ORIGINAL

HEXAGON
SAFETY & INFRASTRUCTURE

PRINCIPAL CONTRACTING DOCUMENT

This Principal Contracting Document together with the Master Terms referenced below constitutes a Master Agreement ("Master Agreement") by and between **CITY OF SAN DIEGO**, a municipal corporation referred to herein interchangeably as "Customer" or "City") and **INTERGRAPH CORPORATION, a Delaware Corporation and doing business as HEXAGON SAFETY & INFRASTRUCTURE** ("Intergraph" or "Hexagon") and is binding upon the Parties on the Effective Date.

1. This Principal Contracting Document incorporates by reference the Master Agreement Terms and Conditions ("Master Terms") attached hereto as Attachment I, including Exhibits A though J, Attachment II - Pledge of Compliance, and Attachment III - Workforce Report.

2. All capitalized terms in this Principal Contracting Document shall have the same meaning as provided in the Master Terms except as may be otherwise defined herein.

3. Term. The Term of the Master Agreement shall be for an initial term of 3 (three) years beginning on the Effective Date and remain in effect until three years after the Effective Date or until the Master Agreement is earlier terminated pursuant to the terms set forth herein or by mutual agreement of the Parties. Customer may, in its sole discretion, extend this Master Agreement for 2 (two) additional 1 (one) year period(s). The term of this Master Agreement shall not exceed five years unless approved by the San Diego City Council by ordinance. To the extent it is reasonably foreseeable that an Order will be completed after the Term of this Master Agreement, then the Parties shall reasonably work together to amend the Term of the Master Agreement to ensure the Order is completed within the Term, as amended.

4. Amount of Compensation. City shall pay Hexagon for goods and performance of all services rendered in accordance with this Master Agreement in an amount not to exceed $5,878,244.48. Any increase in the not to exceed amount will require approval by the San Diego City Council by ordinance.

5. Forms Required to be Submitted by Hexagon to the Customer. Hexagon is required to submit all forms and information delineated in Attachments 2 and 3 to the Customer before this Principal Contracting Document is executed.

6. Any notice to be given pursuant to Section 13 of the Master Terms shall be directed to each Party at the following address, which reflects the Customer's location, in accordance with the Master Terms.

CUSTOMER:	HEXAGON:
Chris Haley	Attn: Safety & Infrastructure Legal Department
San Diego Police Department	305 Intergraph Way
1401 Broadway, MS 739	Madison, Alabama 35758
San Diego, CA 92101	victor.vasile@hexagonsi.com
chaley@pd.sandiego.gov	(256) 730-2000
(619) 531-2413	

DOCUMENT NO. RR-313223
FILED SEP 29 2020
OFFICE OF THE CITY CLERK
SAN DIEGO, CALIFORNIA

7. City's Mandatory Provisions

7.1 Contractor Certification of Compliance. By signing this Master Agreement, Hexagon certifies that Hexagon is aware of, and will comply with, these City-mandated clauses throughout the duration of the Master Agreement.

7.1.1 Drug-Free Workplace Certification. Hexagon shall comply with City's Drug Free Workplace requirements set forth in Council Policy 100-17, which is incorporated into the Contract by this reference.

7.1.2 Contractor Certification for Americans with Disabilities Act (ADA) and State Access Laws and Regulations: Hexagon shall comply with all accessibility requirements under the ADA and under Title 24 of the California Code of Regulations (Title 24). When a conflict exists between the ADA and Title 24, Hexagon shall comply with the most restrictive requirement (i.e., that which provides the most access). Hexagon also shall comply with the City's ADA Compliance/City Hexagons requirements as set forth in Council Policy 100-04, which is incorporated into this Master Agreement by reference. Hexagon warrants and certifies compliance with all federal and state access laws and regulations and further certifies that any subcontract agreement for this contract contains language which indicates the subcontractor's agreement to abide by the provisions of the City's Council Policy and any applicable access laws and regulations.

7.1.3 Non-Discrimination Requirements.

7.1.3.1 Compliance with City's Equal Opportunity Contracting Program (EOCP). Hexagon shall comply with City's EOCP Requirements. Hexagon shall not discriminate against any employee or applicant for employment on any basis prohibited by law. Hexagon shall provide equal opportunity in all employment practices. Hexagon shall ensure that their subcontractors comply with this program. Nothing in this Section shall be interpreted to hold Hexagon liable for any discriminatory practice of its subcontractors.

7.1.3.2 Non-Discrimination Ordinance. Hexagon shall not discriminate on the basis of race, gender, gender expression, gender identity, religion, national origin, ethnicity, sexual orientation, age, or disability in the solicitation, selection, hiring or treatment of subcontractors, vendors or suppliers. Hexagon shall provide equal opportunity for subcontractors to participate in subcontracting opportunities. Hexagon understands and agrees that violation of this clause shall be considered a material breach of the Master Agreement and may result in contract termination, debarment, or other sanctions. Hexagon shall ensure that this language is included in contracts between Hexagon and any subcontractors, vendors and suppliers.

7.1.3.3 Compliance Investigations. Upon City's request, Hexagon agrees to provide to City, within sixty calendar days, a truthful and complete list of the names of all subcontractors, vendors, and suppliers that Hexagon has used in the past five years on any of its contracts that were undertaken within San Diego County, including the total dollar amount paid by Hexagon for each subcontract or supply contract. Hexagon further agrees to fully cooperate in any investigation conducted by City pursuant to City's Nondiscrimination in Contracting Ordinance. Hexagon understands and agrees that violation of this clause shall be considered a material breach of the Contract and may result in contract termination, debarment, and other sanctions.

7.1.4 Contractor Standards. Hexagon shall comply with Contractor Standards provisions codified in the San Diego Municipal Code. Hexagon understands and agrees that violation of Contractor Standards may be considered a material breach of the Contract and may result in Contract termination, debarment, and other sanctions.

7.1.5 Product Endorsement. Hexagon shall comply with Council Policy 000-41 which requires that other than listing the City as a client and other limited endorsements, any advertisements, social media, promotions or other marketing referring to the City as a user of a product or service will require prior written approval of the Mayor or designee. Use of the City Seal or City logos requires City approval.

7.1.6 Business Tax Certificate. Unless the City Treasurer determines in writing that a contractor is exempt from the payment of business tax, any contractor doing business with the City of San Diego is

10. Records Retention and Examination. Hexagon shall retain, protect, and maintain in an accessible location all records and documents, including paper, electronic, and computer records, relating to this Master Agreement for five (5) years after receipt of final payment by City under this Master Agreement. Hexagon shall make all such records and documents available for inspection, copying, or other reproduction, and auditing by authorized representatives of City, including the Purchasing Agent or designee. Hexagon shall make available all requested data and records via email or where the records ordinarily are kept, and as often as City deems necessary, but in no event more than two times per year. If records are not made available via email or within the City or County of San Diego, Hexagon shall pay City's travel costs to the location where the records are maintained and shall pay for all related travel expenses. Failure to make requested records available for inspection, copying, or other reproduction, or auditing by the date requested may result in termination of the Master Agreement. Hexagon must include this provision in all subcontracts made in connection with this Master Agreement.

10.1 Hexagon shall maintain records of all subcontracts entered into with all firms, all project invoices received from Subcontractors and Suppliers, all purchases of materials and services from Suppliers, and all joint venture participation. Records shall show name, telephone number including area code, and business address of each Subcontractor and Supplier, and joint venture partner, and the total amount actually paid to each firm. Project relevant records, regardless of tier, may be periodically reviewed by the City.

11. Quality Assurance Meetings. Upon City's request Hexagon's Account Management team shall schedule quarterly quality assurance meetings with City's Contract Administrator to discuss Hexagon's performance. If requested, Hexagon's Account Management Team shall schedule the first quality assurance meeting no later than eight (8) weeks from the date of commencement of work under the Master Agreement. At the quality assurance meeting(s), City's Contract Administrator will provide Hexagon's Account Management team with feedback, will note any deficiencies in Contract performance, and provide Hexagon with an opportunity to address and correct such deficiencies. The total number of quality assurance meetings that may be required by City will depend upon Hexagon's performance.

12. Hexagon Employees and Contractors.

12.1 Except as formally approved by the City, the individual serving as Resident Systems Administrator ("RSA") shall not be changed. Changes in staffing must be proposed in writing to the City and approved, subject to ordinary personnel resignations, terminations, and illnesses. Proposed replacement personnel must be similarly qualified (absent the knowledge gained by the RSA in working with the City) to the personnel they are replacing.

12.2 The City of San Diego Police Department may conduct background investigations for any individual that may require access to Police facilities (this includes direct or remote access to any of San Diego Police Department's information technology systems), excluding a polygraph examination and credit check. The Background Authorization Forms must be signed by each individual. Fingerprint cards completed by the individual's local law enforcement agency that are acceptable to California DOJ must be provided to the City. The City will be responsible for direct costs associated with the background investigations. City has final decision as to who is allowed access to police facilities.

12.3 Hexagon shall provide any individual assigned to the City of San Diego, a company photo identification badge, which must be worn at all times while on the City of San Diego property. The cost of the photo identification shall be borne by Hexagon. Hexagon employees who successfully complete the City's background process to provide ongoing onsite maintenance support of the system, shall be provided and wear a City identification card within City buildings and work sites.

12.4 The City of San Diego may request Hexagon to immediately remove from assignment to the City of San Diego any employee found unfit to perform duties at the discretion of the City of San Diego. Upon receiving notice from the City that a Hexagon employee is deemed by the City to be unfit to perform such duties, Hexagon will remove the employee from the project.

13. In consideration of the mutual obligations assumed under this Principal Contracting Document, Customer and Hexagon agree to the terms and conditions set forth herein and represent that this Principal Contracting Document has been executed by each Party's duly authorized representative. The signatories represent that they have the authority to bind their respective organizations to this Principal Contracting Document. This Principal Contracting Document may be executed in counterparts or in duplicate originals. Each counterpart or each duplicate shall be deemed an original copy of this Principal Contracting Document signed by each Party for all purposes.

AGREED TO BY:

CITY OF SAN DIEGO
A Municipal Corporation

By: _____
Name: Christiana Gauger
Title: Interim Director
Purchasing and Contracting
Date: 10/6/2020

INTERGRAPH CORPORATION

By: Debra T Huser
Name: Debra T Huser
Title: Finance Director
Date: 08.13.2020

Approved as to form this 13 day of
OCTOBER, 2020.
MARA W. ELLIOTT, City Attorney

By: _____
Deputy City Attorney

Print Name: PAIGE E. FOLKMAN

R- 313223

HEXAGON
SAFETY & INFRASTRUCTURE

MASTER TERMS AND CONDITIONS

These Master Terms and Conditions (the "Master Terms") govern transactions and relations between Customer and Intergraph Corporation doing business as Hexagon Safety & Infrastructure ("Hexagon") (each a "Party" and collectively the "Parties").

Hexagon will make available to Customer and Customer's support vendor (currently Enforcement Support Service) certain proprietary software, including related proprietary documentation, software maintenance services, and professional services, all of which will be provided to Customer pursuant to these Master Terms and an Order. Before Hexagon will provide any Software licenses or any Services, Customer must agree to these Master Terms and to the terms of a corresponding Order. The Parties agree these Master Terms will govern each Order.

These Master Terms consist of the following:

- The General Terms and Conditions set forth below
- Exhibit A – End-User License Agreement
- Exhibit B – Support Terms and Conditions for Software
- Exhibit C – Project Deliverable Sign-Off Form
- Exhibit D – DELETED
- Exhibit E – Subscription Terms and Conditions
- Exhibit F – Common Terms Glossary
- Exhibit G – Criminal Justice Information Security Standards and Guidelines
- Exhibit H – City of San Diego Information Security Standards and Guidelines
- Exhibit I – DELETED.
- Exhibit J – Product Usage Terms
- Schedule 1 – List of Software (as of the Effective Date)
- Schedule 2 – Pricing for Maintenance Services for Covered Products listed in Schedule 1 and RSA Services

GENERAL TERMS AND CONDITIONS

1 Definitions. All capitalized terms not otherwise defined herein shall have the meaning set forth in Exhibit F (Common Terms Glossary).

2 Elements of an Order.

2.1 Order Composition.

2.1.1 Each Order will be comprised of Order Documents.

2.1.2 From time to time, Customer may request from Hexagon or Hexagon may provide Customer a draft Quote and/or SOW for Deliverables. Once the Parties mutually agree upon the contents of the Order Documents, as applicable, the Parties shall accept the Order Documents.

2.1.3 Upon mutual acceptance of the Order Documents, Customer will execute the Order Documents and/or issue a PO or a notice to commence work, unless otherwise specified in the Order Documents. Except as set forth in the Order Documents, Hexagon shall not commence work on the Order until it receives from Customer a PO or notice to commence work.

2.1.4 Notwithstanding the foregoing, Orders for Maintenance Services shall commence on the date specified in the Order Documents regardless of whether Customer has issued a PO or notice to commence work.

2.2 Pricing. The following minimum elements shall be included with the Order Documents associated with the following types of Orders:

2.2.1 For a Software License Sale, a Quote identifying the Software licenses and quantities being procured and the total price for the Software License Sale.

2.2.2 For Time and Materials Project Assignments, a Quote setting forth the number of hours allocated for each grade of Hexagon resource to be utilized on the assignment and the hourly rate for

each grade of Hexagon. Unless otherwise specified in the Order Documents, the Time and Materials Project Assignment shall expire and end six (6) months from the date the Order was formed between the Parties.

2.2.3 For Fixed Price Project Assignments, a Quote and SOW shall set forth the price of the work to be performed for and the Deliverables provided for that Order.

2.2.4 For Orders for Maintenance Services, a Quote identifying the Software to be maintained and the total price for the associated Maintenance Services.

2.2.5 DELETED.

2.2.6 For Subscription License Sales, a Quote identifying the name of the Subscription Licenses, the quantity of the Subscription Licenses being purchased, and the Subscription Term.

2.3 Change Control. During the course of Hexagon's performance under an Order, either Party may request a change in the scope of the Order in writing, delivered to the other Party's project manager. Any changes in price, schedule, or other terms must be documented either by an amendment or Change Order. No change, as contemplated in this paragraph, shall become effective until agreed to by both Parties in a mutually-executed writing.

2.4 Acceptance. Acceptance will occur based upon the following:

2.4.1 For Fixed Price Project Assignments, when the applicable Task Acceptance Criteria has been satisfied in accordance with the Task Acceptance Process as set forth in an SOW.

2.4.2 For Time and Materials Project Assignments, the services are accepted as performed.

2.4.3 For a Software License Sale, once the Software has been electronically delivered.

2.4.4 DELETED

2.4.5 For a Subscription License Sale, once the applicable Subscription License(s) has been delivered or access to the Subscription License has been provided to the Customer.

3 Composition of the Master Agreement.

3.1 Components. The agreement between the Parties (herein referred to as the "Master Agreement") consists of: (1) the Principal Contracting Document, (2) these Master Terms (including the General Terms and Conditions and all Exhibits), (3) any amendments to the Master Agreement, (4) Orders, together with any Change Orders, that may be delivered, prepared, or issued after the Effective Date, and (5) all documents, incorporated by reference in the documents identified in this Section. For certain Third Party Software, additional terms and conditions provided with the Order Documents ("Third Party Terms") will also be applicable and be considered as part of the Master Agreement.

3.2 Order of Precedence. In the event of any conflict or inconsistency among documents forming the Master Agreement, the following order of precedence shall be used to determine the resolution of the discrepancy. Provisions of the Master Agreement addressing the same subject which are consistent but have different degrees of specificity shall not be considered to be in conflict, and the more specific language shall control, unless the Parties mutually agree in writing to an alternative decision.

(1) Any amendments to the Master Agreement;

(2) The Principal Contracting Document;

(3) These Master Terms (excluding exhibits);

(3) Exhibits to these Master Terms; and

(4) Orders, as amended or modified by a Change Order.

For only the Third Party Software subject to the Third Party Terms, the Third Party Terms shall have precedence in the event of a conflict between with the Master Terms and the Third Party Terms.

4 Invoicing and Payment.

4.1 Invoices. Invoices shall be issued based upon the following:

4.1.1 For Software License Sales, Hexagon shall invoice Customer for the amount set forth in the Quote upon electronic delivery of the Software identified in the Order Documents.

4.1.2 Orders for Fixed Price Project Assignments shall be invoiced and become payable upon completion of the Task Acceptance Process related to a payment milestone identified in the SOW.

4.1.3 Time and Materials Project Assignments shall be billed and invoiced on a monthly basis as the hours are expended and Onsite Fees are incurred, or after all hours set forth in the Order Documents have been expended, whichever occurs first.

4.1.4 Orders for Maintenance Services shall be billed and invoiced in accordance with Exhibit B.

4.1.5 DELETED

4.1.6 Orders for Subscription License Sales shall be billed and invoiced in accordance with Exhibit E.

4.2 Payment. Customer shall make payment for any invoices issued by Hexagon within thirty (30) calendar days of the date the invoice was issued.

4.3 Late Payment. If Customer does not make payment within sixty (60) days after the invoice was issued, an interest charge of one percent (1%) per Month (or the maximum allowed by law, whichever is less), which shall be compounded on a monthly basis, will be due on any unpaid and overdue amounts. To the extent the Customer is the subject of an applicable prompt pay act statute or ordinance, the Customer shall be subject to the terms set forth in that statute(s) and/or ordinance(s) in lieu of the prior sentence.

4.4 Taxes. The purchase price is exclusive of all Federal, State, or Local taxes. The City will furnish Exemption Certificates for Federal Excise. The City represents maintenance services are not taxable and taxes on Maintenance Services should not be included to the net amount invoiced unless applicable law otherwise requires. Applicable taxes may be invoiced at any time such taxes become fixed and certain.

5 Termination.

5.1 Termination for Convenience. Except for Orders for Maintenance Services and Subscription License Sales, Customer may terminate the Master Agreement or an Order in its sole discretion at any time upon providing Hexagon with at least thirty (30) days written notice, and Hexagon may terminate: (i) the Master Agreement in its sole discretion at any time upon providing the City with one (1) year written notice or (ii) an Order in its sole discretion upon providing the City with ninety (90) days written notice. The Coverage Period or Subscription Term, (if applicable) shall survive termination if the Master Agreement is terminated for convenience. In the event of a termination pursuant to this paragraph, an equitable adjustment in the Master Agreement price shall be made and Customer agrees to pay Hexagon for Auditable Costs, plus the Auditable Cost of any labor, equipment, or materials ordered in good faith prior to notice of termination that could not be canceled, less amounts previously paid by Customer for such Work and/or Software. No amount shall be allowed for anticipated profit on unperformed services. To the extent a Party exercises its right to terminate a specific Order, that termination shall have no effect upon the remaining Master Agreement, which, along with any other active Orders, shall remain in full force and effect. If a Party desires to terminate the Master Agreement, Hexagon will continue to provide services (only if pursuant to an active Order or other transaction for such work) and the Parties shall proceed as provided in Section 5.4.

5.2 Termination for Cause. Either Party may terminate the Master Agreement or a specific Order, as the case may be, including Orders for Maintenance Services and Subscription License Sale, in the event that other Party materially breaches a material term of the Master Agreement or any Order.

