA Operations Manager
Key Stakeholders:	CP4S/TRUSTAR Admin, Integration engineer
Contributors:	Threat Monitoring analyst, Threat Triage analyst , Threat Response Analyst
Frequency:	Weekly
Duration:	60 min

Operations Scrum

Title:	Operations Scrum
Description:	The PoLA Operations Scrum is used to coordinate operational efforts at an analyst level. Led by PoLA Managers, analysts meet to discuss ongoing investigation and incident activity, post-incident reporting and train on procedural updates enhancements, and briefed on current threat intelligence. REQ 13



Decisions / Actions:	There are no standing decisions or actions assigned to the Operations Scrum, however, based upon the information provided in the session and corresponding discussions may result in analyst assignments or procedural adjustments.
Key Topics and Metrics	1. Awareness / Education and Procedural Updates 2. Team Problem Solving 3. Daily Flash
Session Output:	Analyst assignments, Adjusted workload distribution
Owner / Facilitator:	PoLA Operations Manager
Key Stakeholders:	Threat Monitoring analyst, Threat Triage analyst, Threat Response Analyst
Contributors:	Threat Intelligence analyst, PoLA Admin
Frequency:	Daily (Monday – Friday)
Duration:	30 min

Cloud Pak for Security System Design

During this phase, IBM will work with you to design the elements of the CRC in collaboration with stakeholders, based on CRC requirements as evidenced by deliverables such as, but not limited to, the data collection questionnaire, the network diagrams, regulatory requirement documentation, and skill levels. REQ 14

IBM Responsibilities for System Design

Activity 1 - Process and Data Gathering

The purpose of this activity is to gather and review process documentation and data elements that will be needed to develop or review the implementation strategy for Your environment, objectives, and constraints according to the services contracted. IBM will:

- a. conduct interview(s) and/or workshops and review documentation to establish the business goals, security objectives, and high-level requirements relevant to the implementation;
- b. collect and review stakeholder requirements which may include:
 - 1) Incident management;
 - 2) change management;
 - 3) problem management;
 - 4) configuration management (including asset management);

- 5) security management (including vulnerability management and risk assessments);
 - 6) availability management;
 - 7) CRC operations;
- c. collect and review the following data elements which may include:
- 1) business requirements;
 - 2) threat intelligence;
 - 3) operations
- d. compile collected process documentation and data elements within a central repository for use by IBM delivery personnel and PoLA Authorized Security and Designated Services Contacts.

Activity 2 - Requirements Definition and Documentation

The purpose of this activity is to define, document, and map (or review if already deployed) functional and non-functional requirements for the SIEM Solution. IBM will:

- a. collaborate with PoLA to define, document, and map the following functional requirements as they pertain to the CP4S and TruStar Solutions:
- 1) Stakeholders CTI use case requirements;
 - 2) Data Sources;
 - 3) Intelligence collection;
 - 4) normalization;
 - 5) correlation;
 - 6) storage;
 - 7) system access;
 - 8) reporting; and
 - 9) customization requirements;
- b. collaborate with PoLA to define, document, and map the following non-functional requirements as they pertain to the SIEM Solution:
- 1) monitoring;
 - 2) retention;
 - 3) reporting;
 - 4) regulatory and contractual considerations;
 - 5) high availability;
 - 6) disaster recovery; and
 - 7) success criteria for the target state.

Activity 3 - Architecture Design

The purpose of this activity is to develop the high-level architectural design for

the contracted services. IBM will:

- a. design and document architecture for the CP4S Solution components; and
- b. make recommendations based on findings identified in the Process and Data Gathering and Detailed Functional and Non-Functional Requirements Definition and Documentation Activities.

Activity 4 - System Design

The purpose of this activity is to develop both macro and micro system design elements to be implemented in order to reach an initial steady state of operations. IBM will:

- a. define at the macro system design level:
 - 1) data/event source collection protocols and methods;
 - 2) data/intelligence risk weighting criteria;
 - 3) classification profiles;
 - 4) compliance groupings for intelligence;
 - 5) custom data source requirements;
 - 6) CTI Use Case frameworks and corresponding IBM Cloud-Hosted CP4S Resilient Playbook selection, if applicable;
 - 7) customization requirements;
 - 8) dashboard requirements for the CRC CP4S console; and
 - 9) user accounts and roles; REQ 15
- b. define at the micro system design level:
 - 1) data/event source phased integration plan;
 - 2) Alert classification criteria; REQ 16
- c. prepare the System Design deliverable which will include:
 - 1) strategy considerations including but not limited to CRC business drivers and goals, CP4S security objectives, and functional and non-functional requirements; and
 - 2) architectural, macro, and micro design elements as defined in this activity.

Activity 5 - Design Review

The purpose of this activity is to review the design and finalize the Project Plan. IBM will:

- a. review the architecture and system design;
- b. perform one revision of the Project Plan as appropriate;
- c. deliver the final Project Plan to the PoLA Project Manager; and
- d. deliver the System Design to the Client Project Manager, and if requested, review the design and Project Plan with Your Point of

Contact and Your key stakeholders via teleconference or electronically.

IBM IRIS Cyber Intelligence Services

Our proposed solution is built upon standard and proven capabilities in accordance with the IBM Security Framework. This will be done in order to accelerate the transformation of the Port of Los Angeles Cyber Resilience Center into a best-in-class, intelligence-driven, and agile security operation which will have the right combination of skills, intelligence, tools, and IT Risk Management practices to proactively mitigate advanced threats.

At the same time, to maintain a consistent security program and align internal and service provider resources, enterprises are adopting the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).^{REQ 17} This solution aligns with and expands on the NIST CSF using mature products and capabilities from the IBM Security Services portfolio to provide coverage across the entire threat management lifecycle.



Figure 1: A SMARTER SECURITY SOLUTION TO MANAGE THE 360 DEGREE THREAT LIFECYCLE aligns with NIST CSF

This IBM solution also incorporates innovative response techniques such as threat hunting with real-time forensic detail designed to quarantine suspect code before it enters an organization’s network, or to help isolate an infected host. Information is transparently shared between the CRC and CRC Stakeholders throughout the duration of any security incident using both automated notifications and human-driven responses—so clients know exactly what’s happening and what’s being done.

Our solution comprises platform-driven integration, context-awareness, augmented intelligence, automation, and orchestration, along with digital client engagement. The approach is based on the NIST (U.S. National Institute of Standards and Technology) Cybersecurity Framework and builds upon NIST with a unique IBM point of view and set of capabilities.

Created through collaboration between industry and the U.S. government, this voluntary Framework consists of standards, guidelines, and practices to promote the

protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

However, the NIST framework can be challenging – consisting of five functions, 22 Categories and 98 Subcategories (outcomes or controls) and covering topics related to everything from risk assessment to incident response, leading to legitimate concerns about resource requirements and the overall effort needed for implementation.

IBM provides not only the expertise of its skilled cyber security personnel needed to operationalize the NIST cyber security framework, but also the orchestrated standardized methods that provides scalability, customer-wide standardization, consistency and accuracy.