5.2.1 In the event a Party has materially breached an Order, the non-breaching Party may terminate the Order only after providing a sixty (60) calendar day cure period to cure such breach and the breach has not been cured, except for material breaches arising from non-payment. During the sixty (60) day cure period, the Parties shall try to determine a mutually agreeable plan to cure such breach. If such breach cannot be cured or an acceptable plan is not provided within the sixty (60) day cure period, the non-breaching Party may, but does not have the obligation to, terminate the Order.

5.2.2 In the event a Party has materially breached the Master Agreement or multiple Orders, the non-breaching Party may terminate the Master Agreement or those Orders which a Party has materially breached, only after providing a sixty (60) calendar day cure period to cure such breach and the breach has not been cured except for material breaches arising from non-payment. During the sixty (60) day cure period, the Parties shall try to determine a mutually agreeable plan to cure such breach. If such breach cannot be cured or an acceptable plan is not provided within the sixty (60) day cure period, the non-breaching Party may, but does not have the obligation to, terminate the Master Agreement. If the Master Agreement is terminated pursuant to this paragraph, by the termination date, Hexagon will stop all Work pursuant to any Orders arising under the Master Agreement. Hexagon shall also continue to perform on other Orders not terminated, In the event the Master Agreement is terminated for cause, an equitable adjustment in the Master Agreement price shall be made based upon Auditable Costs, and Customer agrees to pay Hexagon, for the Work performed and Software provided, that are not the subject of the breach, on all ongoing Orders up to the termination date, less amounts previously paid by Customer under the affected Orders and less amounts related to the cause of the breach. No amount shall be allowed for anticipated profit on unperformed services. By accepting payment, Hexagon

discharges City of all of City's payment obligations and liabilities under this Master Agreement with regard to the affected performance.

5.2.3 If City terminates this Master Agreement, in whole or in part, for cause, City may procure, upon such terms and in such manner as the Purchasing Agent may deem appropriate, equivalent goods or services. If, after notice of termination, it is determined that Hexagon had not so failed, the termination shall be deemed to have been affected for the convenience of the City of San Diego pursuant to Section 5.1. In such event, adjustment in the Master Agreement price shall be made as provided in Section 5.1.

5.2.4 Notwithstanding the foregoing, Customer may not exercise a termination pursuant to the terms of Section 5.3 if Hexagon's material breach of the terms and conditions of the Master Agreement or any Order thereunder is proximately caused by Customer's negligence or failure to perform its obligations.

5.3 Rights and Remedies. The rights and remedies of the Parties provided in Section 5 are in addition to any other rights and remedies provided by law or under this Master Agreement. The Parties' remedies are cumulative and are not intended to be exclusive of any other remedies or means of redress to which a Party may be lawfully entitled in case of any breach or threatened breach of any provision of this Master Agreement. This section is subject to Section 8 below.

5.4 DISENTANGLEMENT

5.4.1 Notwithstanding anything to the contrary within Section 5.4, Hexagon's obligations to provide any Services, information, or work as described in this Section 5.4 is expressly conditioned upon the existence of an active and valid Order or other contract (which remains active and has not otherwise terminated) for such Services, information, and/or work. Additionally, nothing in Section 5.4 shall grant any additional or extend rights in and to Hexagon IP not otherwise granted in these Master Terms, including its Exhibits. Moreover, all limitations pertaining to Hexagon IP shall remain in full force and effect.

5.4.2 General Obligations.

In connection with any expiration or termination of the Agreement, or with termination of Hexagon's performance of the Services, or any portion thereof then being provided hereunder, Hexagon shall take all necessary and appropriate actions to accomplish a complete, timely, and seamless transition from Hexagon to City, or to any Third Party service providers designated by City, of the Services being terminated or expiring, without material interruption or material adverse impact on the Services, or any other services provided to City by third parties (all such actions, collectively, a "Disentanglement").

Hexagon shall promptly cooperate with City and any designated service providers, and take all steps necessary and appropriate, or reasonably requested, to assist City in effecting a complete and timely Disentanglement, including the provision to City and any designated service providers of all information necessary to effect the transition. Hexagon shall also provide for the prompt and orderly conclusion of all work related to the Services being terminated, as City may direct, including completion or partial completion and documentation of all work in progress, and other appropriate measures to assure and effect an orderly transition to City or its designated service-providers.

5.4.3 Disentanglement Process. The Disentanglement Period will commence as of the earlier of (a) the specified termination date in a notice of termination given by a Party hereunder if the Agreement is terminated earlier than the end of the Term, or (b) twelve (12) months prior to the Expiration Date (subject to City providing written notice within 30 days prior to the start of the final Contract Year) (the "Disentanglement Commencement Date"), and shall continue for date up to twelve (12) months therefrom (collectively, the "Disentanglement Period"). No later than thirty (30) days following the Disentanglement Commencement Date, Hexagon and City, and any Third Party service-providers, shall reach mutual agreement on and document a written plan (a "Disentanglement Transition Plan") that: (i) allocates responsibilities for Disentanglement and transition of the Services among the Parties and, to the extent applicable, such Third Party service-providers; and (ii) sets forth in reasonable detail the respective services to be provided by each of the Parties and such Third Party service providers, including all Disentanglement Services to be performed by Hexagon. Hexagon shall update such Disentanglement Transition Plan from time to time, as appropriate and subject to City's reasonable approval, in order to address any impact of any unexpected changes in the services as such Disentanglement progresses. For clarity, Hexagon's obligation to provide such Disentanglement Services shall terminate on the earlier of (1) completion of Disentanglement satisfactory to City, including performance by Hexagon of all of its obligations pursuant to this Section, or (2) twelve (12) months following the termination date of the Agreement, or upon the Expiration Date of the Agreement.

5.4.4 Preparation for Successor to this Agreement. At any time or times during the Term, at the written request of City, Hexagon shall provide City with any information that City is entitled to receive under this Agreement that City desires to use in preparing a request for proposal to solicit responses, or responding to proposals, for the purpose of entering into an agreement that would constitute the successor to this Agreement. Such requested information may include, among other things, current and projected transactional or other relevant volumes, resource utilization and performance statistics and trends, forms utilization, and such other information, statistics, and materials related to the provision of the Services or the use, operation, support, and maintenance of the Systems as City shall reasonably deem necessary or appropriate.

6 IP Ownership.

Customer acknowledges Hexagon will retain ownership and title of Hexagon IP made or provided pursuant to any Order. All Hexagon Software provided under the Master Agreement is licensed to Customer in accordance with Exhibit A (End User License Agreement) except as it is inconsistent with the terms set forth herein. Third Party Software is licensed to Customer pursuant to the software license agreement delivered with such Third Party Software product.

Pursuant to that certain Contract between the City and Hexagon for the Design, Implementation, and Maintenance of a Computer Aided Dispatch System dated December 23, 2015 (the "2015 Agreement"), the City received licenses for all Hexagon Software Products identified in Schedule 1 hereto. *See Attachment H (End User License Agreement) of the 2015 Agreement.* In an effort to clarify the duration of the licenses and so as to continue to facilitate continued use of Hexagon Software Products by the City and compliance with applicable law, upon execution of this Master Agreement, all Hexagon Software Products licensed to the City in the 2015 Agreement as identified in Schedule 1 shall be licensed pursuant to this Master Agreement for no additional licensing fees on a perpetual basis and in accordance with Exhibit A (End User License Agreement) hereto. Any licensing rights derived from the 2015 Agreement are terminated upon the Effective Date. This provision does not modify or alter any licenses to Third Party Software provided by Hexagon in the 2015 Agreement, which shall be licensed in accordance with the Third Party Software manufacturer's license provided through the 2015 Agreement.

7 Warranties.

7.1 Software. The Software provided under the Orders is warranted to substantially conform to the user documentation for a period of sixty (60) days from the initial installation. This warranty only applies to Software products that are not already covered by a Support Contract between Customer and Hexagon.

7.2 Subsystem Warranty Coverage. For, and only for, new Subsystems procured/implemented pursuant to an Order under these Master Terms, the warranty coverage shall be set forth in the applicable SOW, which shall be in lieu of the warranty coverage set forth in Section 7.1.

7.3 Third-party Warranty Coverage. To the extent third-party products are supplied by Hexagon, those products are provided with a pass-thru-warranty from the original manufacturer, if any.

7.4 Disclaimer. Any product information Hexagon has shared with Customer during the proposal and/or contract activities to date was to provide an understanding of Hexagon's current expected direction, roadmap, or vision and is subject to change at any time at Hexagon's sole discretion. Hexagon specifically disclaims all representations and warranties regarding future features or functionality to be provided in any Software or Deliverable. Hexagon does not commit to developing the future features, functions, and/or products discussed in this material beyond that which is specifically committed to being provided by Hexagon pursuant to a valid Order. Customer should not factor any future features, functions, or products into its current decisions since there is no assurance that such future features, functions, or products will be developed. When and if future features, functions, or products are developed, they will be made generally available for licensing by Hexagon.

7.5 Warranty Disclaimer. EXCEPT AS SPECIFICALLY SET FORTH IN THIS ARTICLE, HEXAGON DISCLAIMS (TO THE FULLEST EXTENT PERMITTED BY LAW) ALL WARRANTIES ON PRODUCTS FURNISHED PURSUANT TO THE MASTER AGREEMENT, INCLUDING ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WARRANTIES SET FORTH IN THIS ARTICLE 7 IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, AND, EXCEPT AS SET FORTH IN ARTICLE TITLED "INDEMNIFICATION PROVISIONS" BELOW, REPRESENTS THE FULL AND TOTAL WARRANTY OBLIGATION AND/OR LIABILITY OF HEXAGON.

8 LIMITATION OF LIABILITY

OTHER THAN THE INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 9, IN NO EVENT WILL HEXAGON BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES, LOST PROFITS, LOSS OF USE OR PRODUCTION, LOSS OF REVENUE, LOSS OF DATA, OR CLAIMS OF THIRD PARTIES, EVEN IF HEXAGON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH

DAMAGES. OTHER THAN THE INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 9, UNDER NO CIRCUMSTANCE WILL HEXAGON'S LIABILITY UNDER THIS MASTER AGREEMENT EXCEED TWO MILLION DOLLARS ($2,000,000).

9 Indemnification Provisions.

9.1 Hexagon (with legal counsel reasonably acceptable to City) will defend, indemnify, protect, and hold harmless, at its expense, a third party action, suit, or proceeding ("Claim") against Customer and its elected officials, officers, employees, agents, and representatives ("Indemnified Parties"), and indemnify the Indemnified Parties from any and all claims, losses, costs, damages, injuries (including, without limitation, injury to or death of an employee of Hexagon or its subcontractors), expense, and liability of every kind, nature and description (including, without limitation, incidental and consequential damages, court costs, and litigation expenses and fees of expert consultants or expert witnesses incurred in connection therewith and costs of investigation), judgments, settlements, and reasonable attorney's fees resulting therefrom, to the extent such Claim is (i) related to, arises out of, or pertains, directly or indirectly, in whole or in part to bodily injury, death, or physical damage to tangible property caused by Hexagon's willful or negligent acts or omissions arising under the Master Agreement; (ii) based upon an allegation that a Software Product, Customized Software, or Services Deliverable as of its delivery date under the Master Agreement, infringes a valid United States: patent, copyright, or trademark, or misappropriates a third party's trade secret ("Infringement Claim"); or (iii) is related to, arises out of, or pertains, directly or indirectly, in whole or in part to a breach by Hexagon of the confidentiality or data security provisions set forth in this Agreement.

9.2 Hexagon's defense and indemnification obligations are conditioned upon:

9.2.1 Customer providing reasonably prompt written notice to Hexagon in writing of any Claim;

9.2.2 Hexagon having primary control of the defense of any actions and negotiations related to the defense or settlement of any Claim, understanding Hexagon may not settle a claim without first obtaining Customer's written consent if such settlement assigns fault or culpability to Customer or involves injunctive or equitable relief affecting City;

9.2.3 Customer cooperating fully in the defense or settlement of any Claim; and

9.2.4 Customer has the right to participate in the defense of the Claim at its own expense, and in any negotiations and settlement.

9.3 Hexagon will have no obligation to defend Customer or to pay any resulting costs, damages, or attorneys' fees for any Infringement Claims alleging direct or contributory infringement of the Software Product or Service Deliverable (i) by the combination of or integration with a product, process, or system not supplied by Hexagon; (ii) by material alteration by anyone other than Hexagon or its subcontractors; (iii) by use after Customer has been notified of possible infringement; (iv) by use after a return for refund as described below is ordered by Hexagon; (v) if the creation of which was pursuant to specifications provided by Customer; or (vi) by use other than as specified in the documentation associated with the Software Product.

9.4 In connection with any Infringement Claims, Hexagon, at its own expense and option, may either (i) obtain rights for Customer to continue using the allegedly infringing Hexagon supplied item; (ii) replace the item with a non-infringing alternative, or modify the allegedly infringing elements of the item, while maintaining substantially similar software functionality or data/informational content; or (iii) refund to Customer a prorated portion of the license fees paid by Customer for the infringing item(s); provided that proration for perpetually licensed software shall be based on a five (5)-year, straight-line depreciation basis beginning from the initial date of delivery. In the event of a prorated return, Customer will uninstall, cease all use of and return to Hexagon the infringing item(s).

9.5 In no event will the indemnification for Infringement Claims apply to any Beta Software, or sample, hot fix, royalty-free, or evaluation software delivered pursuant to the Master Agreement.

10 Insurance.

10.1 Policies and Coverage Amounts. Hexagon agrees to procure and maintain in force during the term of the Master Agreement, at its own cost, the following policies and amounts of coverage:

10.1.1 Workers' Compensation Insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than ONE MILLION DOLLARS ($1,000,000) per accident for bodily injury or disease.

10.1.2 Commercial General Liability Insurance written on an Insurance Services Office Form CG 00 01 covering CGL on an "occurrence" basis, with minimum combined single limits of ONE MILLION DOLLARS ($1,000,000) each occurrence and TWO MILLION DOLLARS ($2,000,000) general aggregate. The policy shall be applicable to all premises and operations. The policy shall include coverage for products and completed operations, bodily injury, broad form property damage, and personal and advertising injury. There shall be no endorsement or modification of the Commercial

General Liability insurance limiting the scope of coverage for either insured versus insured claims or Contractual liability. All defense costs shall be outside the limits of the policy.

10.1.3 Automobile Liability Insurance written on an Insurance Services Office Form Number CA 0001 covering Code 1 (any auto) or, if Contractor has no owned autos, Code 8 (hired) and 9 (non-owned), with minimum combined single limits for bodily injury and property damage of not less than ONE MILLION DOLLARS ($1,000,000) for any one occurrence, with respect to each of Hexagon's owned, hired or non-owned vehicles assigned to or used in performance of the services or work under the Master Agreement.

10.1.4 Umbrella/Excess Coverage with minimum combined single limits of ONE MILLION DOLLARS ($1,000,000) per occurrence.

10.1.5 Cyber Liability Insurance with a minimum combined single limits of not less than ONE MILLION DOLLARS ($1,000,000) for each claim and an annual aggregate of TWO MILLION DOLLARS ($2,000,000) covering claims resulting from a failure of computer security including liability caused by theft, and disclosure of confidential information, unauthorized access and use of electronic information, unintentional release of private information, and extortion. Such coverage is required only if any products and/or services related to information technology (including hardware and/or software) are provided to Insured and for claims involving any professional services for which Hexagon is engaged with Insured for such length of time as necessary to cover any and all claims.

10.1.6 Professional Liability with limits of at least ONE MILLION DOLLARS ($1,000,000) per occurrence and TWO MILLION DOLLARS ($2,000,000) aggregate, covering the risk of errors and omissions, negligent acts and costs of claims/litigation, including investigation and court costs. If the coverage is written on a "claims-made" form, Hexagon must ensure that the policy retroactive date is before the Effective Date, that coverage is maintained during the duration of performance of this Master Agreement or the term period (whichever is longer) and the policy will be renewed for at least three (3) years following completion or termination of the performance of professional services under this Contract.

10.2 Policy Maintenance. Hexagon shall procure and maintain, and shall cause any subcontractor of Hexagon to procure and maintain, the minimum insurance coverages listed herein. Hexagon shall be responsible for providing the insurance coverage reflected herein on its behalf and on behalf of any subcontractors. Subcontractors shall not be required to provide any separate or corresponding insurance to the City in addition to what is already provided by Hexagon. All policies shall be continuously maintained for the term of the Master Agreement. Hexagon shall not modify any policy or endorsement thereto which increases the City's exposure to loss for the duration of this Master Agreement.

10.3 Certificate of Insurance. A Certificate of Insurance shall be completed by Hexagon's insurance agent(s) as evidence that policies providing the required coverage amounts, conditions, and minimum limits are in full force. The completed Certificate of Insurance shall be sent to the contact person identified in the Principal Contracting Document. Hexagon shall furnish City with original certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this clause. All certificates and endorsements are to be received and approved by City before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive Contractor's obligation to provide them. City reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.

10.4 Insurance Deductible. Hexagon shall be solely responsible for any deductible losses under the policies required above. All deductibles on any policy shall be disclosed to the City at the time the evidence of insurance is provided.

10.5 Other Insurance Provisions. The insurance policies are to contain, or be endorsed to contain, the following provisions:

10.5.1 Additional Insured Status. The City, its officers, officials, employees, and volunteers are to be covered as additional insureds on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of Hexagon including materials, parts, or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to Hexagon's insurance (at least as broad as ISO Form CG 20 10 11 85 or if not available, through the addition of both CG 20 10, CG 20 26, CG 20 33, or CG 20 38; and CG 20 37 if a later edition is used).

10.5.2 Primary Coverage. For any claims related to this contract, Hexagon's insurance coverage shall be primary coverage at least as broad as ISO CG 20 01 04 13 as respects the City, its officers, officials,

employees, and volunteers. Any insurance or self-insurance maintained by City, its officers, officials, employees, or volunteers shall be excess of Hexagon's insurance and shall not contribute with it.

10.5.3 Notice of Cancellation. Hexagon shall provide prompt notice if a policy is prematurely terminated and provide evidence of its new policy having the coverages reflected herein.

10.5.4 Waiver of Subrogation. Hexagon hereby grants to City a waiver of any right to subrogation which the Workers' Compensation insurer of Hexagon may acquire against City by virtue of the payment of any loss under such insurance. Hexagon agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the City has received a waiver of subrogation endorsement from the insurer.

10.5.5 Claims Made Policies (applicable only to professional liability). The Retroactive Date must be shown, and must be before the date of the contract or the beginning of contract work. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the contract of work. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, Hexagon must purchase "extended reporting" coverage for a minimum of five (5) years after completion of work.

10.6 Acceptability of Insurers. Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A-VI, unless otherwise acceptable to City.

City will accept insurance provided by non-admitted, "surplus lines" carriers only if the carrier is authorized to do business in the State of California and is included on the List of Approved Surplus Lines Insurers (LASLI list). All policies of insurance carried by non-admitted carriers are subject to all of the requirements for policies of insurance provided by admitted carriers described herein.

10.7 Special Risks or Circumstances. City reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

10.8 Additional Insurance. Hexagon may obtain additional insurance not required by this Contract.

10.9 Excess Insurance. All policies providing excess coverage to City shall follow the form of the primary policy or policies including but not limited to all endorsements.

11 Security and Breach Notification.

11.1 Hexagon shall take reasonable industry action to prevent, detect, identify, report, track and respond to Security Incidents. In the event of a Security Incident, Hexagon will promptly notify the customer in writing via email and provide a Security Incident report to the Customer or its Affiliates via the support website. The report, including access and system logs, shall be provided as soon as practical following discovery and investigation of a Security Incident. If a Security Breach occurs, or if Hexagon determines or is notified that there is any security vulnerability, Hexagon will promptly notify Customer in writing via email and also by telephone at a phone number (or phone numbers) provided by Customer, provide to Customer a Security Breach report, including access and system logs, via the support website, and apply any remedial workaround immediately and apply necessary patches within thirty (30) days of discovery of the Security Breach or the security vulnerability.

12 Dispute Resolution.

12.1 Resolution Protocol. The Parties shall exercise their best efforts to negotiate and settle promptly any dispute that may arise with respect to the Master Agreement or Order made pursuant to the Master Agreement ("Dispute") in accordance with the provisions set forth herein. If either Party disputes any provision of the Master Agreement (the "Disputing Party"), or the interpretation thereof, or any conduct by the other Party under the Master Agreement, that Party shall bring the matter to the attention of the other Party at the earliest possible time in order to resolve the Dispute except for Disputes for non-payment. If such dispute is not promptly resolved by the employees responsible for the subject matter of the dispute, the Disputing Party shall be permitted to deliver to the non-Disputing Party contact person identified in the Principal Contracting Document a written notice of the dispute, whereupon the Parties shall endeavor in good faith to escalate the dispute to appropriate executives for each Party for resolution within fifteen (15) business days, or such longer period as to which the Parties may mutually agree.

12.2 Mediation. To the extent a dispute is not resolved through the process outlined in the previous section and remains unresolved, the Parties agree to enter into non-binding mediation to resolve the dispute. Within sixty (60) calendar days, of the issuance of the Dispute Notice, or such longer period that is mutually agreeable to the Parties, the Parties agree to identify a mutually acceptable mediator who shall mediate the dispute. The mediator will be knowledgeable in the subject matter of this Master Agreement, if possible. If after making reasonable efforts to identify a mutually acceptable mediator and no later than fifty (50) calendar days after the issuance of the Dispute Notice, the Parties are unable to identify such a mediator, the Disputing Party shall provide the non-disputing party with a list of five (5) proposed mediators. The non-disputing Party shall have

five (5) business days from receipt of such list from the Disputing Party to identify one proposed mediator on the list to use as a mediator. If the non-disputing Party fails to identify and communicate its choice to the Disputing Party in the time allotted, then the Disputing Party shall be permitted to unilaterally identify the mediator from the list of five (5) mediators previously given who shall mediate the Dispute. The mediator shall be an attorney licensed to practice law in the state courts identified in section below titled "Governing Law" of California. Subject to the mediator's availability, the Parties agree to mediate the dispute within thirty (30) days after the Parties have identified a mediator who has agreed to mediate the dispute. To the extent the mutually identified mediator is unavailable, unwilling, or unable to mediate the Dispute, the Parties shall utilize the same steps listed above to identify a new mutually agreeable mediator. To the extent the Disputing Party had to prepare a list of proposed mediators previously, it shall prepare and transmit a revised list within five (5) business days of receiving notice of the proposed mediator's unavailability. Subject to the mediator's requirements, the Parties agree they shall be permitted to attend the mediation via telephone or video conferencing. The expenses of witnesses for either side shall be paid by the Party producing such witnesses. The Parties agree to pay in equal shares all other expenses of the mediation, including the mediator's fee, required traveling and expenses of the mediator, and the cost of any proofs or expert advice produced at the direct request of the mediator unless otherwise agreed to pursuant to a settlement agreement.

12.3 Conduct of Mediation Sessions. Mediation hearings will be conducted in an informal manner and discovery will not be allowed. The discussions, statements, writings and admissions will be confidential to the proceedings (pursuant to California Evidence Code sections 1115 through 1128) and will not be used for any other purpose unless otherwise agreed by the parties in writing. The Parties may agree to exchange any information they deem necessary. Both Parties shall have a representative attend the mediation who is authorized to settle the dispute, though City's recommendation of settlement may be subject to the approval of the Mayor and City Council. Either Party may have attorneys, witnesses or experts present.

12.4 Mediation Results. Any agreements resulting from mediation shall be memorialized in writing. The results of the mediation shall not be final or binding unless otherwise agreed to in writing by the Parties. Mediators shall not be subject to any subpoena or liability, and their actions shall not be subject to discovery.

12.5 Prerequisites to Litigation. Except for disputes for non-payment, only after the Parties have endeavored to resolve the dispute through the processes outlined in the immediately preceding four sections may a Party commence litigation to resolve the dispute.

12.6 Injunctive Relief. Notwithstanding the foregoing, either Party may, before or during the exercise of the informal dispute resolution procedures set forth above, apply to a court identified in the section titled "Governing Law" for a temporary restraining order or preliminary injunction where such relief is necessary to protect its interests pending completion of such informal dispute resolution procedures.

13 Notices.

All notices given between the Parties shall be in writing and shall be considered properly sent by postage prepaid United States Mail or overnight carrier to the Customer and/or Hexagon representative, as applicable and identified in the Principal Contracting Document, or such substitutes as may hereafter be disclosed by proper notification.

14 Force Majeure.

Neither Party shall be deemed to be in default of any provision of the Master Agreement or an Order or be liable for any delay, failure in performance, or interruption of service resulting from acts of war, acts of terrorism, acts of God, acts of civil or military authority, labor disruption, civil disturbance, imposition of government (federal, state, or City) restrictions that prevents performance, government imposed quarantine that prevents performance, or other specific reasons reasonably agreed to by the Parties. Notwithstanding the foregoing, Hexagon shall promptly notify the City in writing if there is, or it is anticipated, that there will be, a delay in performance. The written notice shall include an explanation of the cause for, and a reasonable estimate of the length of the delay. If in the opinion of the City, the delay is material, and the circumstances are within the control of Hexagon, the City may terminate this Agreement as provided in Section 5.2.

15 Place of Performance.

To the extent necessary, Customer, in its sole discretion will provide appropriate work space for the Resident Systems Administrator and other Hexagon resources as may be specified in an Order.

To the extent necessary or as otherwise provided in the Order Documents, Customer at its sole discretion will provide access to relevant data, documents, plans, reports, and analyses; and necessary access to Hexagon personnel to perform work on an Order. To the extent work is performed remotely, and subject to the background provisions outlined in the Principal Contracting Document, Customer will allow secured remote connectivity to all servers and workstations requiring installation/configuration by Hexagon. Hexagon will abide by the remote access guidelines provided in the City's Information Security Standards and Guidelines,

including use of Privileged Access Management (PAM) services when applicable. Hexagon must notify Customer via email when accessing the Customer's system or network, and the purpose of such access.

16 Amendments.

Any and all amendments to the Master Agreement shall specifically reference the fact the amendment is intended to alter these Master Terms. No Order or Change Order shall affect these Master Terms.

17 Confidential Information.

This Master Agreement is not Confidential Information. The Parties agree not to disclose Confidential Information provided to it by the Disclosing Party to the maximum extent allowable under applicable law unless it first obtains the Disclosing Party's written consent to such disclosure. It is further understood and agreed that money damages may not be a sufficient remedy for any breach of this provision of the Master Agreement by the Receiving Party and the Disclosing Party may be entitled to seek equitable relief, including injunction and specific performance, as a remedy for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach of this provision of the Master Agreement but will be in addition to all other remedies available at law or equity. The covenants set forth herein and the rights and obligations related thereto shall continue for a period of five (5) years from the date of disclosure. Notwithstanding the foregoing, nothing in this Master Agreement creates any obligation on the part of the City to notify Hexagon or obtain the Hexagon's approval or consent before releasing information subject to disclosure under the California Public Records Act (CPRA) except if Hexagon provides the City with information that is clearly marked as confidential or proprietary, and the City receives a CPRA requesting such information, then the City agrees to inform Hexagon of the request so that Hexagon may seek an appropriate protective order or other appropriate remedy to safeguard the confidentiality of its information. If Hexagon does not provide a specific and legal detailed basis for withholding the requested information within a reasonable time specified by the City, the City will release the information as required by the CPRA (unless ordered by a court of competent jurisdiction not to do so), and Hexagon will hold the City harmless for the release of this information. If the City withholds public records requested pursuant to the CPRA at Hexagon's direction and the City is the subject of litigation requiring the production of such public records, then Hexagon agrees to defend, indemnify, and to hold harmless the City for its withholding of those public records giving rise to such litigation. It is Hexagon's obligation to defend, at Hexagon's expense, any legal actions or challenges seeking to obtain from the City any information requested under the CPRA withheld by the City at Hexagon's request.

18 Personal Data.

18.1 Customer represents and agrees it shall not knowingly provide Hexagon any data pertaining to a citizen of the European Union. Hexagon and Customer agree that they will each comply with all applicable data protection laws and regulations with respect to dealing with, disclosing and exchanging and Personal Data in connection with this Agreement. Hexagon shall at all times comply with the Criminal Justice Information Services (CJIS) Security Policy (Exhibit G) and the City of San Diego Information Security Standards and Guidelines (Exhibit H). For purposes of clarity, Hexagon is obligated to comply with only those portions of Exhibit H that are expressly applicable to it. Hexagon also agrees that: (i) to the extent it has access to Personal Information, it will keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure, (ii) it will use and disclose Personal Information solely and exclusively for the purposes for which the Personal Information, or access to it, is provided pursuant to the terms and conditions of this Master Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for Hexagon's own purposes or for the benefit of anyone other than Customer, in each case, without Customer's prior written consent; and, (iii) will not, directly or indirectly, disclose Personal Information to any person other than its authorized employees who comply with the security requirements of this Master Agreement, including any subcontractors or agents (an "Unauthorized Third Party"), without express written consent from Customer unless and to the extent expressly required, by applicable law , in which case, Hexagon shall (i) notify Customer before such disclosure or as soon thereafter as reasonably possible; (ii) be responsible for and remain liable to Customer for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Personal Information as if they were Service Provider's own actions and omissions; and (iii) require the Unauthorized Third Party that has access to Personal Information to execute a written agreement agreeing to comply with the terms and conditions of this Master Agreement relating to the treatment of Personal Information.

18.2 Where Customer is responsible for providing Personal Data on behalf of Users directly to Hexagon, Customer will, to the extent possible, secure and maintain all necessary consents and make all necessary disclosures before including Personal Data in Customer Data input to, or otherwise supplied to Hexagon. In the event Customer, including all its Users, does not consent to Personal Data being processed as a result of the Master Agreement, Customer acknowledges Hexagon may be unable to provide Services, Software Products, and/or Maintenance Services (or part thereof).

18.3 Hexagon will only process Customer supplied Personal Data in accordance with the Customer's lawful instructions and to the extent and as necessarily required to provide the applicable goods and services under

the Master Agreement and for no other purpose. Except as may be otherwise required by law, contract, or judicial order, after expiration or earlier termination of the Master Agreement, Hexagon will either destroy all Customer-supplied Personal Data in accordance with applicable data protection laws, or upon Customer's request, Hexagon will immediately provide to the designated Contract Administrator electronic copies of any data collected and recorded, including Personal Data. Data format will be agreed upon by both Customer and Hexagon.

18.4 If Hexagon supplies maintenance, support, or subscription services to Customer with respect to third-party products, and if the third-party supplier or proprietor of such requires Customer be party to any data processing agreement in connection therewith, and if Customer has not separately executed an instrument to satisfy such requirement, then Customer and Hexagon agree that the terms of the applicable third-party data processing agreement detailed in Exhibit I, shall apply.

18.5 Hexagon will comply with the City of San Diego Information Standards and Guidelines detailed in Exhibit H.

19 Assignment.

Neither Party shall assign, sublet, or transfer all or any portion of the Master Agreement, nor any interest in the Master Agreement, without the express written consent of the non-assigning Party, which consent may be granted or withheld in the sole discretion of the non-assigning Party. Any assignment in violation of this paragraph shall constitute a default by Hexagon and is grounds for termination of this Contract at the City's sole discretion. In no event shall any putative assignment create a contractual relationship between City and any putative assignee.

20 Export.

Hexagon IP, including any technical data related to Software, Services, or Maintenance Services is subject to the export control laws and regulations of the United States. Diversion contrary to United States law is prohibited. Hexagon IP, including any technical data related to Software, Services, or Maintenance Services shall not be exported or re-exported, directly or indirectly (including via remote access), under the following circumstances:

- To Cuba, Iran, North Korea, Syria, the Crimean region of Ukraine or any national of these countries or territories.
- To any person or entity listed on any United States government denial list, including, but not limited to, the United States Department of Commerce Denied Persons, Entities, and Unverified Lists, the United States Department of Treasury Specially Designated Nationals List, and the United States Department of State Debarred List (http://export.gov/ecr/eg_main_023148.asp).
- To any entity if Customer knows, or has reason to know, the end use is related to the design, development, production, or use of missiles, chemical, biological, or nuclear weapons, or other unsafeguarded or sensitive nuclear uses.
- To any entity if Customer knows, or has reason to know, that a reshipment contrary to United States law or regulation will take place.

Customer agrees to hold harmless Hexagon and its Affiliates for any causes of actions, claims, costs, expenses and/or damages resulting to Hexagon from a breach of the export restrictions set forth in the Master Agreement by Customer or any User. Any questions regarding export or re-export of the Software should be addressed to Hexagon's Export Compliance Department at 305 Intergraph Way, Madison, Alabama, 35758, USA or at exportcompliance@intergraph.com. If the Software Customer received is identified on the media as being ITAR-controlled, the Software has been determined to be a defense article subject to the U.S. International Traffic in Arms Regulations ("ITAR"). Export of the Software from the United States must be covered by a license issued by the Directorate of Defense Trade Controls ("DDTC") of the U.S. Department of State or by an ITAR license exemption. The Software may not be resold, diverted, or transferred to any country or any end user, or used in any country or by any end user other than as authorized by the existing license or ITAR exemption. Subject to the terms of the EULA included herein, a Software Product may be used in other countries or by other end users if prior written approval of DDTC is obtained.

If Customer is located outside the United States, Customer is responsible for complying with any local laws in Customer's jurisdiction which might impact Customer's right to import, export or use the Software, and Customer represents that Customer has complied with any and all regulations or registration procedures required by applicable law related to the use and importation of the Software Products.

21 Non-Solicitation of Employees.

Customer agrees it will not, without the prior written consent of Hexagon, solicit any Hexagon employee to leave Hexagon's employment and be employed by the City during the Term and for a period of twelve (12) Months after the Master Agreement expires or is terminated. Notwithstanding the foregoing, Hexagon acknowledges

and agrees that nothing herein precludes a Hexagon employee from responding to and being hired from a general solicitation of Customer.

22 Miscellaneous.

22.1 Authority. Each Party represents and certifies to the other Party it has the requisite legal authority to enter into and be bound by the Master Agreement and all Orders arising from the Master Agreement.

22.2 Survival. In addition to other provisions that are specifically identified as surviving termination of this Master Agreement, the rights and obligations in sections titled "IP Ownership", "Limitation of Liability", "Dispute Resolution", "Confidential Information", "Export", and the terms of any license or access granted pursuant to the Master Agreement (including, but not limited to, Exhibit A, Exhibit D, and/or Exhibit E), shall survive and continue after expiration or termination of the Master Agreement, shall remain in effect until fulfilled, and shall apply to any permitted successors and assigns. Upon termination of the Master Agreement, the provisions of the Master Agreement, including those in the preceding sentence, which by their express terms survive termination, shall remain in full force and effect.

22.3 Waiver. The waiver by either Party of any of its rights or remedies in enforcing any action or breach under the Master Agreement in a particular instance shall not be considered as a waiver of the same or different rights, remedies, or actions for breach in subsequent instances.

22.4 Severability. If any provision of the Master Agreement or an Order is void, voidable, unenforceable, or illegal in its terms, but would not be so if it were rewritten to eliminate such terms that were found to be voidable, unenforceable, or illegal and such rewrite would not affect the intent of the provision, then the provision must be rewritten to be enforceable and legal. The unenforceability, invalidity, or illegality of any provision of this Contract shall not render any other provision of this Contract unenforceable, invalid, or illegal.

22.5 Headings. Numbered topical headings, articles, paragraphs, subparagraphs or titles in the Master Agreement are inserted for the convenience of organization and reference and are not intended to affect the interpretation or construction of the terms thereof.

22.6 Governing Law. The Master Agreement shall for all purposes be deemed to be made under, construed in accordance with, and governed by the laws of the State of California. The Parties agree that the venue for any legal action or proceeding relating to the Master Agreement, the interpretation of application of any of its terms and conditions, or any related disputes shall be in the County of San Diego, State of California. The Parties agree to submit to the jurisdiction of and agree that venue is proper in these courts in any such legal action or proceeding. The Parties waive the application of the United Nations Commission on International Trade Law and United Nations Convention on Contracts for the International Sale of Goods as to the interpretation or enforcement of the Master Agreement.

22.7 Independent Contractor. The Parties agree that Hexagon is an independent contractor, that nothing in the Master Agreement shall be construed as establishing or implying a relationship of master and servant between the Parties, or any joint venture or partnership between the Parties, and that nothing in the Master Agreement shall be deemed to constitute either of the Parties as the agent of the other Party or authorize either Party to incur any expenses on behalf of the other Party or to commit the other Party in any way whatsoever. Hexagon and its agents, employees, or subcontractors shall at no time be deemed to be agents, employees, or subcontractors of Customer, or be deemed to be under the control or supervision of Customer when carrying out the performance of its obligations in the Master Agreement. Without the prior written consent of Customer, Hexagon shall not carry on any activity that could be construed as being on behalf of Customer.

22.8 Anti-Bribery. Hexagon hereby certifies it shall comply with all applicable laws in carrying out its duties under the Master Agreement, including, but not limited to, the United States Foreign Corrupt Practices Act ("FCPA"). In particular, Hexagon agrees that it is familiar with the FCPA and its purposes and agrees to comply with the acts. Specifically, Hexagon is aware of and will comply with the FCPA's prohibition of the payment or the gift of any item of value, either directly or indirectly, to an official of a government, political party or party official, candidate for political office, or official of a public international organization, for the purpose of influencing an act or decision in his/her official capacity, or inducing him/her to use his/her influence with the government to assist a company in obtaining or retaining business for, with, or in that country or directing business to any person; Hexagon has not made, and will not make, payments to third parties which such party knows or has reason to know are illegal under the FCPA, or the laws of any applicable jurisdiction; The method of making payment to Hexagon as provided hereunder is not in violation of the law of any applicable jurisdiction.

Customer has the right to terminate the Master Agreement upon any violation of the FCPA or similar laws by Hexagon.

22.9 Hexagon Authority. BY ISSUANCE OF A QUOTE TO CUSTOMER WITHOUT THE WORD "DRAFT" OR SIMILAR MARKINGS OR DISCLAIMERS THEREON, HEXAGON REPRESENTS IT HAS THE REQUISITE LEGAL AUTHORITY TO ENTER INTO AND BE BOUND BY THE MASTER AGREEMENT AND THE ORDER INTENDED TO RESULT FROM THE QUOTE. THE QUOTE SHALL REFERENCE THIS MASTER AGREEMENT AND BY EXECUTING THE QUOTE AND RETURNING IT TO HEXAGON,

CUSTOMER REPRESENTS AND CERTIFIES TO HEXAGON IT HAS THE REQUISITE LEGAL AUTHORITY TO ENTER INTO AND BE BOUND BY THE MASTER AGREEMENT AND THE ORDER ASSOCIATED WITH THE EXECUTED QUOTEHEXAGON AGREES AND ACKNOWLEDGES THAT AN ORDER MAY NOT MODIFY THE SUBSTANTIVE TERMS AND PROVISIONS OF THE MASTER AGREEMENT WITHOUT THE WRITTEN CONSENT OF CUSTOMER IN THE FORM OF AN AMENDMENT TO THE MASTER AGREEMENT OR IN WHICHEVER FORM CUSTOMER, IN ITS SOLE DISCRETION, DETERMINES IS NECESSARY TO COMPLY WITH ITS LEGAL REQUIREMENTS.