This solution is based on an IBM superset of the NIST Cybersecurity framework. The NIST Cybersecurity Framework (CSF) includes 5 functions: Identify, Protect, Detect, Respond, and Recovery. This solution contains all of the business processes contained within the NIST CSF but adds a unique IBM POV or leverages unique IBM capabilities. For example, threat recovery utilizes X-Force IRIS to help return affected systems to their previous state post-incident, and IBM X-Force IRIS Incident Planning for pre-incident resiliency preparation. ^{REQ 18} Additionally, X-Force IRIS offers and tabletop exercises—enabling the teams to practice responses, and ensure they're prepared to quickly and effectively mitigate security events. ^{REQ 19}

Methodology

IBM starts design to identify and prioritize data sources for integration into the CRC Threat Intelligence Solution. We will set the prioritization criteria according to client's assessed value and integration ease. ^{REQ 20} For example, closed sources and partners with data governance restrictions will require additional time to execute signed agreements. ^{REQ 21} We expect data source owners to provide REST API documentation if other data access methods are needed then this may impact data source integration priority. CRC Stakeholders should at minimum be able to accept STIX format. ^{REQ 22} Data sources will be required to classify and highlight indicators of compromise and at minimum prepare the information for TAXII protocol dissemination.

Enterprise Intelligence Management

The CRC Threat Intelligence Solution contains enclaves, a structured data environment, for individual analysis and/or stakeholder investigations enriched with content shared by your partners and peers, while maintaining protective access controls. ^{REQ 23} Enclaves become the stronghold for threat information, analytic assessments, information requests and stakeholder activity. ^{REQ 24} After 3 months, the client can choose to either archive the data or extend this retention period. Standard data retention policy for our clients is normally 3 months. The data retention is limited by the volume of logs being collected and the storage space available. We are able to modify the retention period based on client needs, as long

as there is storage space available. Log retention policies can be modified based on compliance requirements, as long the log retention period doesn't exceed the available storage installed on the system. REQ 25

CRC Stakeholders access the CRC via web interface with TLS encryption or query via TLS encrypted API calls. AES-256 encrypted data at rest would not be co-mingled with other stakeholder sensitive data and not replace any cyber security operations of participating stakeholders. REQ 26 The platform is SOC 2 Type 2 Certified and uses role-based access controls to protect intelligence sharing, administer user roles and adjust for CRC interests. REQ 27

The platform provides ad-hoc manual and programmed data receipt through multiple ingestion methods and in both structured and unstructured data formats. The ingestion process normalizes, parses, and automatically extracts recognized observables such as an IP address, bitcoin wallet, or file hash. REQ 28 The platform correlates incoming reports and observables against all other user available data sources. In return, the data sources' relationships and context are presented back to user. The normalization process performs a defanging task automatically upon data ingestion. This defang task works to provide a safe manner for analysts to copy/paste or export observables from the source report. The platform also includes defanged observables in the indicators of compromise list and in an entity graph. The platform routinely deduplicates, parses, and enriches threat information upon data import regardless of data source as to not introduce overload or saturation. REQ 29

The platform provides existing, bi-directional integrations with JIRA, ServiceNow, Phantom, Demisto, and Resilient for case management. Additionally, a fully RESTful API and Python SDK may be leveraged for those case management tools. This extensibility is not invasive or disruptive to existing systems of participating stakeholders. REQ 30

Analysis-(Analysts)

Enterprise Intelligence Management (EIM) provides near real-time shared information and an integrated analytical workspace. REQ 31 EIM acts as a first level filter and correlation engine for users, collecting and refining data in an iterative feedback loop, reducing noise and surfacing relevant results quicker for analyst review through a programmatic approach to curating and distilling relevant findings. For example, EIM may assess surface web and deep/dark web data sources to help users in identifying assets at risk. This task uses keywords to seed continuous search queries to locate suspicious activity. If the specific user receives a suspicious activity notification, then the recipient should validate the notification per their runbook.

The proposed EIM provides analysts the capability to identify, separate and decipher source information from multiple sources within a single workbench. Analysts could

tag data sources for organization, searching and filtering. This would allow EIM to flag each source within consolidated submissions and supports analytic integrity through references. Analysts may also perform indicator-level tagging. The platform provides indicator and report level tagging for public (all community users have visibility) and private (specific to enclave and/or user). REQ 32

EIM leverages a strict analytic data model to achieve precision within the centralized knowledge base. This knowledge base accommodates machine learning algorithms or artificial intelligence integration. REQ 33

The EIM enclave activity dashboard shows what reports have been enriched, identify data sources with relevant IOCs and what IOCs, malware and vulnerabilities are trending. From this visualization, we assess partners, users and data sources for effectiveness, frequency of use and relative value to EIM. REQ 34

The platform provides intelligence sharing statistics and behavior via CSV format. The platform's design enables this data to be acquired from the cloud infrastructure.

Using the analyst's view, an analyst understands correlations to IOCs, partners, users or data sources using an entity graph. The top bar in the main pane highlights the correlations across a date range. Date last seen and date range information provides clues into threat activity fluctuations. We believe this visualization helps a user make sense of the increased quantity of likely new information.

An effective cyber threat intelligence (CTI) program likely uses the following focus areas to measure program maturity: intelligence scope, scope (security operations), CTI technology and technology integration metrics. The precise breakdown of threat intelligence work into concentration points allows us to identify a user's maturity level, set appropriate sharing expectations and provide feedback to improve CTI operations. For example, individual disciplines at each phase help users to assess EIM value within their organization and observe their CTI operations development.

The proposed EIM facilitates, manages and encourages user-shared intelligence through automated email distributions, direct submissions, interactive sessions and programmable methods. For example, the platform's data ingest method accepts

- Email listservs
- Direct submissions of IOCs
- Requests for Information
- Browser-based input via a Chrome Plug-In

Email listserv distribution. We expect to utilize an email handle for the client's EIM, and any emails sent to EIM email address are automatically added to EIM Enclave with the subject line as the report title and the date and report content properly populated. Users can also use this email handle to submit threat intel directly to EIM Enclave.

Requests for Information (RFI). The platform supports collaboration, RFIs and discussions forums through submissions, embedded chat functionality and threaded comments at the report level. For example, EIM users can easily submit an RFI within the platform and tag responses and related content.

Anonymous Threat Intelligence Sharing. Users may choose to submit information with anonymity. The platform's enclave enables anonymous information exchange. We found users started to deselect anonymity in favor of showing user name/ID. REQ 35

Traffic Light Protocol (TLP) classification system. The platform manages and enforces restrictions, such as the TLP classification. During initial setup, we use a tagging methodology within the platform and apply designators to reports and indicators. We expect the platform to scale and adapt to shifting information sharing guidelines. For example, an analyst could share threat intelligence across multiple enclaves based on the value or presence of a TLP tag. Users may make ad-hoc decisions or use rule-based logic to filter and act appropriately based on TLP classification. REQ 36

Alerts or notifications to users. The platform provides email notifications and alerts to EIM users. Configurable options include:

- Keyword edits and watchlist update frequency
- Daily or Weekly digests to highlight changes to watched indicators or reports
- In-platform notifications of new platform

The reports may be ingested from a data source, create within the platform or a manual upload. An individual report row displays the data enclave, IOC count, number of correlations and tags. These report row properties allow an analyst to visually inspect reports then decide on the most relevant report for their research. The analyst may also append feedback to a report to improve report relevance.

XML structured-based intelligence (e.g., STIX/TAXII, JSON). The platform communicates in a variety of structured intelligence format such as STIX and JSON. A majority of intelligence providers leverage APIs or TAXII services. REQ 37 Fifteen available threat intelligence feeds: Abuse.ch IP Blacklist, Abuse.ch Ransomware, Abuse.ch SSL Blacklist, AIS – DHS, Bambenek, EU-CERT, Hail_a_Taxii, Hybrid Analysis_Public Feed, Broad Analysis, Infosec Island, ISC, Malware Bytes, Packetstorm, Palo Alto Unit 42, and US-CERT.

Cyber Resilience Center Facility

The CRC facility will be located in a Harbor Department building located at 300 Water Street, Wilmington, CA 90744. REQ 38 The Facility build out will be completed by Data Specialties Inc.

Scope

Electrical:

1. It is assumed that the room has sufficient and existing electrical infrastructure and minimum availability of 99.9%, with fail-over and redundancy of critical components. REQ 39
2. Back Up Power Option 1: Provide desktop Uninterruptible Power Supply's (UPS), one for each critical device within the CRC. (Up to 10 Desktop UPS's).
3. Back UP Power Option 2: Provide (1) Complete UPS Back-Up System for the entire CRC. UPS will have to be located in a different room but within 50' of the CRC.
4. Back Up Power Option 3: Provide (1) Complete Redundant A/B UPS System, including UPS-A, UPS-B, and Back-Up generator. UPS-A and UPS-B will have to be located in a different room, but within 50' of the CRC and the generator located within 100' of the UPS's. It is assumed that the building Mechanical Systems shall have the capacity to support the cooling of this equipment. (The UPS and Emergency Generating System shall be sized for the load of the CRC with an additional 20% capacity. REQ 40

Mechanical:

Excluded and DSI assumes the room has adequate mechanical capacity per the RFP.

Cabling and Internet Service Provider (ISP):

1. (2) ISP's shall be provided by IBM
2. DSI shall take the handoff of the ISP at the site Demarcation Point (DMARC) and extend them into the CRC where they shall interconnect with the IBM provided network equipment.
3. DSI shall provide and install the necessary copper cabling to provide a fully functioning network between the desktop work stations and the video wall within the CRC. REQ 41

Fire Suppression:

1. Option 1: Existing fire suppression system shall be utilized; NO fire suppression scope of work is included.
2. Option 2: Provide a fully engineered Gaseous Fire Suppression System for the CRC Room.
 - a) Provide and install a Kidde Fire Systems Intelligent control unit with battery back-up
 - b) Provide and install manual pull stations
 - c) Provide and install abort switches
 - d) Provide and install maintenance by-pass switch
 - e) Provide and install multi-tone evacuation warning horn/strobe
 - f) Provide and install internal discharge warning strobes
 - g) Provide and install connected gaseous agent storage container with supervisory pressure switch.
 - h) Provide and install discharge nozzles
 - i) Provide and install gaseous extinguishing agent in storage container
3. Option 3: Provide a fully engineered Gaseous Fire Suppression System and complete VESDA Detection System for the CRC Room.

- a) Provide and install a Kidde Fire Systems Intelligent control unit with battery back-up
- b) Provide and install manual pull stations
- c) Provide and install abort switches
- d) Provide and install maintenance by-pass switch
- e) Provide and install multi-tone evacuation warning horn/strobe
- f) Provide and install internal discharge warning strobes
- g) Provide and install connected gaseous agent storage container with supervisory pressure switch.
- h) Provide and install discharge nozzles
- i) Provide and install gaseous extinguishing agent in storage container
- j) Provide and install Vesda power supply with battery back-up
- k) Provide and install Vesda Air Sampling Smoke Detectors with sampling points and piping.

Video Wall and Workstations

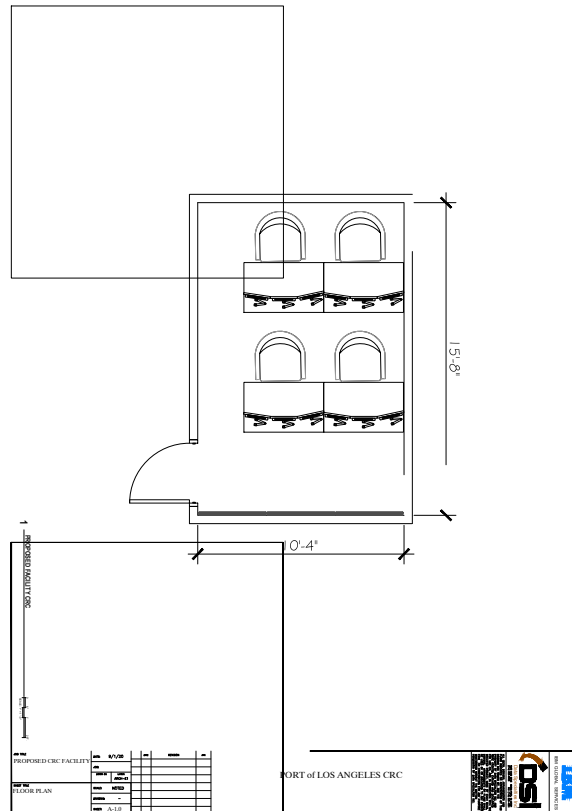
1. Cubicle and Workstation
 - a) The space is confining allowing for 3' deep consoles and 3' space for the operators facing the video wall.
 - b) The consoles will be Qty (2) 2-persons consoles. There is no requirement for typical features like adjustable monitor arms.
 - c) In this case the monitors will reside on the desktop; there is no storage space except for CPUs^{REQ 42}
2. Video Wall
 - a) The Video wall shall include the following:
 - b) Qty (6) 46" ultra-thin Mullion professional grade LED monitors
 - c) Digital video wall processor for connection to internet, TV,
 - d) Intranet, dedicated security computer
 - e) Monitor wall mounts, equipment cabinet
 - f) Five channel sound; type and location to be determined
 - g) Wireless keyboard & mouse
 - h) Digital distribution amplifiers over dual cat 5/6
 - i) Cables, wire and incidental.
 - j) Extended warranties, software support not included
 - k) The above console and video proposal is based on very limited information and for that reason there are assumptions made in order to offer an acceptable product. The 10'4" wall assigned to placement of the video wall does not provide adequate width for 3 end to end 46" displays that are typical for this type installation. For this reason, we suggest alternative 2x2 46" displays or 2x2 55" displays. ^{REQ 43}

Clarifications

1. Installation work will be completed during normal working hours, 6:00am to 2:30pm Monday-Friday.
2. Raised floors will be clean and free of debris.
3. Applicable tax and freight are included.
4. Lighting and wall mounted receptacles are to be provided by others.
5. It is assumed that the CRC room shall be sealed and able to maintain pressure for the fire suppression system.