23 Entire Agreement.

The Master Agreement constitutes the entire agreement between the Parties with regard to the subject matter hereof. Except as otherwise provided in the Principal Contracting Document, the Master Agreement supersedes any and all prior discussions and/or representations, whether written or oral, and no reference to prior dealings may be used to in any way modify the expressed understandings of the Master Agreement. Any future representations, promises and oral agreements related to the products, product features, future product enhancements, product functionality, or services covered by the Master Agreement will be of no force or effect unless reduced in writing and made a part of the Master Agreement or an Order thereto. The Master Agreement may not be amended or modified unless so done in a writing signed by authorized representatives of both Parties. The pre-printed terms and conditions of Customer's PO or any other terms and conditions of a Customer PO shall be void, even if issued subsequent to the effective date of the Master Agreement, and shall not be deemed to constitute a change to the Master Agreement.

HEXAGON
SAFETY & INFRASTRUCTURE

EXHIBIT A

END-USER LICENSE AGREEMENT

IMPORTANT—READ CAREFULLY: This EULA is a legal agreement by and between User and Hexagon for the Software Product. Software Products are also subject to the Use Terms. Any software, including, without limitation, any open source components and/or Upgrades, associated with a separate end-user license agreement is licensed to User under the terms of that license agreement. All use of the Software Product is subject to applicable Order Documents.

1.0 LICENSE GRANT. Provided User is not in breach of any term or condition of this EULA, Hexagon hereby grants User and its support vendor (currently Enforcement Support Service) a limited, non-exclusive license up to the quantity of Software Product licenses purchased by User to: (i) install and use the Software Product, in object code form only; (ii) use, read, and modify documentation prepared by Hexagon and delivered to User pursuant to the Order Documents; and/or (iii) view and/or use Hexagon audio-visual training materials provided to User pursuant to the Order Documents; provided all of the foregoing shall be strictly for User's internal use and strictly in accordance with this EULA and the applicable Order Documents. The license is non-transferable, except as specifically set forth in this EULA.

2.0 UPDATES AND UPGRADES. If the Software Product is an Update to a previous version of the Software Product, User must possess a valid license to such previous version to use the Update. Except as otherwise provided for herein, Neither the Software Product nor any previous version may be used by or transferred to a third party. All Upgrades are provided to User on a license exchange basis and are subject to all of the terms and conditions of the EULA provided with the Upgrade provided that User expressly consents to the terms of the new EULA. . Hexagon acknowledges this EULA will not be altered for version 9.4 Upgrade. By using an Update, User agrees to voluntarily terminate User's right to use any previous version of the Software Product, except to the extent that the previous version is required to transition to the Update or Upgrade; and (ii) acknowledges and agrees that any obligation that Hexagon may have to support the previous version(s) of the Software Product will end upon City's Cutover to the Update or Upgrade. If an Update is provided, User will take prompt action to install such Update as directed by Hexagon. If User fails to do so, User acknowledges that the Software Product may not work correctly or that User will not be able to take advantage of all of the Software Product's available features. In such event, Hexagon will not be liable for additional costs User incurs because of User's failure to install such Update. Hexagon will continue to support and allow Customer to use Version 9.3 and Version 9.4 of Software Product for Term of the Agreement subject to the terms herein, including Exhibit B (Support Terms).

3.0 RIGHTS AND LIMITATIONS

3.1 **The Following are Permitted for User's License:**

User may make one copy of the Software Product media in machine readable or printed form and solely for backup purposes. Hexagon retains ownership of all User created copies. User may not transfer the rights to a backup copy unless User transfers all rights in the Software Product and license as provided for in Section 3.2.1. Any other copying of the Software Product, any use of copies exceeding the number of copies User has been authorized to use and has paid for, and any distribution of the Software Product not expressly permitted by this EULA, is a violation of this EULA and of federal and/or applicable governing law.

Notwithstanding anything else to the contrary, Enforcement Support Services ("ESS") is permitted to use Software Products licensed to the Customer, for, and only, for Customer's internal business use. ESS shall be, and Customer shall ensure ESS is, bound to the same limitations pertaining to Software Products reflected herein as if ESS was a User. Additionally, ESS may not: (1) market or sell services pertaining to Hexagon Software Products in any way, (2) copy or modify Software Products; or (3) install Software Products on workstations owned by ESS. The Customer and ESS shall keep confidential in the strictest manner possible under applicable law and shall not disclose the limited rights granted herein to ESS. The confidentiality of ESS's

use of the Software Products and the limited rights provided hereunder to ESS for the exclusive benefit of the Customer is a material term of this Master Agreement.

3.2 **The Following are Prohibited for User's License:**

3.2.1 User shall not sell, rent, license, lease, lend or otherwise transfer the Software Product, or any copy, modification, or merged portion thereof without Hexagon's express written consent for such transfer, which consent may not be unreasonably withheld. Any such unauthorized transfer will result in automatic and immediate termination of the license.

3.2.2 The Software Product is licensed as a single product. Without Hexagon's consent, User shall not, and User shall not authorize anyone else to: (i) decompile, disassemble, or otherwise reverse engineer the Software Product; (ii) work around any technical limitations in the Software Product that were not otherwise directed by Hexagon; (iii) publish the Software Product for others to copy or use; (iv) use, copy, modify, distribute, disclose, license or transfer the Software Product, or any copy, modification, or merged portion, in whole or in part, except as expressly provided for in this EULA; (v) re-use the component parts of the Software Product with a different software product from the one User is licensed to use or on different computers; (vi) circumvent any license mechanism or in the Software Product or the licensing policy; (vii) publish to a third party any results of benchmark tests run on the Software Product (viii) use or view the Software Product for any purposes competitive with those of Hexagon; (ix) use the Software Product except as expressly set forth in this EULA; and (x) unless otherwise specifically permitted in writing by Hexagon, use the Software Product outside the country in which it is licensed.

3.3 **Fault Tolerance**

The Software Product is not one hundred percent (100%) fault-tolerant. Unless the Software Product's documentation expressly provides the contrary: Software Product is not designed or intended for use in any situation where failure or fault of any kind of the Software Product could lead to death or serious bodily injury of any person, or to severe physical, property or environmental damage ("High-Risk Use"); and, User is not licensed to use the Software Product in, or in conjunction with, any High-Risk Use. High-Risk Use is STRICTLY PROHIBITED. High Risk Use includes, for example, the following: operation of aircraft or other modes of human mass transportation, nuclear or chemical facilities, and Class III medical devices. Notwithstanding the foregoing, Hexagon agrees and acknowledges that User may use the product in its owned or leased helicopters and such use (but not for aviation or navigation of the aircraft) will not be considered a High-Risk Use. User hereby agrees not to use the Software Product in, or in connection with, any High-Risk Use. High Risk Use shall not mean use of the Software Product for purposes for which it is regularly marketed and sold (e.g. public safety and utility dispatch software may be used to dispatch police, fire, emergency medical services, and emergency utility services).

3.4 Licensing Mechanism Disclaimer.

Without waiver of any of its rights herein, Hexagon may at its sole discretion provide User who is operating public safety Software Products a licensing mechanism to allow such Software Products to be available for use even when User has accessed all of its purchased licenses. Regardless of whether it receives the licensing mechanism, User acknowledges it is permitted to use the Software Products only up to the amount of licenses it has purchased. Any usage of Software Products beyond the amount purchased by User will be subject to the payment of additional fees by User to Hexagon at then current prices for the Software Products in like manner as provided in Section 6.2 (Audit).

4 USER OBLIGATIONS

4.1 The Software Product may require User's System to comply with specific minimum software, hardware and/or Internet connection requirements. The specific minimum software, hardware and/or Internet connection requirements vary by Software Product and type of license and are available from Hexagon upon request.

4.2 User is responsible, and bears the sole risk, for backing up all systems, software, applications, and data, as well as properly using the Software Product.

4.3 At all times, User must keep, reproduce and include all copyright, patent, trademark and attribution notices on any copy, modification or portion of the Software Product, including, without limitation, when installed, used, checked out, checked in and/or merged into another program.

4.4 User shall comply with the Use Terms, including limitations that apply to specific types of licenses identified therein.

5 **TERM.**

5.1 For a Perpetual License, this EULA is effective until terminated (a) by User, by returning to Hexagon the original Software Product or by permanently destroying the Software Product, together with all copies, modifications and merged portions in any form; (b) by Hexagon, upon User's breach of any of the terms hereof or User's failure to pay the appropriate license or subscription fee(s); (c) upon User's installation of an Upgrade that is accompanied by a new license agreement covering the Software Product Upgrade, provided that the User expressly consents, in writing, to use of the new license agreement, which it must do before using the Upgrade; or (d) by expiration of the applicable license files, if this is a temporary license. User agrees upon the termination of this EULA to cease using and to permanently destroy the Software Product (and any copies, modifications and merged portions of the Software Product in any form, and all of the component parts of the Software Product).

5.2 For a Subscription License, this EULA is effective until the User's Subscription Term expires without being renewed; by Hexagon upon User's breach of any of the terms hereof or User's failure to pay the appropriate Subscription License fee(s); or the Subscription is otherwise terminated. User agrees upon the termination of this EULA or expiration of User's Subscription to cease using and to permanently destroy the Software Product (and any copies, modifications and merged portions of the Software Product in any form, and all of the component parts of the Software Product).

6. AUDIT.

6.1 Hexagon shall have the right to:

6.1.1 Audit User's use of the Software Product and User's compliance with the provisions of this EULA during User's normal business hours. Hexagon will provide User with thirty (30) days prior written notice of an audit under this Section. Hexagon's right to conduct this type audit shall be limited to once per calendar year. Prior to the start of an audit, Hexagon's personnel will sign a reasonable non-disclosure agreement provided by User. During the audit, User shall allow Hexagon's personnel to be provided reasonable access to both User's records and personnel.

6.1.2 Obtain certain documentation from User, as follows. If the Software Product includes logging mechanisms intended to track usage volume or quantity, User shall transmit log files associated therewith to Hexagon upon Hexagon's demand and in accordance with Hexagon's reasonable transmission instructions. Hexagon will not demand the transmission of usage tracking log files more frequently than two (2) times in any calendar year.

6.2 In the event the results of the audit in Section 6.1.1 or the documentation provided by User in Section 6.1.2 indicate User has used unlicensed Software Products or quantities thereof, User agrees to promptly pay Hexagon(i) the lesser of the negotiated price, which would have to be negotiated within ten days of Hexagon of notifying the Customer of the audit results or current list price (which will be the payment required if the parties do not finalize a negotiated price in the time prescribed) for each unlicensed Software Product(s) used by User.

END OF EXHIBIT A

HEXAGON
SAFETY & INFRASTRUCTURE

EXHIBIT B

SUPPORT TERMS AND CONDITIONS FOR SOFTWARE

These terms and conditions ("Support Terms") govern the provision of maintenance and support services by Hexagon with respect to Covered Products.

1. DEFINITIONS

All capitalized terms not otherwise defined herein shall have the meaning set forth in the associated Exhibit titled "Common Terms Glossary."

2. TERM

2.1. Term. The Support Contract shall begin, retroactively (if applicable), on the first calendar day of the first Month of the Coverage Period and shall expire on the last calendar day of the last Month of the Coverage Period. The Coverage Period shall be for whole Months only.

2.2. Renewal. Prior to expiration of the Coverage Period, Hexagon may submit to Customer a renewal quote with pricing for extension of the Coverage Period. The Parties may extend the Coverage Period pursuant to Order Documents.

2.3. Lapse. In the event of a Lapse: (i) Hexagon shall, at any time, be entitled to discontinue Maintenance Services, in whole or in part, for the affected Covered Products; (ii) Hexagon shall be relieved of any previously provided pricing commitments or options for Maintenance Services, if any, related to time periods following the Lapse; and, (iii) Hexagon may permit Customer to reinstate support for Covered Products pursuant to Hexagon's then current policies and practices, including any policies or practices related to payment of reinstatement fees.

3. SCOPE OF COVERAGE FOR COVERED SOFTWARE PRODUCTS

Maintenance Services described in this Section apply to Covered Software Products only. Maintenance Services for Covered Third Party Products are separately stated.

Hexagon offers three levels of Maintenance Services for Covered Software Products, dependent upon the Software Product and other factors. Under all levels of Maintenance Service, Hexagon shall provide reasonable commercial efforts to aid in the diagnosis and correction of Defects within the Defect resolution targets defined in Exhibit F. For I/CAD version 9.3, Hexagon will provide reasonable commercial efforts to resolve Defects, including P1 issues (Level One Defect) except as follows. Subject to the Customer implementing and using I/CAD 9.3 MR6, Hexagon will address Level One Defects even if it is a Source Code Defect for which a patch or other source code modification is necessary. However, Source Code Defects to COTS Software for 9.3 MR6 that are Level Two Defects may be addressed through a separate Order. If the Customer desires Hexagon to develop a patch or source code modification to resolve a Level 2 Defect that is a Source Code Defect, it will submit a request for a quote for such Order, and Hexagon shall provide a Quote and SOW for such a resolution so long as the patch or source code modification is reasonably feasible. To the extent the Customer agrees to the Quote and SOW, it may contract with Hexagon for such work in same manner as any other Order for a Fixed Price Project Assignment. Level 3 Defects or lower (including enhancements) within I/CAD 9.3 (any maintenance release) and requiring patches or other source code modifications will only be addressed in future versions of Hexagon's computer aided dispatch Software (e.g. I/CAD 9.4).

Upon Cutover of I/CAD version 9.4, Hexagon will provide reasonable commercial efforts to resolve Defects until the Covered Product as installed by Customer reaches Version Limitation I or Version Limitation 2. The Version Limitation will reset upon Customer's Cutover of an Update, which includes an incremental release of I/CAD 9.4, or Upgrade. Upon reaching Version Limitation I, Hexagon will continue to provide commercially reasonable efforts to resolve Defects, except Source Code Defects. After the Covered Product reaches Version Limitation 2, all Defects will continue to be addressed except Source Code Defects will only be addressed in future Updates, including an incremental release of I/CAD 9.4, or Upgrades.

Hexagon agrees, at a minimum, it will provide Updates to I/CAD 9.4 through the Term, September 30, 2025 of the Master Agreement.

Levels of Maintenance Services are as follows:

3.1. Advantage Support. Advantage Support will include and be limited to the diagnostic and Defect correction support as described above, and the following: Out-of-the-box functionality support via the support help desk (telephone or eService via Hexagon's support website; and, access to any applicable Hexagon problem knowledge base online self-help tool. Phone support is available Monday through Friday from 8AM – 5PM at Customer's local time, excluding Hexagon-observed holidays. Local variances in support hours will be posted on the Customer Support Web Site or applicable local support website or can be determined by contacting Customer's local Hexagon office.

3.2. Standard Support. Standard Support will include and be limited to the following:

3.2.1. All features of Advantage Support.

3.2.2. Access to available Updates of Covered Software Products. Hexagon will notify Customer when Updates are made available for any Covered Software Products for which Maintenance Service have been purchased, by way of posting notices of such to the "Support Notices and Announcements" section on the Customer Support Web Site or applicable local support website or via direct notification by Hexagon. Updates are shipped to Customer upon Customer request, logged in the Customer Support Web Site. Hexagon is not obligated to produce any Updates. For avoidance of doubt, a Customer's entitlement to Updates shall not include entitlement to any therein embedded or otherwise related module or function which is licensed and priced separately from Covered Product(s) for which Customer has purchased an entitlement to Updates.

3.3. Premium Support. Premium Support will include all features available under Standard Support(subject to Version Limitations and other provisions set forth in Section 3 above). Additionally, for a Level 1 Defect, phone support is also available after-hours and on Hexagon-observed holidays.

3.4 Product Change Requests (also referred to as CR-E) will be reported in like manner as set forth in Section 3.1. Hexagon will review Product Change Requests and at its sole discretion decide whether to make the requested change to the Covered Product(s) through an Update. Product Change Requests not accepted may be the subject of a separate contract between the Parties. For the avoidance of doubt, to the extent Hexagon agrees to make a requested change to a Covered Product pursuant to a Product Change Request, any and all IPR resulting from the Update including the change or modification is and shall remain the property of Hexagon.

4. MINIMUM PERFORMANCE SPECIFICATIONS

Subject to Version Limitations, I/CAD versions 9.3 and 9.4 shall substantially perform at a minimum as follows:

I/CAD Subsystem

For the I/CAD subsystem, performance standards are based on the following assumptions:

- The I/CAD System is configured and maintained according to Hexagon recommendations for workstation, system, and application configuration, as well as for database maintenance
- Anti-virus scanning software installed by the City on the I/CAD System must be configured according to Hexagon's Best Practice Guide for Anti-Virus Settings for CAD
- Minimum network speed between I/CAD Database Server #1 and I/CAD Database Server #2 = 100Mb/sec
- A maximum average round-trip latency exists (as measured by "ping") of ≤ 10ms between I/CAD Database Server #1 and I/CAD Database Server #2, and ≤ 30ms between call taker/dispatcher workstations and the database servers

Subject to the City meeting the above performance assumptions, Hexagon is generally able to meet the following CAD subsystem response times:

- Less than 1 second for 90 percent of the following Dispatcher commands:
  - Accept Event

- Unit Status Change
- Add Event Comment
- Dispatch Unit
- Close Event

- Less than 2 seconds for 90 percent of the CAD transactions that require geographic validation
- Less than 5 seconds for 90 percent of amplifying information:
  - Unit and incident history queries
  - Premise history queries
  - Status queries
- Less than 5 seconds for 90 percent of queries performed as background operations
- Seconds to minutes for reports performed as background operations

Many factors can impact response time, including network latency, complexity of the map display, interaction with external systems, and data volumes retained on the production database servers. For example, Hexagon recommends the City retain a maximum of 30 days of query response text on the Production database and move response data older than 30 days to the separate Archive/Report server.

The majority of I/CAD application commands will meet the criteria stated above. However, commands requiring responses from external data sources, such as queries to external systems, may take longer based on the responsiveness of the external system and network speed/traffic.

Compound commands that perform multiple operations for the call taker or dispatcher upon selection of a single command might not meet the stated response times. An example of a compound command is a Traffic Stop command configured to automatically spawn Create Event, Dispatch Unit, and Add Supplemental Information commands.

With regard to external database queries, the system will meet the performance requirement in most cases. However, due to factors such as network latency and external system responsiveness, it is not possible to commit to response times for ad hoc external database query requests.
Please note that Hexagon cannot guarantee response times where that response time depends on the performance of the network, system load, and any external systems (e.g., queries to state databases).

5. MINIMUM SYSTEM REQUIREMENTS; CUSTOMER'S OBLIGATIONS

Performance of Maintenance Services by Hexagon is specifically conditioned upon the following minimum system requirements and fulfillment by Customer of the following obligations (collectively, minimum system requirements and customer obligations hereinafter referred to as "Customer Obligations"):

5.1. System Requirements. Customer is responsible for ensuring: the System Equipment and network infrastructure meet minimum system requirements specified by Hexagon and made available to Customer upon request; its System Equipment and network infrastructure are adjusted as required to accommodate Updates of Covered Products; compatibility of non-Hexagon provided products with products provided by Hexagon; and, its systems, software, and data are adequately backed up. Hexagon is not liable for lost data.

5.2. Hexagon Access and Customer Cooperation. Customer's system and/or System Equipment must have input and output devices that enable the use of Hexagon's diagnostic programs and supplemental tests. Customer will permit Hexagon employees authorized by the City to electronically access Customer's system via SecureLink™, a tool providing secure, auditable remote access to Customer's system for Hexagon to effectively render Maintenance Services. Hexagon will notify the City prior to accessing the City's system, specify the reason for the access, and mutually agree with the Customer on the time to perform the maintenance. Notwithstanding the foregoing, if the City reports a Priority 1 Defect, such reporting shall constitute the City's consent for Hexagon to access the City's System in the manner described above for the limited purpose of diagnosing and addressing the reported Defect. Customer will ensure availability of its own system technical support personnel so that Hexagon can fulfill its Maintenance Services obligations. When reporting problems to Hexagon's support help desk, Customer will provide a complete problem description, along with

all necessary documents and information that is available to Customer and required by Hexagon to diagnose and resolve the problem. Customer will grant all necessary access to all required systems as well as to the Covered Products, and any other reasonable assistance needed. Customer will carry out any reasonable instructions and will install any necessary patches, Defect corrections, or Updates. Customer will appoint a minimum of two and a maximum of three contact people who are each authorized to make use of the Maintenance Services ("Authorized Contacts"). Customer must assure Authorized Contacts have adequate expertise, training, and experience to provide professionally accurate descriptions of malfunctions and facilitate Hexagon's efficient response. Subject to the Customer having contracted for and continuing to contract for a Resident System Administrator, Authorized Contacts may contact Hexagon without having first undergoing Hexagon training for System Administrators; however; within three (3) years of the Customer resource being designated as an Authorized Contact, that person shall have received formal Hexagon product training for System Administrators.

6. EXCLUDED SOFTWARE SERVICES

Services for the following are outside the scope of the Support Contract and may be available under separate Order at an additional charge (collectively "Excluded Services"):

6.1. Installation of any Covered Product, Update, or interface software.
6.2. Network configuration.
6.3. Creation of configurations or customizations of Covered Products to Customer or other third party requirements, except as necessary to remedy a Defect with an existing Covered Product. For purposes of clarity, if an Order expressly states a customization or configuration is included as part of an Order, then it will not be subject to this exclusion.
6.4. System-level tuning and optimization and system administration support.
6.5. Training.
6.6. Services required because the Authorized Contact is not available.
6.7. On-site services (unless waived by Hexagon, in its sole discretion).
6.8. Services required due to modifications of Covered Products by Customer unless otherwise directed by Hexagon
6.9. Services required due to use other than in the ordinary manner intended for the Covered Products, or use in a manner that contravenes terms hereunder, or Customer's disregard of the installation and operating instructions according to the Documentation provided with the Covered Products.
6.10. Services required due to failure of software or hardware that is not a Covered Product.
6.11. Services required due to Customer's use of hardware or software that does not meet Hexagon specifications or failure of Customer to maintain or perform industry standard maintenance on Customer's hardware or software.
6.12. Services required due to software or portions thereof that were incorrectly installed or configured (other than by Hexagon) or use in an environment inconsistent with the support environment specified by Hexagon, or used with peripherals, operational equipment or accessories not conforming to Hexagon's specifications.
6.13. Services required due to cases of force majeure, especially lightning strikes, fire or flood, third-party criminal acts, or other events not caused through Hexagon's fault.
6.14. Services required due to Customer's failure to fulfill the Customer Obligations.
6.15. Services required due to faulty or incomplete Customer data.

7. COVERED THIRD PARTY PRODUCTS

Support and Updates of Covered Third Party Products shall be provided in the fashion and to the extent or duration that Hexagon is authorized to provide such by the third party manufacturer of the Covered Third Party Products, and such Covered Third Party Products and related services may be subject to additional terms and conditions of the third party manufacturer of the Third Party Software.

Services and updates for any Third Party Software that are not listed in the Order Documents as Covered Products must be obtained from the third party owner of the products or their designated representative.

8. REQUIRED COVERAGE

8.1. Multiple or Interdependent Licenses. If Customer holds multiple licenses for any Covered Product, all held licenses must be included as Covered Products in the Support Contract.

8.2. Prerequisite Licenses. All prerequisite licenses for Software Products necessary to operate the Covered Products, together with all licenses of Software Products interoperating with Covered Products in a single solution, must be included as Covered Products in the Support Contract.

9. ADDITIONS AND REMOVALS OF COVERED PRODUCTS

9.1. Additions of Covered Products. Software Products licensed from Hexagon during the term of the Support Contract may be added as Covered Products, if such addition is addressed through additional related Order Documents. If Software Products are not added as Covered Products by commencement of Production use thereof, Hexagon may permit Customer to add support, but subject to additional fees payable pursuant to Hexagon's then current policies or practices.

9.2. Removal of Covered Products from Maintenance The Customer may provide written notice to Hexagon at least sixty (60) calendar days prior to the end of any Coverage Period Anniversary of its intent to remove any individual Covered Products from the Support Contract at the end of the then current and contracted Coverage Period or any Coverage Period Anniversary. The Customer may remove Covered Products only at Coverage Period renewal or extension or Coverage Period Anniversary; Customer may not remove from the Support Contract individual software licenses of a Covered Product for which Customer has multiple copies under Maintenance Services or for Covered Products that are being used interdependently, unless Customer has first certified to Hexagon on a "Software Relinquishment Agreement" that it surrenders and relinquishes all rights in and to the applicable Software licenses and the copies of the Covered Product for which Customer desires to cease Maintenance Services (the "Relinquished Licenses") for the renewal Coverage Period have been uninstalled and removed from its system(s). Should Customer desire to resume usage of the Relinquished Licenses at a later date, Customer must re-purchase the licenses at the then current list price.

9.3. To the extent Hexagon elects to remove a product from Maintenance and does not offer a replacement product with a comparable purpose, then Hexagon shall provide thirty (30) months advance notice to the Customer of such intention. For Covered Products that will be removed from maintenance but which it offers a replacement product with a comparable purpose and the Customer receives rights to the replacement product hereunder, then Hexagon may remove the Covered Product upon providing the City eighteen (18) months notice. For purposes of clarity, removal of maintenance in the context listed above means removal of all versions of the Covered Product and not a particular version of the Covered Product. Hexagon may rename Covered Products (the Software remains the same but the name has changed) and notify the Customer of the renaming when it provides the Quote for Maintenance Services.

10. PAYMENT

10.1. Terms of Payment. Charges for Maintenance Services are due and payable annually and in advance. Invoices will not be issued until after the City enters into an Order for Maintenance or at applicable anniversary date as specified in the Order. Services, or prior to the beginning of the applicable Coverage Period, whichever is earlier. Charges for Covered Software Products added during a Coverage Period shall be prorated to the remaining Months of the Coverage Period, in whole Month increments only, and such charges shall be due and payable in full upon receipt of invoice. Covered Third Party Products added during a Coverage Period are subject to Section 7 of these Support Terms.

10.2. Past Due Accounts. HEXAGON RESERVES THE RIGHT TO REFUSE SERVICE TO ANY CUSTOMER WHOSE ACCOUNT IS PAST DUE. At the discretion of Hexagon, Customers who have not paid any charges when due (i) under the Support Contract, (ii) under any other agreement between the Parties, or (iii) under any agreement between Hexagon and Customer's parent and/or subsidiary, may not be rendered Maintenance Services until all past due charges are paid in full. The start of the Coverage Period shall not be postponed due to delayed payment of any charges.

10.3. Customer's Responsibilities Concerning Invoice Questions. Subject to applicable law, if Customer intends to dispute a charge or request a credit, Customer must contact Hexagon within fifteen (15) calendar days of the date on the invoice. Customer waives any right to dispute a charge or receive a credit for a charge for Maintenance Services that Customer does not report within such period.

11. CUSTOMER ACKNOWLEDGEMENTS

During the Coverage Period, Customer commits to the following:

11.1. Customer shall have reviewed the Order Documents and by executing the Order Documents confirms the Order Documents accurately reflects all Hexagon software in its possession or control

11.2. Customer acknowledges and confirms that for all Covered Products supported under the Support Contract, all licenses of a Covered Product for which Customer has multiple copies in its possession and all prerequisite licenses necessary to operate Covered Products, are accounted for in the Order Documents. If all like Covered Products or prerequisite software licenses are not accounted for in the Order Documents, Customer agrees to notify Hexagon so that Hexagon may issue a revised Quote to Customer.

11.3. Customer acknowledges and confirms Maintenance Services provided herein shall be utilized only for the quantity of Covered Products licenses listed in the Order Documents.

11.4. Customer shall, and Customer shall cause each of Customer's employees and representatives to, comply with each and every term and condition of the EULA applicable to the Covered Products supported under the Support Contract.

12. ADDITIONAL TERMS

12.1. Software License. Any Updates furnished hereunder shall remain the property of Hexagon, Hexagon's Affiliate, or applicable third party, and are licensed in accordance with the then current Hexagon EULA, EULA of Hexagon's Affiliate, or third party SLA, which shall supersede any EULA or SLA associated with prior releases of the Covered Software Products or Covered Third Party Products, provided that User expressly consents, in writing to such agreement. Upon Customer's request, Hexagon shall provide Customer with such EULA or SLA. Upon Hexagon's request, Customer agrees, subject to the requirements described in this Section. 12.1, to execute a EULA or SLA, as applicable, for Covered Products.

12.2. Pass-Through Third Party Warranties. Covered Third Party Products are only warranted pursuant to a pass-through warranty to Customer from the applicable Third Party Software manufacturer and only to the extent warranted by the applicable Third Party Software manufacturer.

12.3. Remedies. In the event a warranted Maintenance Service, Covered Product, or Update provided pursuant to the Support Contract does not substantially comply with the limited warranties set forth in the Support Contract, Hexagon's entire liability and Customer's exclusive remedy shall be, in Hexagon's sole and absolute discretion, either (i) providing of a Service, Covered Product, or Update which conforms substantially with the warranty; or (ii) a refund of the purchase price of the particular warranted Service, Covered Product, or Update for the period of time that the warranted Service, Covered Product, or Update did not substantially conform to the limited warranties set forth in the Support Contract.

Hexagon is acting on behalf of its suppliers for the sole purpose of disclaiming, excluding and/or limiting obligations and liability as provided in the Support Contract, but in no other respects and for no other purpose.

12.4. WARRANTY DISCLAIMERS. In addition to the Warranty Disclaimer provided in the Master Terms, except as otherwise provided herein Hexagon does not warrant that any Services, Covered Products, and Updates will operate uninterrupted or error or Defect free.

12.5. Third Party Providers. Hexagon reserves the right to provide Maintenance Services through a third party provider, provided that Customer expressly consents to use of such third party provider.

HEXAGON
SAFETY & INFRASTRUCTURE

EXHIBIT C

PROJECT DELIVERABLE SIGN-OFF FORM

CUSTOMER NAME, CUSTOMER CITY – PROJECT NAME

Submission Date:	Month/Day/Year	Sign-Off Target Date:	Month/Day/year
Submitted By:	Hexagon Contact Name	Submitted To:	Customer Contact Name
Customer Contract #:	Customer Contract Number	Customer/Project #:	Hexagon Project Number

TYPE OF DELIVERABLE

☐ SOW Tasks ☐ Payments ☐ Plans/Designs ☐ Training ☐ Other

DELIVERABLE INFORMATION

DELIVERABLE DESCRIPTION
THIS SECTION DESCRIBES THE DELIVERABLE

$AMOUNT OF PYMT
(If applicable)

With the deliverable described above complete, the Customer shall have ten(10) business days after receipt of a written request from Hexagon, to either sign-off that the deliverable has been met or state in writing to Hexagon the reason the deliverable has not been met.

Sign-off of the deliverable shall be based solely upon the deliverable meeting the requirements stated in the Contract between Hexagon and CUSTOMER NAME dated Month/Day/Year and shall be indicated by the Customer signing the Project Deliverable Sign-off Form. If the Customer does not provide such sign-off or rejection within the ten (10) business day period then the deliverable will be deemed to have been signed off.

The signature below acknowledges that the deliverable described in the Contract and listed above meets all of the appropriate criteria and supersedes all prior requirements for this item.

Customer acknowledges completion of this payment milestone according to the Contract Payment Milestone Schedule and provides authorization to invoice this milestone.

Authorized Customer Representative
Customer Contact Name

_____ _____

SIGNATURE **DATE**

HEXAGON
SAFETY & INFRASTRUCTURE

EXHIBIT D

CLOUD PROGRAM CONDITIONS

INTENTIONALLY DELETED

END OF EXHIBIT D

HEXAGON
SAFETY & INFRASTRUCTURE

EXHIBIT E

SUBSCRIPTION TERMS AND CONDITIONS

These Subscription Terms and Conditions ("Subscription Terms"), govern the licensing and support for the Subscription.

1. **DEFINITIONS**. All capitalized terms not otherwise defined herein shall have the meaning set forth in Exhibit F (Common Terms Glossary).

2. **SERVICES PROVIDED**.

2.1 Access. Subject to an Order for a Subscription License Sale and these Master Terms, including Exhibit A (End User License Agreement), Hexagon will make the Subscription Licenses available to Customer for Customer's use during the Subscription Term. Any renewal or extension of the Subscription Term shall be subject to such terms and product components as reflected in the applicable renewal or extension Quote issued by Hexagon and expressly agreed to in writing by the Customer (the "***Renewal Quote***").

Customer acknowledges and agrees that Customer shall compensate Hexagon for Customer's continued use of a Subscription after expiration or termination of a Subscription Term, at a rate equitably and proportionately calculated based upon the Renewal Quote and based upon the period of such extended use; *provided that* if no Renewal Quote is issued prior to expiration or termination of the Subscription Term, the initial Quote shall be substituted in the calculations set forth in this Section 2.1.

2.1.1 As it pertains to Metered Licenses, the Customer's right to use the Metered Licenses shall end upon the earlier of: (i) expiration of the Subscription Term, or (ii) Customer's use of the its allotment of units of service as set forth in the Quote.

2.2 Maintenance and Support. During the applicable Subscription Term, Hexagon will provide maintenance services and support to the Customer for the Subscription Licenses in accordance with Exhibit B (Support Terms and Conditions) of these Master Terms.

2.3 Services. These Subscription Terms only provide for the licensing and support of the Subscription. If the Customer desires for Hexagon to provide Services for implementation, configuration, training, or other work in relation to the Subscription, then Customer may contract with Hexagon pursuant to these Master Terms for Services under a separate Order.

3. **INVOICES**. Hexagon shall invoice Customer for the amount set forth in the Quote upon delivery of or access having been provided to the Subscription Licenses identified in the Quote. To the extent the Quote includes multiple types of Subscription Licenses, Hexagon shall invoice the Customer once the first type of Subscription License is allowed to be invoiced as provided in this section. The Order must be approved by the City's Contract Administrator identified in the Master Agreement prior to invoicing. The Order shall only be binding upon the City upon the acknowledgment described in Section 22.9 of the General Terms within this Master Agreement.

4. **CUSTOMER OBLIGATIONS.**

4.1 Customer Control. Customer's and its authorized Users of the Subscription shall at all times comply with Exhibit A (End User License Agreement). Customer will be solely responsible for administering and monitoring the use of login IDs and passwords provided by Customer to authorized Users pursuant to the Subscription, or by Hexagon on behalf of Customer. Upon the termination of employment of any authorized User, Customer will terminate that individual's login ID and password. Hexagon is not responsible for any damages resulting from Customer's failure to manage the confidentiality of its login ID and passwords and Customer is responsible for any actions arising out of use or misuse of Customer's login IDs.

4.2 Security. Customer shall take commercially reasonable security precautions to prevent unauthorized or fraudulent use of Hexagon IP by Customer, Customer's employees, consultants, agents, or any other third parties authorized by Customer to access the Subscription on Customer's behalf.

HEXAGON
SAFETY & INFRASTRUCTURE

EXHIBIT F

COMMON TERMS GLOSSARY

"Activity" or **"Activities"** means a single work activity/event or collection of work activities/events by a Party or by both Parties under a specified Task.

"Affiliate" means, for business entities, the parent business entity of a Party and any business entities in which a Party or its parent company directly or indirectly holds a controlling ownership interest. "Affiliates" means, for government entities which are Customers, an entity which has entered into an intergovernmental agreement with Customer which: (i) relates to or addresses the subject matter of the Principal Contracting Document; and (ii) was disclosed to, and acknowledged by, Hexagon (A) prior to the Effective Date for any existing intergovernmental agreements, and (B) prior to any renewal date of such Principal Contracting Document for any intergovernmental agreements entered into after the Effective Date. "Control" for the purposes of this definition means that Customer owns in excess of fifty percent (50%) of the ownership interest of the Affiliate or owns a majority of the voting shares of the Affiliate.

"Auditable Cost" means the documented amount corresponding to the price of the Software delivered and/or Services performed, which in the case of a Fixed Price Project Assignment will be calculated by multiplying the hours worked by the Hexagon's employee's billable rate for all Hexagon and subcontractor resources not to exceed the Purchase Order value of the Fixed Price Project Assignment..

"Background Authorization Forms" means those certain documents provided by the Customer to Hexagon prior to the Effective Date of this Agreement to facilitate compliance with CJIS and CLETS requirements titled (i)_"Authorization to Conduct a Criminal Background Investigation" (1 page), (ii) "Background Investigations Confidential Applicant Control Sheet" (2 pages), and (iii) "Fingerprint Validation Statement" (1 page) , and which were specifically developed by the parties for its relationship.

"Beta Software" means any version of Software prior to a generally available commercial release of such Software.

"Business Day" means any day other than a weekend or public holiday in the country listed on the Quote.

"Catastrophic Event" means a rare circumstance in which mass casualties and/or significant property damage has occurred or is imminent (e.g. September 11th, hurricanes, earthquakes greater than 6.1 on the Richter scale)

"Change Order" means a document executed or accepted in writing by both Parties that modify the scope, price, milestones, and/or project schedule of an Order

"Confidential Information" means any data or information, tangible or intangible, disclosed or made available by either Party (the "Disclosing Party") to the other Party (the "Receiving Party") that the Disclosing Party considers confidential or proprietary and is not generally known in the industry or to competitors of the Disclosing Party and which shall include: (i) tangible information marked by the Disclosing Party with the word "Confidential" or otherwise identified by an appropriate stamp or legend indicating its confidential nature; (ii) Confidential Information disclosed orally or visually and identified by the Disclosing Party as confidential when disclosed, and confirmed by the Disclosing Party in a written notice within thirty (30) days following disclosure, which notice shall include markings similar to those outlined above; and (iii) all other information that, notwithstanding the absence of markings or designations, would be understood by the Parties, exercising reasonable business judgment, to be confidential. The term Confidential Information does not include information that: (i) is or becomes available in the public domain through no act of the Receiving Party; (ii) has been received on a non-confidential basis from a third party without breach of the Principal Contracting Document, where the Receiving Party has no reason to believe that such third party is bound by any confidentiality obligation to the Disclosing Party; (iii) was developed independently by the Receiving Party without reliance on the disclosed Confidential Information, provided that such independent development can be substantiated; (iv) is confirmed by the Disclosing Party as not being confidential in writing; or (v) or the is otherwise subject to release under the California Public Records Act and is not otherwise exempted under the Act.