6. All network equipment shall be provided by IBM, unless otherwise specified in the proposal.
7. It is assumed the CRC is built on a raised floor and there is adequate space for electrical and cabling within this space.
8. It is assumed that the raised floor is rated and capable of supporting the weight of the furniture, and equipment being installed upon it.
9. All Audio is excluded except for what is specified in the proposal.
10. Any work not included within this proposal is excluded from DSI's scope unless negotiated within another agreement.
11. DSI can't offer a firm, fixed price based on the current information provided to us. A final price would require a review of the existing infrastructure at the respective location. We can provide this budgetary information as well as the assurance that the core functionality requested in the bid documents is covered by this Proposal.
12. Secure badge access control to enter the CRC facility will be provided by the Harbor Department. REQ 44
13. Sketch of the proposed CRC facility layout



Disaster Recovery

The Facility will be build upon the physical CRC facility that was offered in the Request. This facility will be used as the on-site CRC work location for a cloud and managed Security services provider location. This facility will be used as the on-site CRC work location for a cloud and managed Security services provider location. REQ 45

CRC Installation

IBM will not start any project without the Notice-to-Proceed with the installation notice from the Executive Director of the Harbor Department. IBM will be responsible for Permits along with naming convention between the ports and wall plates with cable and connector information. IBM will integrated all the new new equipment and verify that it is operational. REQ 46

Data sharing agreements

The concept of sharing cyber threat information immediately begs the questions of what kind of information to share and how to share it. This policy guidance provides answers to these and related issues, such as what are the typical sources of threat information that an organization may wish to share; deciding on what information to share and when to share it; how such information might be categorized according to NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing and relevant models; and how to protect privacy when sharing information. REQ 47

The term “threat information” refers to any information related to a cyber threat that may help an organization identify an attacker’s activities or defend against a cyber threat. Threat information often refers to specific indicators (also called Indicators of Compromise (IOC)) such as IP addresses or phishing emails and may also include a broad range of cyber threat-related information, such as attacker’s behavior or “tactics, techniques, and procedures” (TTPs); security alerts such as advisories or bulletins; vulnerability notifications; or threat intelligence reports.

CRC Stakeholders are likely to possess a variety of threat information that can be used to support the information sharing community. Such data/information may originate from within an organization’s security tools as well as reside in suspicious emails sent to the Partner organization or its members. Typical security tools that contain threat information include firewalls, intrusion detection/prevention tools (IDS/IPS), anti-virus products, operating system artifacts and logs, browser history and caches, Security Information and Event Management (SIEM) tools, email systems, case management systems, and other system artifacts.

Systems and tools that are already in place and designed to gather threat information to assist decision-making regarding cyber threats—such as SIEMs—are likely to be a good starting point for automatically sharing information such as IOCs to other Partners. Threat information derived from incident response engagements conducted in response to potential cyber threats, such as TTPs and IOCs, is also likely to be useful. Finally, inbound emails that suggest an organization is being targeted for attack are likely to contain threat information of value.

Organizations are typically inundated with potential threat information derived from their internal security operations, many of which are likely to be classified as false positives. When deciding whether to share threat information, organizations should first apply an internal vetting process to determine that the indicator may pose harm

to an organization and therefore may also threaten other CRC Stakeholders. Once an organization has decided that there is a reasonable case to be made that the threat information e.g. an IOC may be malicious, the organization should consider sharing that information within the CRC.

After having made a decision that threat information may be of value to other CRC Stakeholders it should be shared as quickly as possible. This is especially important in the case of IOCs such as IP addresses, domain names, or file hashes which may have a very short lifespan. Attacker behavior or TTPs should also be shared quickly as such information could be particularly valuable to CRC Stakeholder' Incident Response teams who might be investigating a similar incident. REQ 48

CRC Stakeholder Onboarding

Stakeholder onboarding methodology is a 4 stage process to support new and continuing stakeholders.

- Stage 1: Knowledge Transfer. Our onboard team will conduct knowledge transfer meeting(s) to ensure a smooth transition from initial setup to the first day. The onboard team will designate a critical point-of-contact (POC) and work hand-in-hand with the stakeholder.
- Stage 2: The onboard team will perform a hand-off call with the stakeholder. A very detailed playbook will be reviewed outlining objectives, current infrastructure and integration requirements, data ingestion requirements, customer-specific workflow for documentation and reference, checklists, and more.
- Stage 3: The onboard team will walk through an Integration Checklist to make sure all integrations are identified and prepared for deployment.
- Stage 4: The onboard team works with the stakeholder to activate and extend training to other members of the stakeholder's organization. This process can be conducted in person for a single large group or can easily accommodate multiple smaller groups via video conferencing. REQ 49

Operations

IBM's assigned CRC staff will deliver according PoLA's service delivery model with a minimum of two analysts from 8:00 am to 5:00 pm, Monday to Friday, and automated alerts and notifications for after-hours on-call coverage and call-back if needed. This model will support PoLA's 24 hours a day 7 days a week need IBM may be required to travel to stakeholder and other locations. Travel expenses to be reimbursed shall be in accordance with City of Los Angeles travel policy. The CRC website(s) shall be hosted under designated domain(s) of the Port of Los Angeles. REQ 50

The staffing plan and coverage hours will address the requirements identified in the RFP:

- The CRC will be fully staffed with trained experts who are dedicated to watching the pane of glass, alerting and escalating to stakeholders.

- The lead person operating the CRC will possess and maintain a Certified Information Systems Security Professional (CISSP) certification.
- Alternate certifications/experience in lieu of the CISSP will be provided. Additional industry certifications (e.g. GCIH, GCIA, GMON, GICSP, GRID, etc.) that are relevant to the role will also be provided.
- All staff have excellent communication and customer service skills.
- All staff will meet security requirements, including criminal and drug background checks.
- All staff shall be subject to review and approval by the Harbor Department, at the proposal stage and during the term of the agreement if staffing changes are proposed by IBM. REQ 51

Data Sharing with Stakeholders

CRC Data shall be able to be displayed with existing dashboards desktops/laptops, tables and/or smartphones. The data shall be accessible to participating stakeholders at any time and from anywhere security with an internet connection. The CRC Shall Communicate to participating stakeholders in real-time. REQ 52

Warranty

Warranty, maintenance and support shall be provided for everything provided under the agreement, for the duration of the agreement. This shall include, but is not limited to, hardware, software, services, licenses, updates, and 3rd party items. REQ 53

Closeout

Ownership of the complete functioning CRC, and all that it entails shall be held by the Harbor department at the conclusion of the contract. The Harbor Department may have full ownership rights to continue to operate and develop the CRC with its own staff or another contractor. All data shall be given to the Harbor Department with no copies retained by the contractor. At the end of the contract all access/login credentials shall be given to the Harbor Department.

There shall be a transition at the end of the contract so there is no disruption in services. At the conclusion of the contract IBM will provide a final report that includes technical details at the time of the closeout and other pertinent documents.

REQ 54



RFP Requirements Matrix

REQUIREMENT	(Yes or No) If Yes, provide page #
1) GOVERNANCE	
1.1 The contractor shall establish a collaborative governance structure that includes an Executive Steering Committee and a Technical Committee (collectively “Governance Committees”). Both Governance Committees shall consist of select stakeholder representatives.	25
1.2 The contractor shall establish protocols for both Governance Committees, including roles, responsibilities, policies, procedures, communications, etc., for collaborative and effective governance.	26
1.3 The contractor shall assist with the facilitation of both Governance Committees for the duration of the agreement.	23
2) DESIGN	
2.1 General Design	
2.1.1 The contractor shall design the CRC solution in collaboration with participating stakeholders.	23
2.1.2 The CRC shall be a closed information solution. Data will be received from participating stakeholders and from external cyber intelligence sources. However, data will be distributed only to participating stakeholders. Data will not be distributed outside of the CRC.	34
2.1.3 The CRC platform shall enable Port of Los Angeles stakeholders to automatically and manually exchange cyber threat intelligence to increase the collective knowledge base of known threat actors, activity, and malware.	34
2.1.4 The CRC shall be compliant with relevant state, federal and international laws and regulations.	10
2.1.5 The CRC platform shall be based on, and compliant with the National Institute of Standards and Technology (“NIST”) Special Publication 800-150, Guide to Cyber Threat Information Sharing.	33
2.1.6 The CRC platform shall be capable of data sharing via an API, sensor and/or STIX/TAXII protocol.	34
2.1.7 The CRC will be a system of systems, and shall not replace any cyber security operations of participating stakeholders.	35
2.1.8 The CRC shall not be invasive or disruptive to existing systems of participating stakeholders.	35
2.1.9 The CRC shall not include stakeholder proprietary information.	35
2.1.10 The CRC shall not identify or expose stakeholder cyber vulnerabilities.	35
2.1.11 The CRC shall not be burdensome to stakeholder staff.	34
2.1.12 The CRC shall have a minimum availability of 99.9%, with fail-over and redundancy of critical components.	38



2.1.13 The CRC shall have a hot standby disaster recovery solution.	40
2.1.14 The CRC platform shall have tools and capabilities for authorization, authentication, and accounting.	35
2.1.15 Data at rest and in motion shall be encrypted with latest cryptographic standards.	35
2.1.16 The CRC solution shall be flexible and scalable to be able to meet future needs.	35
2.1.17 The CRC website(s) shall be hosted under designated domain(s) of the Port of Los Angeles.	42
2.1.18 Contractor may be required to travel to stakeholder and other locations. Travel expenses to be reimbursed shall be in accordance with City of Los Angeles travel policy, found in Section 1.8 of the City Controller’s Manual	42
2.2 Data Collection And Integration	
2.2.1 Data elements required to meet the CRC objectives shall be identified in collaboration with stakeholders.	34
2.2.2 The CRC shall receive, normalize, aggregate and integrate data received from different stakeholder sources and from external cyber intelligence sources. Data source platforms and formats are expected to be different.	35
2.2.3 The CRC shall be able to effectively ingest data from multiple sources without failure due to overload or saturation.	35
2.2.4 The CRC must be capable of storage of data allowing for a minimum of 90 days retrieval. Data retention time shall be configurable.	34
2.2.5 Data From Stakeholders:	
• Data elements that stakeholders agree to share shall be automatically transmitted from stakeholder systems to the CRC.	34
• A secure data collection portal shall be created and available for stakeholders to manually share additional data with the CRC.	34
• Data shall be transmitted from the source system to the CRC in real-time such that source data are available in the CRC at the same time as in the source system.	35
2.2.5 Data From Stakeholders:	
• Data elements that stakeholders agree to share shall be automatically transmitted from stakeholder systems to the CRC.	34
• A secure data collection portal shall be created and available for stakeholders to manually share additional data with the CRC.	34
• Data shall be transmitted from the source system to the CRC in real-time such that source data are available in the CRC at the same time as in the source system.	35
2.2.6 Data From External Threat Intelligence Sources:	



<ul style="list-style-type: none"> • In addition to stakeholder data, the CRC shall be able to receive data from multiple external cyber intelligence sources. 	37
<ul style="list-style-type: none"> • Contractor shall provide proposed intelligence consumption processes for the intake of external intelligence data for analysis, classification and integration into CRC operations. 	37
<ul style="list-style-type: none"> • Contractor’s proposal shall include up to ten recommended external threat intelligence sources. 	37
2.3 Analysis	
2.3.1 The CRC shall perform data analytics, data correlation, categorization and enrichment of threat indicators utilizing the latest security technologies.	35
2.3.2 The CRC should process data such that it may be used by participating stakeholders to help them classify, identify, and disseminate indicators of compromise and other selectors for blacklisting within firewalls, servers, appliances and tools.	35
2.3.3 The CRC shall include only data that is related to the maritime transportation industry, including secondary transportation sectors such as trucking and rail serving the Port of Los Angeles.	36
2.3.4 The CRC shall incorporate machine learning and artificial intelligence capabilities.	36
2.4 Data To Stakeholders	
2.4.1 The CRC data shall be distributed only to the participating stakeholders.	34
2.4.2 The CRC data shall provide actionable maritime cyber security information to stakeholders that may be used as an early detection and warning of cyber threats that may help to improve cyber defenses.	36
2.4.3 The CRC shall also be an information resource to assist with cyber information for incident recovery assistance, as may be appropriate to participating stakeholders.	34
2.4.4 Data shared with stakeholders shall not be automatically ingested by stakeholder systems. Each stakeholder will have the control to decide whether to use the CRC provided data, or not, as appropriate to their operations.	35
2.4.5 Data shared with stakeholders shall be anonymized so as not to disclose the stakeholder that originally provided the information.	37
2.4.6 The CRC shall not simply pass through irrelevant or redundant data that creates “noise” and burden for stakeholders.	35
2.5 Visualization	
2.5.1 At the CRC Facility	
<ul style="list-style-type: none"> • The CRC shall provide visibility into the cyber posture of the Port’s ecosystem. 	11
<ul style="list-style-type: none"> • The CRC shall include real-time graphical static & dynamic displays and dashboards that present threat data for situational awareness, including global trends and maritime business sector displays. 	11



<ul style="list-style-type: none"> • The contractor shall preconfigure a minimum of three dashboards for likely incident scenarios. 	32
<ul style="list-style-type: none"> • A Cyber Alert Indicator (similar to MS-ISAC Cyber Alert Level Indicator) for the Port of Los Angeles ecosystem shall be developed and displayed on the dashboard. The Cyber Alert Indicator shall show the current level of cyber risk in the PoLA ecosystem based on Traffic Light Protocol. 	32
<ul style="list-style-type: none"> • Contractor’s proposal shall include proposed examples of dashboard views. 	7
2.5.2 For Stakeholders	
<ul style="list-style-type: none"> • The CRC shall enable participating stakeholders to observe threat data in various dashboard models through a secure portal. Visualization for stakeholders shall include their own data and anonymized data that other stakeholders agree to share. 	32
<ul style="list-style-type: none"> • The CRC shall incorporate role-based access controls, and security into the design of the platform. The CRC shall have the capability to provide separate views for stakeholders and system administrators depending upon the data and their roles. 	32
<ul style="list-style-type: none"> • The CRC data shall be able to be displayed with existing stakeholder dashboards, desktops/laptops, tablets and/or smartphones. 	43
<ul style="list-style-type: none"> • The CRC data shall be accessible to participating stakeholders at any time and from anywhere securely with an internet connection. 	43
<ul style="list-style-type: none"> • The CRC shall communicate (e.g. alerts, notifications, updates, etc.) to participating stakeholders in real-time. 	43
<ul style="list-style-type: none"> • Contractor’s proposal shall include proposed examples of stakeholder views. 	54
2.6 CRC Facility	
2.6.1 Primary Facility Location	
<ul style="list-style-type: none"> • Contractor shall build a physical CRC facility that will be the location from which CRC operations will be conducted. 	37
<ul style="list-style-type: none"> • The CRC facility will be located in a Harbor Department building located at 300 Water Street, Wilmington, CA 90744. The dimensions of the room are 15 ft 8 in x 10 ft 4 in, with 9 feet high ceiling (See Attachment 4). The video monitors should be along the 10 ft 4 inch wall. 	37
<ul style="list-style-type: none"> • The CRC shall be completely independent from the Harbor Department’s Information Technology infrastructure. 	6
<ul style="list-style-type: none"> • The CRC facility shall include all necessary components including, but not limited to, the following: 	
<ul style="list-style-type: none"> • Furniture, hardware, software, supplies; 	39
<ul style="list-style-type: none"> • Four console work stations/consoles for CRC operations staff/analysts; 	39
<ul style="list-style-type: none"> • Two Internet Service Provider (ISP) connections, minimum 1 gbps per ISP; 	38
<ul style="list-style-type: none"> • Voice telephone lines, with redundancy, which function like a dispatch call center where incoming calls are sent to the same number; 	38
<ul style="list-style-type: none"> • Video wall, with minimum 6 monitors and a video wall controller; 	39
<ul style="list-style-type: none"> • Multimedia video and audio system; 	39
<ul style="list-style-type: none"> • Video teleconference system; 	39
<ul style="list-style-type: none"> • Smartboard and whiteboard; 	39
<ul style="list-style-type: none"> • Sufficient power supply; 	38