"Core" means a physical processor on a computer server that can respond to and execute the basic instructions that drive the computer. A Central Processing Unit ("CPU") may have one or more Cores, and a given server may have multiple CPU sockets that may each contain multiple Cores.

"COTS" means commercial off the shelf Intellectual Property in the form generally released and distributed to Hexagon's customers and not including any functionality or features requiring source code changes.

"COTS Documentation" means commercial off the shelf Documentation in the form generally released and distributed to Hexagon's customers and not including or requiring changes thereto.

"Coverage Period" means the period of performance of Maintenance Services with respect to a Covered Product, as stated in the Order Documents. Coverage Periods may differ for discrete Covered Products.

"Coverage Period Anniversary" means, in the case where the Coverage Period is greater than one (1) year, the anniversary of the date on which the Coverage Period commenced.

"Covered Products" means collectively, Covered Software Products and Covered Third Party Products.

"Covered Software Product(s)" means Software Product(s) identified in the Order Documents as software for which Maintenance Services are to be provided by Hexagon. Covered Software Products shall not include Third Party Software.

"Covered Third Party Products" means Software Product(s) identified in the Order Documents as Third Party Software for which Maintenance Services are to be provided by Hexagon. Covered Third Party Products shall not include Software Products.

"Customer" means the City of San Diego, a municipal corporation.

"Customer Data" means all electronic data or information: (i) provided by Customer to Hexagon in connection with the Deliverables provided pursuant to an Order. "Customer Data" shall not mean data which (i) is in the public domain, and/or (ii) is of value to the general implementation, development, operation, or use of Hexagon products or services for the benefit of other customers. For the avoidance of doubt, Customer Data shall not include the, Software Products, Documentation written by Hexagon, and any other data and information constituting a Hexagon Deliverable.

"Customized Software" means those Services Deliverables that are software or computer code, whether in source code or object code.

"Cutover" means the point in time in which a Software Product(s) is first used by User for its generally marketed purpose.

"Defect" means a reproducible instance of an adverse and incorrect functioning of a Software Product that impacts the ability to use functionality intentionally integrated in the design of the Software Product, assuming proper usage of the Software Product in its required operating environment. Defects are further classified into four levels as follows:

Defect Priority Levels, Response Times, and Resolution Targets

Priority	Problem Description	Response Time Target	Resolution Target
▸ Level One	*No workaround available and either:* ▸ *Loss of data* ▸ *Data corruption* ▸ *Productive use prohibited, or* ▸ *Aborts.*	M-F, 7:00AM-7:00PM Central Time – Immediate* or within 30 minutes of notification	▸ 12 hours – Program code correction or a procedural work around
▸ Level Two	*No workaround available and either:* ▸ Primary purpose compromised, or ▸ Productive use significantly impacted	M-F, 7:00AM-7:00PM Central Time – Immediate* or within one hour of notification during normal business hours	▸ 48 hours – Program code correction or a procedural work around
▸ Level Three ▸	▸ Productive, but incomplete operation ▸ Level Three Defects generally have a workaround or do not	M-F, 7:00AM-7:00PM Central Time – Immediate* or within eight hours of notification during normal business hours	▸ One week – Procedural workaround ▸ Program code correction in a future software release

	otherwise substantially impair productive use.		
▸ Level Four	▸ Defects not qualifying as Level One, Two, or Three, including defects of a cosmetic nature and defects not materially limiting complete productive use	M-F, 7:00AM-7:00PM Central Time – Immediate* or within eight hours of notification during normal business hours	▸ One week – Procedural workaround ▸ Program code correction in a future software release

Customer shall classify a Defect in accordance with the foregoing; provided that, Hexagon shall reclassify the Defect as appropriate following its review thereof.

"Deliverable(s)" means all Services Deliverables, software, hardware, , and other items delivered or to be delivered by Hexagon to Customer and identified in the Order.

"Documentation" means, whether in electronic or printed form, User's Guides, Reference Guides, Administrator's Guides, Configuration Guides, and Help Guides made available at the support website (https://support.hexagonsafetyinfrastructure.com) for Software provided by Hexagon to the Customer. Documentation will be provided for all Software Applications as part of and after Upgrade to I/CAD version 9.4.

"Effective Date" means the later of the date and time the last Party signs the Principal Contracting Document and it is approved by the City Attorney in accordance with San Diego Charter Section 40, or the expiration date of the existing agreement between the Parties.

"**EULA**" means that certain End-User License Agreement set forth in these Master Terms as Exhibit A.

"Fixed Price Project Assignment" means a type of Order where Hexagon will provide Services and/or Software licenses for a fixed price.

"Hexagon IP" means Hexagon or Hexagon Affiliate developed, created, or prepared Intellectual Property.

"Installation Guide" means a computer file in a Microsoft Word or Adobe PDF document or a text file that contains information a User may need to install or operate a Software Product.

"Intellectual Property" or "**IPR"** means all forms of intellectual property including, but not limited to, patents, trademarks, copyrights, trade secrets, methodologies, logos, techniques, processes, know-how, formulae, algorithms, logic designs, screen displays, schematics, source and object code computer programs or software, documentation, mask work rights, design, ideas, product information, inventions and improvements thereto (whether or not patentable), and all works of authorship fixed in any medium of expression (including any form of online, digital, or electronic medium), whether or not copyrightable and whether registered or not.

"Lapse" means an occurrence of any period of time, regardless of duration, during which (i) a Covered Product is not the subject of an active Order for Maintenance Services or other Support Contract and an active Coverage Period, and/or (ii) payment is past due to Hexagon under a Support Contract. Extension of a Coverage Period and/or payment to Hexagon after the occurrence of a Lapse shall not negate a Lapse, absent Hexagon's express written waiver.

"Maintenance Services" means only those services described in the document titled "Support Terms and Conditions for Software" provided by Hexagon with respect to Software and other Deliverables licensed to Customer and identified in the Order Documents as the subject of Maintenance Services.

"Metered License" means a specific type of Subscription License that allows the Customer to use the Subscription License up to the number of hours set forth in the Quote during the Subscription Term. For reference, a Subscription License that is a Metered License shall have the word "Metered" in the Software Product name and/or have the letters "MTR" at the end of the product number for the Software Product instead of the other identifiers corresponding to an unmetered Subscription License referenced in its definition.

"Month" means, unless otherwise stated in the applicable provision, a calendar month.

"Onsite Fee" means a fixed fee encompassing Hexagon's travel expenses for an individual trip (an individual trip means to travel from the Hexagon resource's primary duty station in furtherance with Order and lasting no more than five (5) consecutive days).

"Order" means Order Documents that have been executed and/or accepted by both Parties documenting the purchase of any item or service and referencing the Principal Contracting Document.

"Order Documents" shall mean written documents, the terms of which include Hexagon's commitment to provide products, licenses, and/or services at a specified price, subject to the terms and conditions of the Principal Contracting Document. Order Documents may consist of a single document executed by the parties or a combination of documents that together form an Order.

"Perpetual License" means a type of license for a Software Product which allows the User to use the Software Product in perpetuity so long as the User does not otherwise violate the terms of the EULA. For reference, a Perpetual License on a Quote is denoted by its absence of either the terms "Subscription," "SaaS," or "Metered" and/or the absence of the letters "SU" or "MTR" at the end of the Software Product number or the letters "HCL" at the beginning of the Software Product number.

"Personal Data" means data, including but not limited to criminal justice information, and other information which corresponds to a living individual person defined to be Personal Data under the applicable Personal Data protection laws of the Customer's jurisdiction. Personal Data shall also include any information relating to an identified or identifiable natural person and an "identifiable person" is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, including but not limited to social security numbers, government-issued identification card numbers, financial account numbers (including credit or debit card numbers and any related security codes or passwords), health-related or medical information, health insurance identification numbers, and information in a health insurance application or claims history.

"Primary License" means the license(s) of the Software Product provided to Customer for general production use as authorized by the EULA.

"Principal Contracting Document" means the contract document accepted by the Parties which references and incorporates this Terms Glossary and/or references and incorporates a document to which this Terms Glossary is an exhibit or attachment.

"Production" means, as applicable, where a Subsystem is used in production/operation with an aim to accomplish one or more of its ultimate intended purposes. Operation solely for testing or training is not Production.

"Purchase Order" or **"PO"** means a document issued by Customer to Hexagon to authorize the delivery of certain Services or Deliverables.

"Quote" means a document issued by Hexagon reflecting Services, Maintenance Services, and/or Deliverables, which Hexagon offers to provide Customer, as well as the prices and fees therefor, the Customer's name and location, and references the Principal Contracting Document. To the extent any document or information is identified in the Quote with the intention of it being incorporated into the Quote, it will form part of the Quote.

"**Security Breach**" means: (i) any act or omission that compromises either the security, confidentiality or integrity of Personal Information, Customer Data or the physical, technical, administrative or organizational safeguards put in place by Hexagon or a Third Party Service Provider that relate to the protection of the security, confidentiality or integrity of Personal Information or Customer Data or, (ii) a breach or an alleged breach of this Agreement relating to such privacy practices.

"**Security Incident**" means an event or set of circumstances resulting in a compromise of the security, confidentiality, or integrity of Customer Data under Hexagon's control. Examples of Security Incidents include: (i) Security Breaches to Hexagon's network perimeter or to internal applications resulting in compromise of Customer's Data; and (ii) material vulnerability of Hexagon's security controls, methods, processes or procedures that result in compromise of the security, confidentiality or integrity of Customer Data, including, but not limited to, security vulnerabilities that Hexagon discovers or is notified of by Customer, the FBI, or any other law enforcement organization; and (iii) the unauthorized disclosure of Customer Data.

"Services" means the work, services, projects, assignments, or tasks Hexagon shall perform pursuant to an Order. Services do not include Maintenance Services.

"Services Deliverable" means any data, document, information, Customized Software, Third Party Software, or material provided to Customer as a product of Hexagon's performance of Services pursuant to the Principal Contracting Document.

"Software" means the software owned by Hexagon or an Affiliate and Third Party Software that is licensed to Customer.

"Software License Sale" means a type of an Order that involves only the sale of Perpetual Licenses from Hexagon to Customer. This type of Order does not include Services.

"Software Product" means the Hexagon software product(s) identified in the Order Documents, which includes (i) any associated Hexagon files or media with which the software is provided, (ii) any associated templates, data, printed materials, and "online" or electronic Documentation, and (iii) any Updates or Upgrades of such Software Products not made the subject of a separate license agreement. The term Software Products shall not include, and no rights of use are granted to User for, Third Party Components, Hexagon products, or dependencies unnecessary to operate products made the subject of the Order Documents, but incidentally delivered within the same files or media. Software Product shall not mean any Third Party Software. Software Products are subject to all of the terms and conditions of the End-User License Agreement which the Parties agree will apply to the same; and in the absence of such agreement, then the terms of the End-User License Agreement provided with the Software Product.

"Source Code Defect" a type of Defect that can be resolved only through a patch, Update, or other modification to the source code of the COTS Software.

"SOW" means a statement of work setting forth the scope of Services being provided pursuant to an Order.

"Subscription" means the collection of Subscription License(s) identified on the Quote and or purchased by the Customer.

"Subscription License" means a particular type of license to a Software Product that allow s a Customer to use the Software Product for a specified period of time identified in the Quote. For reference, a Software Product that is a Subscription License shall have the word "Subscription" in the Software Product name and/or have the letters "SU" at the end of the product number for the Software Product.

"Subscription License Sale" means a type of an Order that involves only the sale of Subscription Licenses from Hexagon to Customer. This type of Order does not include Services.

"Subscription Term" means the period of time during which Users are authorized to use the Subscription License as set forth on the applicable Quote beginning on the date the Subscription Licenses are provided to the User or the User is provided license keys or access to the Subscription License, unless otherwise noted in the Order Documents.

"Subsystem" means a Hexagon solution that is designed to provide a specific capability independent of the procurement of any other Subsystem. Hexagon's computer aided dispatch system ("I/CAD"), records management system ("RMS"), field based reporting ("FBR"), G/Technology (G/Tech), In/Service and mobile for public safety ("MPS") are each an example of a Subsystem.

"Supplementary License" means a license(s) of the Software Product which is made available by Hexagon for select Software Products to augment Primary Licenses for special purposes. Each Supplementary License requires a Primary License and the term of the Supplementary License shall not exceed the term of the applicable Primary License.

"Support Contract" means a contract under which Hexagon provides Maintenance Services to Customer in relation to Covered Products and under which Customer is to compensate Hexagon therefor.

"System" means a physical or operational location where the Software Product resides and operates on an individual server or where a single operational identification number ("Site ID") has been assigned by Hexagon.

"System Equipment" means all computer-related hardware, including but not limited to, servers, workstations, cables, mice, keyboards, cameras, and SAN's; operating system software; database software; and other third party software.

"Task" means an Activity or combination of Activities of any nature whether tangible or intangible, whether onsite or remote, or an event, as further identified in an SOW.

"Task Acceptance" means the event when the Task Acceptance Criteria has been satisfied in accordance with the Task Acceptance Process.

"Task Acceptance Criteria" means the criteria by which a Task will be evaluated for completion as described in an SOW.

"Task Acceptance Process" means the process by the Customer and Hexagon verify completion of the Task Acceptance Criteria as further described below. Once Hexagon believes the Task Acceptance Criteria has been successfully completed, Hexagon shall submit for execution by Customer's project manager a sign-off form in substantial conformity with Exhibit C, "Project Deliverable Sign-off Form." Within ten (10) business days of receipt of the applicable Project Deliverable Sign-off Form for the completed milestone or Task, Customer's project manager will either: (i) execute the Project Deliverable Sign-off Form provided by Hexagon, or (ii) provide a written description of all deficiencies to Hexagon. If Customer fails to perform either action identified in the preceding sentence within ten (10) business days, or if the Deliverable, including the Software contained in the

Fixed Price Project Assignment Order, is placed into production or utilized in a live environment, then the Task or milestone shall be deemed accepted.

"Term" means the duration of performance under the contract into which this Terms Glossary is incorporated by reference.

"Third Party Software" means computer software or other technology in which any person or entity, other than Hexagon or Hexagon's Affiliate, has any right, title or interest, including any restrictions or obligations (such as obligations to obtain consents or approvals and restrictions that may be eliminated only by obtaining such consents or approvals) applicable to the computer software or technology, but does not include software embedded in the Software Products by license from third parties. The use of Third Party Software is subject to all of the terms and conditions of the third party's software license or similar agreement ("SLA") provided with the Third Party Software. "Third Party Software Products" also means, where applicable, pre-requisite third party software products used by Hexagon in order for Customer to receive other components licensed by Hexagon and used by the Customer to use the Software Product.

"Time and Materials Project Assignment" means Hexagon will perform the Services set forth in an Order on an hourly basis until the project is either completed or the authorized hours are exhausted, whichever comes first.

"Update" means any Upgrade, modified version, fix, patch and/or update of the Software Product. Updates not meeting the definition of Upgrades are subject to all of the terms and conditions of the EULA provided with User's then current version of the Software Product.

"Upgrade" means each new release of the Software Product. Upgrades require a full installation and may be provided with a separate EULA, provided that User expressly consents to the terms of the new EULA.

"User" means Customer or an individual employed by Customer and authorized by Hexagon to use a particular Software Product or Third Party Software Product on behalf of the Customer. A User may also include Customer's contractor who requires temporary use in order to provide services on Customer's behalf. A person can only be authorized and a User if the person is an employee or designee of Customer and Customer has purchased the requisite number of licenses to provide Credentials for that User.

"Use Terms" means the Hexagon Product Usage Policy and Product Specific Terms that are at Exhibit J to these Master Terms.

(including an incremental release for I/CAD 9.4) on the third anniversary of the Customer's first operation of that version in a live production environment.

"Version Limitation II" is a status reached by a Software Product version (including an incremental release for I/CAD 9.4) on the fourth anniversary of the Customer's first operation of that version in a live production environment, or upon the Customer's failure to commence live operation prior to the availability of two newer versions of the Software Product.

"Version Limitations" means, separately and collectively, limitations on Services to be provided hereunder based upon a Covered Product reaching Version Limitation I and/or Version Limitation II.

"Virus" means any thing or device (including any software, code, file or program) which may: (i) prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; (ii) prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by rearranging, altering or erasing the program or data in whole or part or otherwise); or (iii) adversely affect the user experience or security, including worms, Trojan horses, viruses and other similar things or devices.

"Work" means, as applicable, the performance or providing of Services or Maintenance Services.

END OF EXHIBIT F

EXHIBIT G

CRIMINAL JUSTICE INFORMATION SECURITY STANDARDS AND GUIDELINES

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

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

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

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

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

1.00 Definitions

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

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

2.00 Responsibilities of the Contracting Government Agency.

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

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is

executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

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

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

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

5.00 Audit

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

6.00 Scope and Authority

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

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

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

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

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

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

EXHIBIT H

City of San Diego Information Security Standards and Guidelines

Information Technology

Department of Information Technology

Policy

Revision: 3.1.0

Information Security Standards and Guidelines

Effective Date: 1/21/2020

Contents

1. Purpose 6
2. Scope 6
3. Responsibilities 6
4. Document and Policy Approval Process 7
5. Security Exceptions 7
5.1. Exceptions to Security Policies 7
6. Users Acceptable Use 7
6.1. General Use and Ownership 7
6.2. Unacceptable Use 8
7. Hardware Inventory and Control 8
7.1. City-Owned Devices 8
7.2. Personal Devices 8
8. Software Inventory and Control 8
8.1. Gold Images and Templates 8
8.2. Citywide Applications 8
8.3. Departmentwide Applications 9
8.4. Unsupported Applications 9
8.5. Vendor-supported Applications 9
9. Physical Security 9
9.1. Physical Data Protection 9
9.2. Physical Access 9
10. Vulnerability Management 9
10.1. Patch Management 9
10.2. Vulnerability Scanning 9
10.3. Vulnerability Assessment 10
11. Configuration Management 10
11.1. Governance 10
11.2. Change Management 10
11.3. Configuration Modifications 10
12. Log Management and Monitoring 10
12.1. Security Information and Event Management 10
13. Malware Defenses 11
13.1. Endpoint Protection 11
14. Network Management 11

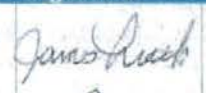
14.1. External Connections to City Network 11
14.2. Remote Access 11
14.3. Domain Name System 11
14.4. Network Equipment 11
14.5. DMZ 11
14.6. Firewall Rules 12
15. Media Disposal 12
15.1. Document Shredding 12
15.2. Computer Destruction 12
16. Data Protection 12
16.1. Data Classification 12
16.2. Data Storage and Transfer 13
16.3. Data Access 14
17. Identity Access Management 14
17.1. Principle of Least Privilege 14
17.2. User Accounts and Access 14
17.3. Applications and Services 14
18. Service Accounts 15
19. Key Management 15
20. Security Awareness and Training 16
20.1. Cyber Security Training 16
21. Application Software Security 16
21.1. Software Development Lifecycle 16
21.2. Software Updates 16
22. Cloud Providers and Services 16
22.1. Cloud Service Solutions 16
23. Incident Response and Management 17
23.1. Reporting Policies 17
23.2. User Responsibilities 17
23.3. Incident Management 17
23.4. Incident Response Plan 17
24. Compliance 18
24.1. Legal Requirements 18
24.2. Compliance Policies 18
25. References 18

25.1. External Resources 18
25.2. Internal Resources 18
Appendices 19
Appendix A – Security Objectives 19
Appendix B – Contacts 20

Document History

Version	Date	Author	Changes
3.0.0	2/4/19	Kyle/Ryan	Rework of Policy
3.0.1	2/4/19	Kyle	Added - 14.2.5
3.0.2	5/14/19	Kyle/Ryan/Becca	Changed password length from 8 to 12 Added 14.2.1.2, 16.1.1.8, 17.2.7, 23.1.4
3.0.3	6/27/19	Jon	Added 16.2.8
3.1.0	1/15/20	Jon/Kyle	Added 21.2, 21.2.1-6

Document Approval

Version	Approver Name	Title	Approver Signature	Date
3.1.0	Jim Luther - Reviewer	Deputy Chief Information Security Officer		1/15/2020
3.1.0	Darren Bennett	Chief Information Security Officer		1/15/20
3.1.0	Jonathan Behnke	Chief Information Officer		1/15/20

1. Purpose

   1.1. The purpose of this document, in conjunction with other referenced security policies, regulations and documentation, is to provide security, confidentiality, integrity and accountability within the City of San Diego.