• Back-up power for critical components; and	38
• Other facility components to meet the CRC objectives.	37
• Secure badge access control to enter the CRC facility will be provided by the Harbor Department.	40
• Contractor’s proposal shall include a sketch of the proposed CRC facility layout.	40
• Contractor’s proposal shall include all proposed network diagrams (low level and high level), and technical related documentation.	30
2.6.2 Alternate Facility Location	
• The CRC shall be designed such that if the CRC Primary Location is not available, then an Alternate Location with an internet connection can be used to stand up the CRC and resume operations.	40
2.7 CRC Operations Manual	
2.7.1 The contractor shall prepare an organized and succinct Operations Manual that describes how the CRC will operate. The Operations Manual shall be based on a Cyber Resilience Framework to achieve the CRC objectives. This shall include, but is not limited to, the CRC sharing cyber threat indicators and defensive measures, and the CRC serving as an operations center where stakeholders can get information during an incident in the ecosystem.	12
2.7.2 The Operations Manual shall include, but is not limited to, CRC policies, procedures, roles, responsibilities, staffing levels, work shifts and contact information.	12
2.7.3 The Operations Manual shall include, but is not limited to, visuals of processes, data collection, integration and distribution flows.	12
2.7.4 The Operations Manual shall include, but is not limited to, visualization, descriptions, and uses of CRC facility dashboards.	12
2.7.5 The Operations Manual shall define and identify typical use cases and threat scenarios that may be submitted to the CRC, including how they should be handled.	12
2.7.6 The Operations Manual shall define minimum technical requirements for stakeholders to connect to the CRC.	12
2.7.7 The Operations Manual shall define how outages due to scheduled maintenance and other CRC disruptions will be handled, including protocols to notify stakeholders and back-up procedures.	12
3) DATA SHARING AGREEMENTS	
3.1 Based on the CRC Design, the Contractor shall develop and write a uniform data sharing agreement to be entered into by each CRC participating stakeholder.	41
3.2 The data sharing agreement shall be based on the National Institute of Standards and Technology (NIST) information sharing guidelines (NIST SP 800-150) or similar.	41
3.3 Data sharing agreements shall be reviewed and approved by the Harbor Department Executive Director.	33
3.4 The Contractor shall be responsible for obtaining each participating stakeholder’s approval to enter into the data sharing agreement.	42
4) CRC INSTALLATION	



4.1 Upon receiving a Notice-to-Proceed with the CRC installation from the Executive Director of the Harbor Department, the contractor shall procure and install the CRC facility per the Design within the location selected by the Harbor Department. Contractor shall not incur expenses for the installation (e.g. hardware, software, construction, etc.) until after a Notice-to-Proceed has been issued.	41
4.2 Contractor shall be responsible for required permits, if any.	41
4.3 In addition to the installation of the CRC Facility, the contractor shall also perform the following:	
• Run all necessary cables between components and properly label all ports and wall plates with cable and connector information;	41
• Integrate all new equipment with existing equipment and infrastructure, as applicable;	41
• Verify that all equipment is operational.	41
5) STAKEHOLDER ON-BOARDING	
5.1 Contractor shall on-board stakeholders in coordination with stakeholder availability and in accordance with the CRC Design (Section 2) and Data Sharing Agreements (Section 3).	42
5.2 Contractor shall be responsible for all technical aspects of connecting the stakeholder systems to the CRC platform.	42
5.3 Contractor shall provide training to stakeholders, including but not limited to, use of the CRC platform, use of dashboards, use of data and available reports. Training shall also include communications and interactions between stakeholders and CRC Operations.	42
5.4 Contractor shall develop on-boarding documentation and provide documentation to stakeholders. This documentation shall be detailed and organized such that it can later be used as a stakeholder operations manual or reference guide.	42
5.5 Contractor may be required to travel to stakeholder and other locations. Travel expenses to be reimbursed shall be in accordance with City of Los Angeles travel policy.	42
6) OPERATIONS	
6.1 The CRC shall be staffed and operated 24 hours per day, 7 days per week (24x7).	42
6.2 The contractor shall conduct operations in accordance with the CRC Operations Manual. The CRC Operations Manual shall be periodically reviewed and updated with new information and when changes are made.	12
6.3 The CRC shall achieve International Organization for Standardization/International Electrotechnical Commission 27001 (ISO 27001) certification within 6 months of going live and continue to maintain the certification for the duration of the contract.	43
6.4 Contractor shall provide feedback and recommendations for continuous improvement of the CRC.	43
6.5 Contractor staff that operate the CRC:	



6.5.1 The lead person operating the CRC must possess a Certified Information Systems Security Professional (CISSP) certification. Additional industry certifications (e.g. GCIH, GCIA, GMON, GICSP, GRID, etc.) that are relevant to the role are recommended.	43
6.5.2 Must have excellent communication and customer service skills.	43
6.5.3 Must meet security requirements, including criminal and drug background checks.	43
6.5.4 Shall be subject to review and approval by the Harbor Department, at the proposal stage and during the term of the agreement if staffing changes are proposed by the consultant.	43
6.6 Operations Tools	
6.6.1 An automated service management tool shall be used to manage and track inquiries and work orders.	10
6.6.2 Automated technical tool(s) shall be used to monitor and manage the CRC and connections to stakeholders to confirm proper operations. The tool(s) shall monitor the entire CRC environment and up to the demarcation point with the participating stakeholders.	10
6.7 On-Going Training	
6.7.1 Contractor shall provide annual refresher CRC training for all participating stakeholder staff that interface with the CRC. This annual training shall also include tabletop exercises.	34
6.7.2 Contractor shall provide annual general cyber security awareness training that participating stakeholders may use for their end users, as appropriate for their company's cyber program.	34
6.8 Reports	
6.8.1 CRC shall generate and distribute periodic reports for situational awareness and preventive operations.	10
6.8.2 CRC shall create and provide sanitized post-incident reports with lessons learned.	29
6.8.3 CRC shall provide ad-hoc reports as needed.	29
7) WARRANTY, MAINTENANCE AND SUPPORT	
7.1 Warranty, maintenance and support shall be provided for everything provided under the agreement, for the duration of the agreement. This shall include, but is not limited to, hardware, software, services, licenses, updates, and 3rd party items.	43
8) CLOSEOUT	
8.1 Ownership of the complete functioning CRC, including all intellectual property, software source code and documentation developed under this contract, shall be assigned by contractor to the Harbor Department at the conclusion of the contract.	43
8.2 The Harbor Department shall have full ownership rights to continue to operate and develop the CRC with its own staff or with another contractor.	43
8.3 All data shall be given to the Harbor Department. No copies of the data shall be retained by the contractor.	43
8.4 All CRC access/login credentials shall be given to the Harbor Department.	43



8.5 Contractor shall transition the CRC operations to the Harbor Department or designee so there is no disruption in services. This shall include knowledge transfer to the Harbor Department staff or a new contractor.	43
8.6 The contractor shall provide a final report that includes technical details at the time of closeout, including detailed configuration documents, security protocols, details of the developed API/STIX/TAXII protocols, process flow documents, data maps, details of analytical tools and displays, and general user documents.	43
9) SCHEDULE	
The Harbor Department’s desired schedule is presented below. However, proposers may include in their proposal an alternate schedule to achieve the CRC requirements.	
1. Governance, Design and Data Sharing Agreements: Within 4 months of contract award:	
o Executive Steering and Technical Committees shall be established and in operation.	53
o Design of the CRC completed.	53
o Data sharing agreements should be signed with the first group of participating stakeholders (up to 20). The initial group of stakeholders will be determined during project planning.	53
2. Installation And On-Boarding Of First Group Of Stakeholders (up to 20): Within 6 months after the Harbor Department issues the Notice-to-Proceed (NTP) for the CRC installation:	
o CRC should be installed.	53
o First group of participating stakeholders should be on-boarded.	53
3. On-Boarding 10 Additional Stakeholders (Total Of 30): Within 6 months after completion of Installation:	
o Data sharing agreements should be entered into with ten more stakeholders, for a total of thirty stakeholders on-boarded.	53
4. On-Boarding 10 Additional Stakeholders (Total Of 40): Within 12 months after completion of Installation:	
o Data sharing agreements should be established with ten more stakeholders, for a total of forty stakeholders on-boarded.	53
5. On-Boarding 10 Additional Stakeholders (Total Of 50): Within 18 months after completion of Installation:	
o Data sharing agreements should be established with ten more stakeholders, for a total of fifty stakeholders.	53
6. On-Boarding Additional Stakeholders (Total Of Up To 100): Until the end of the agreement:	
o Data sharing agreements should be established with additional stakeholders, for a total of up to one hundred stakeholders until the end of the agreement.	53
7. ISO 27001 Certification: Within 6 months after CRC is in operation:	
o CRC should achieve ISO 27001 certification. This certification shall be maintained for the duration of the agreement.	53
8. On-Going Operations, Maintenance, and Enhancements:	
o Shall be provided from the completion of the CRC Installation until the end of the agreement.	53

Project Management

IBM has precise Project Management model that it has used repeatedly for many years with much success. This process has been utilized by hundreds of clients. Initially there is a Project kick off meeting with all the essential stakeholders. Then we follow with regularly weekly scheduled meetings and written progress reports to identify issues/concerns. IBM utilizes previous management techniques to solve any risks and issues that may occur.

IBM's value proposition from our Project Management team:

- Completing projects more quickly and cheaply
- Being more predictable
- Saving effort and cost with proactive scope management
- Better solution "fit" the first time through better planning
- Resolving problems more quickly
- Resolving future risk before the problems occur
- Communicating and managing expectations with customers, team members and stakeholders more effectively
- Building a higher quality solution the first time
- Improved financial management
- Stopping "bad" projects more quickly
- More focus on metrics and fact-based decision making
- Improved work environment

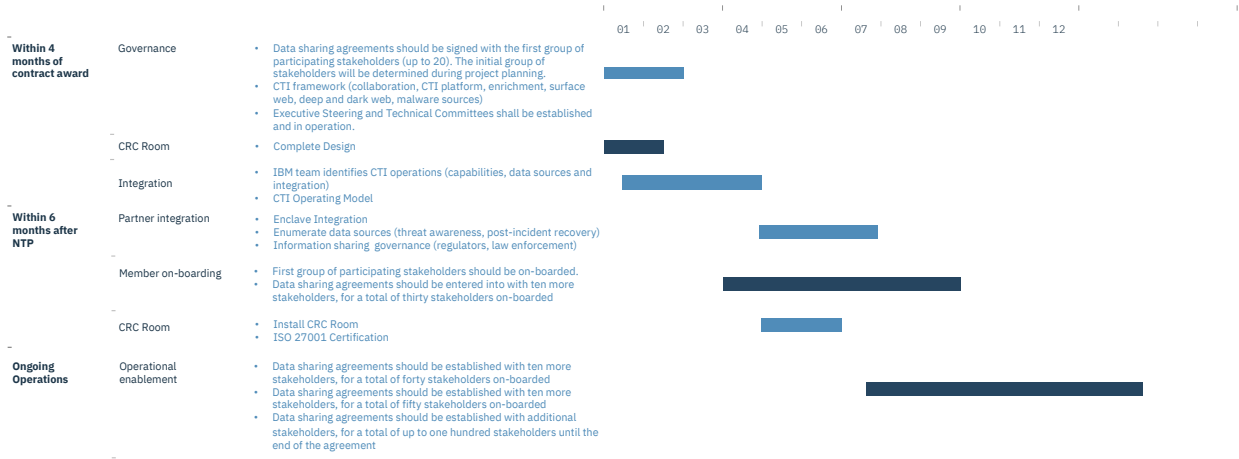
Typical Weekly Project Management responsibilities – (4 to 8 Hr plus hours for other tasks noted below)

1. Build project schedule, issues, risks and generally project controls (6 to 10 HR)
2. Schedule and Chair Weekly Project Meetings (1 to 3 Hr)
3. Publish Project Meeting minutes/notes (.5 to 1 Hr)
4. Weekly Status Report (1 to 2 Hr)
5. Review project financials/claims (.5 Hr)
6. Resource management (.5 Hr)
7. Attend weekly Governance meetings.(.5 Hr)
8. Ad hoc troubleshooting (0-20 Hr)



Schedule

CRC Schedule





Sample Reports

1. IRIS Intel Sample_Adversary_Malware Report
2. Sample Post_Incident Report
3. Stakeholder_Views
4. Content Sharing Agreement - Sample



Cost

[SEE EXHIBIT B]



[This Page Intentionally Left Blank]

EXHIBIT B

Cyber Resilience Center Pricing Table

Contractor must receive a written Notice-to-Proceed from the Executive Director, or designee,
before starting work or incurring expenses for any deliverable below.