2. Scope

   2.1. The City of San Diego Information Security Policy document encompasses all data, devices and information systems that exist in or interact with any environment or resources owned, operated or utilized by the City of San Diego.

   2.2. City employees, third-party contractors or other entities utilizing internal City resources or services, hereby referred to as "users", shall read, understand and carry out the policies outlined in this document.

3. Responsibilities

   3.1. The City of San Diego Cyber Security Team shall review and update this document on at least an annual basis.

   3.2. The City of San Diego Cyber Security Team reserves the right to change, modify or otherwise adjust this document at any time to satisfy modern technologies, manage new threats, adhere to industry regulations or better comply with best practices.

   3.3. The City of San Diego Cyber Security Team reserves the right to shut down, remove or disable systems, services, applications, accounts or devices that pose a security risk to the City of San Diego, its employees, its partners or its residents.

   3.4. The City of San Diego Cyber Security Team reserves the right to monitor all systems, services, applications, accounts, data and devices used for City business, or connected to City systems, services, applications, accounts, data or devices.

   3.5. The City of San Diego Cyber Security Team reserves the right to obtain and retain root access to any City system at any time in the interest of auditing, incident response or secure implementation.

   3.6. Modifications or additions to City information systems that affect security controls must be explicitly approved by the City of San Diego Cyber Security Team prior to being implemented.

   3.7. New or modified information technology contracts between the City and third parties must be explicitly reviewed and approved by the City of San Diego Cyber Security Team.

   3.8. Third party contracts pertaining to information technology software and/or services are expected to contain adequate security controls, service definitions and service delivery levels.

   3.9. Department Directors, Information Systems Analysts and Information Security Liaisons are responsible for assisting the City of San Diego Cyber Security Team in carrying out the policies outlined in this document.

   3.10. Supervisors are responsible for notifying their department's Information Systems Analysts of staff changes such as new hires, transfers or departures within one day of awareness.

   3.11. Information Systems Analysts are responsible for notifying the Department of Information Technology of staff changes within one day of awareness.

3.12. Department Policies, performance plans, and work standards as applicable, must include requirements for compliance with information security policies and standards.

3.13. Questions regarding terms, policies or details of this document may be directed to the City of San Diego Cyber Security Team.

4. Document and Policy Approval Process

4.1. The following steps outline the general process to be taken by the City of San Diego Cyber Security Team when updating this document:

4.1.1. New or changing technologies, threats, industry regulations or best practices are identified.

4.1.2. Research is conducted to target effective response strategies.

4.1.3. New policy, process or is decided upon and written into this document.

4.1.4. Deputy CISO reviews and approves new policy.

4.1.5. CISO reviews and approves new policy.

4.1.6. CIO reviews and approves new policy.

4.1.7. Policy update is communicated to relevant stakeholders.

4.1.8. Updated document is uploaded to IT Cyber Security Site.

5. Security Exceptions

5.1. Exceptions to Security Policies

5.1.1. Departments must employ all security controls as outlined in this document unless specific, documented exceptions are explicitly granted by the City of San Diego Cyber Security Team.

5.1.2. Policy violations that haven't been formally documented as an exception will be treated as security incidents.

6. Users Acceptable Use

6.1. General Use and Ownership

6.1.1. City of San Diego business data stored on devices whether owned or leased by the City of San Diego, an employee or a third party, remains the sole property of the City of San Diego.

6.1.2. Users are responsible for reporting potential security incidents per Incident Response and Management – User Responsibilities.

6.1.3. Users may access, use or share City of San Diego sensitive information only to the extent it is authorized by Federal, State and Local laws and regulations, City policy and only as necessary to fulfill assigned job duties.

6.1.4. Users that are not City employees must sign an NDA and be sponsored by a Deputy Director (or above) with the City prior to use of City systems.

6.1.5. Users are responsible for exercising good judgment regarding the reasonableness of personal use outside of the unacceptable use statement.

6.1.6. Users are responsible for securing their devices when not in use.

6.1.7. Workstations are to be locked behind a password when not in use.

6.1.8. Service Owners are responsible for the security of their systems unless otherwise designated in the Service Design Package.

6.1.9. The City of San Diego Cyber Security Team reserves the right to audit or perform penetration testing on networks and systems at any time.

6.1.10. Information Technology systems must be reviewed and approved by the City of San Diego Cyber Security Team prior to development, implementation or use.

6.1.11. Service delivery reports and other records from third party providers outsourced IT services must be reviewed by the City of San Diego Cyber Security

6.1.12. Team at least annually to ensure compliance with contract requirements related to information security.

6.2. Unacceptable Use

6.2.1. Users may not use City information technology resources for non-job-related functions.

6.2.2. Mechanisms that circumvent the authorized access control mechanisms found in operating systems, access control packages, or network devices are not permitted and shall not be used.

6.2.3. The City of San Diego Cyber Security Team may not conduct cyber investigations unrelated to potential security incidents without the express knowledge and approval of the Human Resources Department.

7. Hardware Inventory and Control

7.1. City-Owned Devices

7.1.1. An inventory of City-owned hardware must be maintained and updated regularly by the Department of Information Technology.

7.1.1.1. Departments must maintain the accuracy and currency of all hardware assets within their business control.

7.1.2. Non-information/data assets within the city's information systems environment (computer equipment, peripheral devices, etc.) shall be owned by the Department of Information Technology.

7.2. Personal Devices

7.2.1. Individuals must not use their personally owned systems in any City facility.

7.2.2. Personal devices are not permitted to be attached to any City network.

7.2.3. Personal devices accessing non-network City resources must be in compliance with all standards outlined in this document.

8. Software Inventory and Control

8.1. Gold Images and Templates

8.1.1. Gold images and templates are defined as master images or base images used for initial system installation or for system re-installations. The use of golden images can save time and ensure security and consistency by eliminating the need for repetitive configuration changes and performance tweaks. Gold Images must be reviewed and updated on at least a quarterly basis.

8.1.2. Gold images and templates must be scanned, reviewed and approved by the City of San Diego Cyber Security Team prior to production deployment.

8.1.3. Gold images and templates must include endpoint protection, detection and response agents.

8.1.4. Gold images and templates are required to be used.

8.2. Citywide Applications

8.2.1. Citywide applications must retain full and proper documentation regarding policies, procedures and security points of contact.

8.2.1.1. This documentation must be reviewed and updated at least annually by the document owner or department.

8.3. Departmentwide Applications

8.3.1. Departmentwide applications must be supported by a designated service owner and security contact within their department.

8.3.2. Departmentwide applications must retain full and proper documentation regarding policies, procedures and security points of contact.

8.3.2.1. This documentation must be reviewed and updated at least annually by the document owner or department.

8.4. Unsupported Applications

8.4.1. Applications not supported by the Department of Information Technology or the department of the user, must be explicitly approved for use by the City of San Diego Cyber Security Team.

8.4.1.1. Unsupported applications discovered are subject to immediate removal.

8.5. Vendor-supported Applications

8.5.1. Applications supported by third parties and associated vendor third party must be explicitly approved by the City of San Diego Cyber Security Team.

9. Physical Security

9.1. Physical Data Protection

9.1.1. Physical copies of Protected data must not be visible in plain sight.

9.1.2. Removeable media such as diskettes, zip drives, tapes, CDs, DVDs, USB or memory cards containing Protected data must be secured at all times.

9.1.3. Workstations must be locked when not in use.

9.2. Physical Access

9.2.1. Systems with access to City networks must be physically secured via room locks, facility controls or being physically controlled by the user of the system(s) at all times.

9.2.2. Facilities housing Protected data must have physical barriers such as walls or fences controlled with entry gates, access card entry doors, cipher logs, security guards or manned reception desks.

9.2.3. Rooms housing Protected data must be restricted to authorized persons only.

9.2.4. Access to areas housing Protected data must be traceable.

9.2.5. Smoke/fire alarm and suppression systems are required for all data centers, server rooms and telecommunication closets.

9.2.6. Environmental controls such as temperature, humidity, and ventilation control measures must be in place for all data centers and server rooms.

9.2.7. Physical and electronic keys (such as RSA or YubiKey) must be tracked and issued to authorized users and not be shared with other users.

10. Vulnerability Management

10.1. Patch Management

10.1.1. Systems must be patched on at least a monthly basis.

10.2. Vulnerability Scanning

10.2.1. Workstation scans must be performed on at least an annual basis.

10.2.2. Server scans must be performed on at least a monthly basis.

10.2.3. New or modified servers must be scanned, and security vulnerabilities remediated before being connected to the network.

10.2.4. Vulnerabilities discovered on existing systems must be remediated within at least 30 days of discovery.

10.2.5. Discovered vulnerabilities shall be assigned a risk ranking such as High, Medium, and Low.

10.2.5.1. High rated vulnerabilities must be patched/remediated within 24 hours.

10.2.6. All Application, Service and Systems must be scanned, and security vulnerability remediated prior to product deployment and/or external exposure.

10.3. Vulnerability Assessment

10.3.1. Vulnerability assessments must be performed on at least an annual basis.

10.3.2. Vulnerability assessments on production systems must include a communication plan with said system owners.

10.3.3. Vulnerability assessments may only be managed by the City of San Diego Cyber Security Team.

10.3.4. The City of San Diego Cyber Security Team reserves the right to perform vulnerability assessments at any time without notice to end users.

11. Configuration Management

11.1. Governance

11.1.1. New or significant changes to systems must go through the Department of Information Technology governance process and be approved by the City of San Diego Cyber Security Team.

11.1.1.1. This includes the following:

11.1.1.2. New service or product including new module implementation.

11.1.1.3. New system feature implementation.

11.1.1.4. Application upgrades greater than n-1.

11.1.2. Changes that may impact security of City systems need to be approved by the City of San Diego Cyber Security Team prior to being made.

11.2. Change Management

11.2.1. Changes to enterprise-wide systems must go through the City's Change Management process.

11.2.2. Changes that result in significant security risks, as designated by the City of San Diego Cyber Security Team, must be rolled back immediately or otherwise mitigated.

11.2.3. Changes intended to remediate significant security risks, as designated by the City of San Diego Cyber Security Team, must be made "Urgent" or "Emergency" changes.

11.3. Configuration Modifications

11.3.1. Configuration modifications that do not qualify for change management must be documented and include communications to stakeholders.

11.3.2. Configuration modifications that result in significant security risk, as designated by the City of San Diego Cyber Security Team, must be rolled back immediately.

12. Log Management and Monitoring

12.1. Security Information and Event Management

12.1.1. Systems storing or transferring Protected data must have logs that permit traceability.

12.1.1.1. Said logs must have a retention policy of at least 90 days.

12.1.2. Security, audit, and activity logs must be sent to the City's Security Information Event Management (SIEM) tool.

13. Malware Defenses

13.1. Endpoint Protection

13.1.1. City-owned workstations, mobile devices and servers must have City-standard Anti-Virus and Endpoint Detection and Response agents installed and running.

13.1.1.1. City-standard Anti-Virus and Endpoint Detection and Response agents are determined by the City of San Diego Cyber Security Team.

13.1.2. If a device does not have endpoint protection such as Anti-virus or Advance Endpoint protection it may be removed from the City's Network.

14. Network Management

14.1. External Connections to City Network

14.1.1. External connections and any modifications to the City's network must be explicitly approved by the City of San Diego Cyber Security Team prior to being activated.

14.2. Remote Access

14.2.1. Remote access to the City's network must be explicitly approved by the City of San Diego Cyber Security Team prior to use.

14.2.1.1. Client VPN connections are required for remote access.

14.2.1.2. VPN for non-City employees requires City sponsorship from an appointing authority or higher.

14.2.1.3. Site-to-site VPN connections with the City's network are not permitted.

14.2.2. Remote access authentication and access logs must be monitored.

14.2.3. Individual remote access sessions must not exceed 24 hours.

14.2.4. User are not permitted to access the City's network, systems or service from outside of the USA without formal approval from the City of San Diego Cyber Security Team.

14.2.5. The City of San Diego Cyber Security Team reserves the right to revoke remote access at any time.

14.3. Domain Name System

14.3.1. Changes to the City's external DNS records must be approved by the City of San Diego Cyber Security Team.

14.3.2. New internal or external DNS zones must be approved by the City of San Diego Cyber Security Team.

14.3.3. DNS records inoperative for 30 or more days must be removed promptly.

14.4. Network Equipment

14.4.1. Network equipment on the City's network must be approved by the City of San Diego Cyber Security Team and installed and configured by the City of San Diego Network Team.

14.4.2. Different parts of the City defined by unique functions and/or data must be logically segmented.

14.5. DMZ

14.5.1. Any new systems or services as well as all changes to the City's DMZ environment must be explicitly approved by the City of San Diego Cyber Security Team, in advance of being implemented.

14.5.2. External services connecting internal web services, APIs, and web applications shall use reverse proxies.

14.5.3. Reverse Proxy Standards

14.5.3.1. Must use modern encryption methodologies (such as TLS 1.2)

14.5.3.2. All URLs shall be case-insensitive, this shall not be achieved via redirect.

14.5.3.3. All subdomains must have a separate SSL certificates for that subdomain, and must not use the wildcard sandiego.gov certificate (IE *.sandiego.gov not allowed, {subdomain}.sandiego.gov)

14.5.3.4. Proxies shall be Linux and Apache based

14.5.3.5. Remote Administrators and user connections to proxy via SSH or other remote access protocol shall not be accessible from outside of SANNET.

14.5.3.6. Only port 443 with HTTPS shall be allowed to connect to a proxy from outside of SANNET.

14.6. Firewall Rules

14.6.1. Firewall rule changes must be explicitly approved by the City of San Diego Cyber Security Team prior to implementation.

15. Media Disposal

15.1. Document Shredding

15.1.1. The disposal of all business-related paper documents which contain Protected data must involve cross-cut or 'confetti' shredding.

15.2. Computer Destruction

15.2.1. Computers or external storage devices no longer needed must have their storage drives erased or overwritten. Using secure data destruction technologies (either physical or via software "wiping").

16. Data Protection

16.1. Data Classification

16.1.1. Confidential – The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions, result in major damage to organizational assets, result in major financial loss, or result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries. Examples include but are not limited to:

16.1.1.1. Health Insurance Portability and Accountability Act (HIPAA) data

16.1.1.2. Protected Health Information (PHI)

16.1.1.3. California Law Enforcement Telecommunication System(CLETS)

16.1.1.4. Attorney–client data

16.1.1.5. Payment Card Industry (PCI)

16.1.1.6. Personally Identifiable Information (PII)

16.1.1.7. City IT system data

16.1.1.8. Per California Assembly Bill No. 375, now know as the California Consumer Privacy Act, vendors must be pursuing compliance or be compliant with this bill.

16.1.2. Private – The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced, result in significant damage to organizational assets, result in significant financial loss, or result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries. Examples include but are not limited to:

16.1.2.1. Financial Reports

16.1.2.2. Audit Reports

16.1.2.3. Configuration files

16.1.3. Sensitive (FOUO) – The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced, result in minor damage to organizational assets, result in minor financial loss, or result in minor harm to individuals. Examples include but are not limited to:

16.1.3.1. Sensitive Emails

16.1.3.2. Draft Documents

16.1.3.3. Contract Evaluations

16.1.4. Protected – Sensitive, Private or Confidential data as defined above.

16.1.5. Public – The loss of confidentiality, integrity, or availability could be expected to have a minimal effect on organizational operations, organizational assets, or individuals only to the degree that data might have been exposed in a manner not initially intended. This includes the following:

16.1.5.1. Data that has been explicitly approved for public release by an appropriate authority

16.2. Data Storage and Transfer

16.2.1. Data classified as Protected must be clearly marked as such.

16.2.2. Different types and classifications of data must be logically segregated.

16.2.3. Data must be automatically backed up on a continual basis.

16.2.3.1. Backups must be tested on at least a biannual basis.

16.2.4. Data stored or transmitted by the City of San Diego or on the behalf of the City must be encrypted at rest and in transit.

16.2.4.1. Data must be encrypted utilizing an approved cypher at 256 bits or higher.

16.2.5. The location of any data at rest must be shared with the City of San Diego Cyber Security Team.

16.2.6. Data leaving the City of San Diego's intranet must be approved by the City of San Diego Cyber Security Team prior to being shared or exposed.

16.2.7. All applications, systems, and services with the capability to share with 3rd parties must be reviewed and approved by the City of San Diego Cyber Security Team.

16.2.8. All new or modified data storage must be configured to allow the City's data classification and auditing tools.

16.2.8.1. A ticket must be submitted for the security team to configure the storage so that the necessary tools are compatible.

16.2.8.2. Until approval from the City of San Diego Cyber Security Team, the storage cannot be used in a production environment.

16.3. Data Access

16.3.1. Access to data must be limited to those who have job requirements facilitating the need to view it.

16.3.2. Access to data classified as Protected must have access logging.

16.3.3. Changes to data access in which the data is classified as Protected must have audit logs.

16.3.4. Sensitive data is not to leave the City environment without prior written approval by the City of San Diego Cyber Security Team.

17. Identity Access Management

17.1. Principle of Least Privilege

17.1.1. Users must be assigned 'Least Privilege access' to all data storage, applications, systems and systems access as required by their assigned work responsibilities.

17.1.2. Individuals responsible for performing system or user account administration functions shall not have the authority to approve system or user account changes.