Deliverable	Description	Qty	Unit	Unit Price	Total
1	50% Design deliverable document, Governance Stand-Up	1	lump sum	\$ 382,215.00	\$ 382,215.00
2	80% Design deliverable document	1	lump sum	\$ 229,328.00	\$ 229,328.00
3	100% Design deliverable document	1	lump sum	\$ 152,886.00	\$ 152,886.00
4	Finished Data Sharing Agreement (final, ready to be signed)	1	lump sum	\$ 94,440.00	\$ 94,440.00
5	Signed Data Sharing Agreements (groups of 10)	10	group of 10	\$ 11,018.00	\$ 110,180.00
	CRC Solution and Installation				
6A	- TruStar Software and Management	1	lump sum	\$ 1,100,000.00	\$ 1,100,000.00
6B	- Cloud Pak for Security (1000 Servers)	1	lump sum	\$ 105,223.00	\$ 105,223.00
6C	- Resilient (3 Users)	1	lump sum	\$ 62,452.00	\$ 62,452.00
6D	- Cloud Pak for Security Deployment	1	lump sum	\$ 99,600.00	\$ 99,600.00
6E	- CRC Physical Buildout - Deliver hardware for CRC Solution	1	lump sum	\$ 335,000.00	\$ 335,000.00
6F	- CRC Physical Buildout - Completed CRC Solution and Installation	1	lump sum	\$ 455,000.00	\$ 455,000.00
6G	- On-Board Stakeholders (up to 100 on-boarded over 3 years)	10	group of 10	\$ 11,018.00	\$ 110,180.00
7	Operations - staffing, subscriptions, warranties, maintenance, support, on-going governance and other operations costs to meet CRC requirements. On-site staffing of a minimum of two analysts from 8:00 am to 5:00 pm, Monday to Friday, and automated alerts and notifications for after-hours on-call coverage and call-back if needed.	26	month	\$ 100,074.15	\$ 2,601,928.00
8	ISO 27001 certification	1	lump sum	\$ 25,000.00	\$ 25,000.00
9	ISO 27001 surveillance audit	1	lump sum	\$ 15,000.00	\$ 15,000.00
10	Contingency - for new requirements that are beyond the original scope and are required to meet the objectives of the CRC.	TBD	TBD	TBD	\$ 921,568.00

TOTAL: \$ 6,800,000.00

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

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

AFFIRMATIVE ACTION PROGRAM PROVISIONS

Sec. 10.8.4 Affirmative Action Program Provisions.

Every non-construction contract with or on behalf of the City of Los Angeles for which the consideration is \$100,000 or more and every construction contract with or on behalf of the City of Los Angeles for which the consideration is \$5,000 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 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, religion, ancestry, national origin, sex, sexual orientation, age, disability, marital status, domestic partner status, or medical condition.
 - 1. This provision 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 will, 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, religion, ancestry, national origin, sex, sexual orientation, age, disability, marital status, domestic partner status, or medical condition.

- C. As part of the City's supplier registration process, and/or at the request of the awarding authority or the Office of Contract Compliance, 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, religion, ancestry, national origin, 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 Office of Contract Compliance, for the purpose of investigation to ascertain compliance with the Affirmative Action Program provisions of City contracts, and on their or either of their request to provide evidence that it has or will comply therewith.

AFFIRMATIVE ACTION PROGRAM PROVISIONS

- 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 contract. Such 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 Board of Public Works, Office of Contract Compliance. No such 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, such breach may be the basis for a determination by the awarding authority or the Board of Public Works that the said contractor is an irresponsible bidder or proposer pursuant to the provisions of Section 371 of the Los Angeles City Charter. In the event of such determination, such 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 (\$10.00) for each person for each calendar day on which such 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 Office of Contract Compliance 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. The Contractor shall submit an Affirmative Action Plan which shall meet the requirements of this chapter at the time it submits its bid or proposal or at the time it

AFFIRMATIVE ACTION PROGRAM PROVISIONS

registers to do business with the City. The plan shall be subject to approval by the Office of Contract Compliance prior to award 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 Plan. Affirmative Action Programs developed pursuant to this section shall be effective for a period of twelve

months from the date of approval by the Office of Contract Compliance. In case of prior submission of a plan, the contractor may submit documentation that it has an Affirmative Action Plan approved by the Office of Contract Compliance within the previous twelve months. If the approval is 30 days or less from expiration, the contractor must submit a new Plan to the Office of Contract Compliance and that Plan must be approved before the contract is awarded.

1. Every contract of \$5,000 or more which may provide construction, demolition, renovation, conservation or major maintenance of any kind shall in addition comply with the requirements of Section 10.13 of the Los Angeles Administrative Code.
 2. A contractor may establish and adopt as its own Affirmative Action Plan, by affixing his or her signature thereto, an Affirmative Action Plan prepared and furnished by the Office of Contract Compliance, or it may prepare and submit its own Plan for approval.
- L. The Office of Contract Compliance shall annually supply the awarding authorities of the City with a list of contractors and suppliers who have developed Affirmative Action Programs. For each contractor and supplier the Office of Contract Compliance shall state the date the approval expires. The Office of Contract Compliance shall not withdraw its approval for any Affirmative Action Plan or change the Affirmative Action Plan after the date of contract award for the entire contract term without the mutual agreement of the awarding authority and the contractor.
- M. The Affirmative Action Plan required to be submitted hereunder and the pre-registration, pre-bid, pre-proposal or pre-award conference which may be required by the Board of Public Works, Office of Contract Compliance or 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;

AFFIRMATIVE ACTION PROGRAM PROVISIONS

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.
- N. Any adjustments which may be made in the contractor's or supplier's workforce to achieve the requirements of the City's Affirmative Action Contract Compliance Program in purchasing and construction shall be accomplished by either an increase in the size of the workforce or replacement of those employees who leave the workforce by reason of resignation, retirement or death and not by termination, layoff, demotion or change in grade.
- O. Affirmative Action Agreements resulting from the proposed Affirmative Action Plan or the pre-registration, pre-bid, pre-proposal or pre-award conferences shall not be confidential and may be publicized by the contractor at his or her discretion. Approved Affirmative Action Agreements become the property of the City and may be used at the discretion of the City in its Contract Compliance Affirmative Action Program.
- P. 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 or suppliers engaged in the performance of City contracts.
- Q. All contractors subject to the provisions of this section shall include a like 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 E
SMALL/VERY SMALL BUSINESS ENTERPRISE PROGRAM
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 __% VSBE participation.** The North American Industry Classification System (NAICS) Code for the scope of services is **541512**. 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 \$_ 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

International Business Machines Corporation (IBM)

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.

EXHIBIT E

(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: Alana Muntz

Title: Client Executive

Printed Name: Alana Muntz

Date Signed: August 25, 2020

Consultant Description Form

PRIME CONSULTANT:

Contract Title: CYBER RESILIENCE CENTER

Business Name: International Business Machines Corporation LABAVN ID#: 19876

Award Total: \$ _____

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: _____

Address: 600 Anton Blvd.

City/State/Zip: Costa Mesa, CA 92626

County: Orange

Telephone: (310) 882-0695 FAX: () n/a

Contact Person/Title: Alana Muntz

Email Address: alana.muntz@ibm.com

SUBCONSULTANT:

Business Name: Data Specialties, INC LABAVN ID#: 99825

Award Total: (% or \$): _____

Services to be provided: Construction Services

Owner's Ethnicity: White Gender Male Group: SBE VSBE MBE WBE DVBE OBE (Circle all that apply)

Local Business Enterprise: YES NO _____ (Check only one)

Primary NAICS Code: 236220

Address: 8400 Kass Drive

City/State/Zip: Buena Park / CA / 90621

County: Orange County

Telephone: (714) 523-8489 FAX: (714) 523-1861

Contact Person/Title: Jon McSweeney

Email Address: jon@webulddatacenters.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: _____

Address: _____

City/State/Zip: _____

County: _____

Telephone: () _____ FAX: () _____

Contact Person/Title: _____

Email address: _____

EXHIBIT E

Consultant Description Form

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

Data Specialties 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: Sharon Tye
Printed Name: Sharon Tye

Title: Data Center Consultant
Date Signed: 08.28.2020

EXHIBIT F

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.