17.1.3. Access to systems containing Protected data must be audited on at least an annual basis.

17.2. User Accounts and Access

17.2.1. Users must have a unique ID for authentication.

17.2.2. User account passwords must meet the following complexity requirements:

17.2.2.1. Passwords must be at least 12 characters

17.2.2.2. Passwords must contain characters from at least 3 of the following categories:

17.2.2.2.1. Upper-case alpha letters (A-Z)

17.2.2.2.2. Lower-case alpha letters (a-z)

17.2.2.2.3. Base-10 (Arabic) numerals (0-9)

17.2.2.2.4. The following symbols: ~,!,@,#,$,%,^,&,*,(,),-,_

17.2.2.3. Users cannot repeat their last 24 passwords

17.2.2.4. Passwords cannot contain 3 or more of the same characters in a single sequence.

17.2.3. User account passwords must expire every 90 days.

17.2.4. Non-City employee user accounts and access must be approved by the City of San Diego Cyber Security Team.

17.2.5. User account access must be revoked immediately when a user no longer requires said access.

17.2.6. Account and access provisioning and deprovisioning procedures for City systems must be documented.

17.2.7. San Diego Cyber Security Team requires access to any City system upon request.

17.3. Applications and Services

17.3.1. Authentication credentials must be encrypted in transit using modern encryption methodologies.

17.3.2. Audit logs must be maintained and made available to the City of San Diego Cyber Security Team.

17.3.3. Administrative logins and actions must be monitored, log and sent the City's SIEM.

17.3.4. Access must be regularly audited on at least an annual basis by the application owner.

17.3.5. User Access to applications shall follow the model of least privileged access

17.3.5.1. Users shall not have access that is higher than their responsibilities require.

17.3.5.2. Users shall not have access to data not required by work responsibilities.

17.3.5.3. When users change job roles, function or responsibilities their user access must be reviewed and changed to their new responsibilities.

17.3.5.4. Departments are responsible for notifying the City of San Diego Cyber Security Team and other stakeholders of changes to users' responsibilities, roles or functions within 24 hours.

17.3.6. Applications or Services are not permitted to connect directly to the Active Directory LDAP from outside of City's Internal Network.

17.3.7. Simple authentication shall not be used with City applications or Services.

17.3.8. Web applications and Services must be authenticated to through the City's Single Sign-on solution with Security Assertion Markup Language version 2.0 (SAML 2.0) or higher.

17.3.9. Services or Applications that are available outside of the City Internal Network that contain Protected data must have at least 2-factor authentication setup.

17.3.10. Applications or Services that have Administrative activities that are accessible from outside of the City's internal network must require admin users use 2-factor authentication.

18. Service Accounts

18.1. Service accounts must have a documented owner and description.

18.1.1. The owner will be responsible for managing the account and will serve as the primary point of contact for the account.

18.1.2. The description should entail what the account will be used for.

18.2. Service accounts may only have a single application or service use.

18.3. Service accounts must not have the ability to perform interactive logins.

18.3.1. Service accounts must not have normal user login abilities enabled.

18.4. Service account passwords must expire every 180 days.

18.5. Service accounts cannot have domain administrator permissions.

18.6. Service accounts must only be shared with users who are responsible for the account.

18.7. Service accounts must be audited on at least an annual basis.

19. Key Management

19.1. Cryptographic keys (hereby referred to as "key" or "keys") and key access must be audited on at least an annual basis.

19.2. City access keys must be centrally managed and maintained by the City of San Diego Cyber Security Team.

19.3. Key access must be logged and monitored.

19.4. Keys must have an expiration date that is no greater than 2 years from the creation date.

20. Security Awareness and Training

20.1. Cyber Security Training

20.1.1. Cryptographic keys and key access must be audited on at least an annual basis.

20.1.2. City access keys must be centrally managed and maintained by the City of San Diego Cyber Security Team.

21. Application Software Security

21.1. Software Development Lifecycle

21.1.1. Production systems must have at least one mirrored non-production system.

21.1.2. Non-production and production environments must be logically separated.

21.1.3. Only system administrators may move software from non-production to production.

21.2. Software Updates

21.2.1. Software must be no more than 1 version behind the current security patch level.

21.2.2. Software patches labeled critical by the software vendor must be applied within 24 hours of release.

21.2.3. Applications must be built on a supported platform that receives regular security updates.

21.2.4. Software must be developed with modules, packages, APIs, SDKs, and/or libraries that receive regular security updates.

21.2.5. Software modules, packages, APIs, SDKs, and/or libraries must be updated within 30 days of a security update release.

21.2.6. Software must be able to run on no more than 1 major version behind the latest host operating system release version, web browser, firmware or workstation operating System.

22. Cloud Providers and Services

22.1. Cloud Service Solutions

22.1.1. Cloud tenants must be securely architected using industry standards.

22.1.2. Cloud solutions must rest on the City's standard tenant.

22.1.3. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) solutions must be proposed to and approved by the City of San Diego Cyber Security Team during planning and prior to being implemented.

22.1.3.1. Proposals must include documentation which shall be created and maintained by the proposing entity. At minimum, documentation should include the following information:

22.1.3.1.1. Network Diagrams

22.1.3.1.2. Access Lists

22.1.3.1.3. Firewall Rules

22.1.3.1.4. IAM Information

22.1.3.1.5. Data Classification Usage

22.1.3.1.6. Overall Security Plan

22.1.3.2. Modifications to documentation presented at time of proposal must be recorded and approved by the City of San Diego Cyber Security Team during planning and prior to being implemented.

22.1.4. The City of San Diego Cyber Security Team shall receive and retain root administrative access to any cloud hosting services.

22.1.5. The City of San Diego Cyber Security Team shall receive and retain full read access to real-time logs of any PaaS or SaaS systems.

23. Incident Response and Management

23.1. Reporting Policies

23.1.1. User reports must be discrete and will be classified as Confidential data.

23.1.2. Users must comply and cooperate with the City of San Diego Cyber Security Team during an incident relevant to their system(s).

23.1.3. Any attempt to interfere with, prevent, obstruct or dissuade an employee or other user in their efforts to report potential security-related concerns is strictly prohibited.

23.1.4. Any attempt to destroy incident related materials is strictly prohibited.

23.2. User Responsibilities

23.2.1. Supervisors must report subordinates believed to be potential security risks to their Information Security Liaison and the City of San Diego Cyber Security Team in a timely manner.

23.2.2. Users must report theft, loss or unauthorized disclosure of City of San Diego Protected data to their Information Security Liaison and the City of San Diego Cyber Security Team in a timely manner.

23.2.3. Users must report unauthorized access to physical areas housing Protected data to their Information Security Liaison and the City of San Diego Cyber Security Team in a timely manner.

23.2.4. Users must report identified system flaws, misconfigurations or vulnerabilities to their Information Security Liaison and the City of San Diego Cyber Security Team immediately.

23.2.5. Users must report anomalous or suspicious activities to their Information Security Liaison and the City of San Diego Cyber Security Team immediately.

23.2.6. Users must report lost or stolen devices to their Information Security Liaison and the City of San Diego Cyber Security Team immediately.

23.2.7. Users must send suspicious emails as an attachment to anti-spam@sandiego.gov.

23.2.8. Users found to be involved in or associated with incidents must retake the Cyber Security Training.

23.3. Incident Management

23.3.1. Incident information is classified as Confidential data and must be handled and protected as such.

23.3.1.1. Incident information is distributed at the sole discretion of the City of San Diego Cyber Security Team.

23.3.2. Incident priority levels are determined and modified at the sole discretion of the City of San Diego Cyber Security Team.

23.3.3. Incident management standard operating procedures must be reviewed on at least an annual basis.

23.4. Incident Response Plan

23.4.1. The Incident Response Plan shall be maintained by the City of San Diego Cyber Security Team.

23.4.2. The Incident Response Plan shall be reviewed on at least an annual basis.

23.4.3. The Incident Response Plan shall be tested as follows:

23.4.3.1. Incident Response Team will engage in a tabletop exercise that would simulate the appropriate response to a theoretical Cyber Security Incident on at least an annual basis.

23.4.3.2. Designated staff will participate in any testing of the Incident Response Plan at the discretion of the City of San Diego Cyber Security Team.

23.4.4. Further detail can be found in the Incident Response Plan document.

24. Compliance

24.1. Legal Requirements

24.1.1. The City shall conduct or cause to be conducted, at least annually, a formal compliance audit of the information security controls for those information and communications systems which are governed by state or federal laws or regulations.

24.1.2. City records and other information assets shall be protected from loss, destruction, tampering or falsification by following the City Clerk's policies and procedures, and applicable statutes, by implementing information security controls and measures commensurate with the security classification of such information.

24.1.3. By using City information systems, Individuals acknowledge that any information they store on City systems will be released to law enforcement when appropriate or when subpoenaed.

24.2. Compliance Policies

24.2.1. Policies relevant to specific compliance regulations shall be created and maintained in separate documents by the City of San Diego Cyber Security Team.

25. References

25.1. External Resources

25.1.1. https://www.cisecurity.org/controls/

25.1.2. https://www.sans.org/security-resources/policies

25.2. Internal Resources

25.2.1. https://citynet.sandiego.gov/it/services/it-security

25.2.2. https://www.sandiego.gov/humanresources/resources/ar

Appendices

Appendix A – Security Objectives

Objective	Definition	Effect
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.	The unauthorized modification or destruction of information.
Availability	Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system.

Appendix B - Contacts

Cyber Security Team

Role	Name	Email	Primary Phone
Chief Information Security Officer	Darren Bennett	dbennett@sandiego.gov	(619) 533-4840
Deputy CISO	Jim Luther	jfluther@sandiego.gov	(619) 533–3419
Cyber Security Architect	Kyle Smith	smithk@sandiego.gov	(619) 533–3413
Senior Cyber Security Engineer	Ryan Ermert	rermert@sandiego.gov	(619) 533-3418
Cyber Security Engineer	Jonathan Mui	jmui@sandiego.gov	(619) 533-3020
Cyber Security Compliance	Rebecca Trott	rtrott@sandiego.gov	(619) 236-7212
Cyber Operations Manager	John Bortscheller	jnbort@sandiego.gov	(619) 533-4807
User Account Administrator	Kamal Scott	kscott@sandiego.gov	(619) 533-4886
Information Systems Analyst	Matthew Alger	malger@sandiego.gov	(619) 533-3489

Exhibit I

DELETED.

EXHIBIT J

PRODUCT USAGE TERMS

These Use Terms, including Product-Specific Terms included in this document, apply to Software Product(s) licensed to User by Hexagon pursuant to the EULA, including any version of EULA that is part of any other agreement between User and Hexagon that references the Use Terms. Some Product-Specific Terms for Software Products sublicensed to User by Hexagon do not modify the EULA, but instead supersede the EULA and are identified as such. Separately, other product terms included herein are for software products sold by Hexagon, but not licensed to user by Hexagon.

1.0 PRODUCT USAGE POLICY

1.1 DEFINITIONS. As used in the Use Terms, the following terms are defined as follows, and other capitalized terms set forth in the EULA shall have the meaning ascribed to them in the EULA:

1.1.1. "Auxiliary System License" means a license(s) of Software Product made available by Hexagon for select Software Products to augment Production System Licenses. Each Auxiliary System License requires a corresponding Production System License and the term of the Auxiliary System License shall not exceed the term of the applicable Production System License.

1.1.2. "Client" means computing devices connected to a Server

1.1.3. "Core" means a physical processor on a computer server that can respond to and execute the basic instructions that drive the computer. A Central Processing Unit (CPU) may have one or more Cores, and a given server may have multiple CPU sockets that may each contain multiple Cores.

1.1.4. "Production System License" means the license(s) of Software Product provided to User for general production use.

1.1.5. "Product-Specific Terms" modify or supersede the EULA, and (ii) in the event of a conflict between the EULA and Product-Specific Terms, Product-Specific Terms shall govern for the applicable Software Product. In the event of a conflict of terms between the EULA, any prior Product-Specific Terms (including any product-specific terms delivered in the form of an addendum to the EULA), and these Product-Specific Terms, these Product-Specific Terms shall take precedence over the EULA and any prior Product-Specific Terms regarding the subject Software Product.

1.1.6. "Server-based Software Product" means server-based software that is accessed by one or more Clients.

1.1.7. "XML Files" means the XML (Extensible Markup Language) files generated by the Software Product, where applicable.

1.1.8. "XSL Stylesheets" means the XSL (Extensible Stylesheet Language) presentation of a class of XML Files which, when included with the Software Product, describe how an instance of the class is transformed into an XML (Extensible Markup Language) document that uses the formatting vocabulary.

2.0 LICENSING METRICS. Software Products are licensed as either Production System Licenses or Auxiliary System Licenses. There are two (2) types of Production System Licenses and six (6) types of Auxiliary System Licenses as described below. Depending on User's license, a license may be used in either Concurrent-Use mode or Node-Locked mode. If an electronic license manager tool is incorporated in the Software Product, the license type will be verified by the Hexagon license system. If not otherwise indicated, User's Client license type and mode will be a Concurrent-Use Production System License. Each license of the Software Product is subject to the EULA, Use Terms, and Order Documents.

2.1 Production System Licenses are identified, and applicable terms described, below:

2.1.1 Concurrent-Use mode (CC) a type of Client license that allows for the checking in and checking out of the total available licenses of the Software Product for Users. At any point, User may run as many copies of the Software Product as User has Client licenses. If the Software Product is enabled

to be run in a disconnected mode, as set forth in the Installation Guide, a User may check out a license from the System for disconnected use, thus reducing the total number of licenses available in the license pool until the license is checked back in to the System. User is responsible for assuring the number of Users using the Software Product concurrently does not exceed the number of licenses User has purchased. User consents to the use of a license mechanism, license files, hardware keys, and other security devices in connection with the Software Product.

2.1.2 Node-Locked mode (NL) a type of license that allows a single copy of either a Client or Server-based Software Product Software Product to be stored on a hard disk and loaded for execution on a single designated workstation, device, or server.

2.2 Auxiliary System Licenses are identified, and applicable terms described, below:

2.2.1 Passive Disaster Recovery License (BCK) is licensed solely for temporary use when manual switchover of the Software Product to the Auxiliary System License is required in the event of failure of the Production System License. This license may be used in the production system only during the period of failure of the Production System Licenses.

2.2.2 Development System License (DEV) is a license of a Server-based Software Product that is delivered solely in connection with the Production System License of such Software Product for the purposes of developing and testing User's website built only with the Software Product. Development System Licenses shall not be used for production purposes (i.e. a fully deployed website).

2.2.3 Active Disaster Recovery License (RDT) is licensed solely for temporary use when automatic switchover of the Software Product to the Auxiliary System License is required in the event of failure of the Production System License. This license may be used in the production system only during the period of failure of the Production System License.

2.2.4 Test System License (TST) is licensed solely for testing and development purposes. Test licenses may not be used for training purposes.

2.2.5 Training System License (TRN) is licensed solely for training purposes.

2.2.6 Load Balancing License (LOB) is licensed solely to distribute the traffic evenly among multiple servers.

3.0 RIGHTS AND LIMITATIONS.

3.1 THE FOLLOWING ARE PERMITTED FOR USER'S LICENSE:

3.1.1 Unless otherwise stated in the Installation Guide, for Software Products that are delivered with an Application Programming Interface ("API") and/or configuration set-up, User may use the API(s) to write User's own extensions to the Software Products, and User may use configuration setup to configure the Software Product, but only to the extent permitted by the API(s) and/or configuration setup. Insofar as Hexagon does not transfer to User any rights in its Intellectual Property (as that term is defined in Exhibit E) by allowing User to write User's own extensions using the API(s) or to configure the software via the configuration set-up, User hereby agrees and acknowledges that Hexagon retains all rights in its Software Product, API(s), and configuration setup. Hexagon does not make any representations or warranties with respect to such extensions and/or configurations and to the maximum extent permitted by applicable law, Hexagon and its suppliers disclaim all warranties, either express or implied, relating to such extensions and/or configurations, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, high risk use, and non-infringement. User's use of such extensions and/or configurations is solely at User's own risk, and subject to applicable law, User hereby agrees to indemnify and hold harmless Hexagon and its suppliers with respect to such extensions and/or configurations.

3.1.2 For Server-based Software Product(s):

(i) User may run multiple Websites and provide multiple Webservices to User's client users with a single license provided all websites and webservices reside on the licensed server.

(ii) User may load a Server-based Software Product on

multiple machines within a cluster that is acting as a single web server, provided User has obtained the applicable number of licenses or number of Cores from Hexagon, and the total number of Cores deployed do not exceed the quantity licensed.

(iii) User may not use the Software Product's java script code for any purpose other than the application for which it was written.

(iv) Unless otherwise stated in the Installation Guide, for Software Products which contain XSL Stylesheets for presenting XML Files, User may only use the XSL Stylesheets and derivative works thereof for the purpose of presenting XML Files and derivative works thereof (collectively, "XML Products") for User's enterprise. User may not distribute the XSL Stylesheets or XML Products on a stand-alone basis. XSL Stylesheets may not be used in the production of libelous, defamatory, fraudulent, lewd, obscene or pornographic material, or any material that infringes upon any third party intellectual property rights, or otherwise in any illegal manner. All XSL Stylesheets supplied with the Software Product are and will remain the property of Hexagon.

3.2 THE FOLLOWING ARE PROHIBITED FOR USER'S LICENSE:

3.2.1 For a Software Product that is Node-Locked:

User may not allow the Software Product to be used by multiple Users on a single workstation at the same time; provided, however, if a Node-Locked license with remote access allows uncounted clients to connect to the application server, that does not count number of connections.

3.2.2 For Server-based Software Product:

(i) User may not use the Server-based Software Product to operate software as a service or hosting without the prior written consent of Hexagon.

(ii) User may not, and User may not authorize or allow anyone else to, use the Developer's License for production purposes (i.e., a fully-deployed website).

4.0 DELETED.

5.0 PRODUCT-SPECIFIC TERMS. Product-Specific Terms are applicable to User if User has licensed from Hexagon Software Product(s) identified in this section.5.0.

5.1 Product-Specific Terms That Modify the EULA
One or more of the following addenda (evidenced by the following hyperlinks) shall be applicable to Customer in the event that certain Software Products provided to Customer also make use of the products identified in such addenda.

I/Map Editor for ArcGIS If User has obtained I/Map Editor for ArcGIS, this addendum ("Addendum") is applicable to User. With regard only to I/Map Editor for ArcGIS, (i) this Addendum modifies the End User License Agreement or other applicable software license agreement ("EULA") between User and Intergraph Corporation doing business as Hexagon Safety & Infrastructure ("Hexagon") related to I/Map Editor for ArcGIS, and (ii) in the event of a conflict between the EULA and this Addendum, this Addendum shall govern specifically with regard to I/Map Editor for ArcGIS. The EULA and this Addendum together constitute the "License" applicable to I/Map Editor for ArcGIS. Hexagon grants to User a license and permission to use, copy, and reproduce the Esri Character Marker Symbol font files taken from a licensed copy of Esri's ArcGIS Desktop software to use in Hexagon's Intergraph I/CAD product suite for User's own internal use. For clarification, User may distribute the Character Marker Symbol font files to User's

workstations, servers, tablets, and/or mobile devices that contain a copy of the I/Map Editor for ArcGIS-created .MAP file solely for the purpose of properly rendering the map. No other use of the Esri Character Marker Symbol font file is permitted.

SCHEDULE 1

LIST OF SOFTWARE PRODUCTS AS OF THE EFFECTIVE DATE

Part #	Product Description	Qty
IPS0001HA	I/Executive for High Availability	1
IPS0001HABCK	I/Executive for High Availability - Backup License	1
IPS0001HATRN	I/Executive for High Availability - Training License	1
IPS0001HATST	I/Executive for High Availability - Test License	1
IPS0002	I/Dispatcher CC	71
IPS0002TRN	I/Dispatcher CC - Training License	10
IPS0002TST	I/Dispatcher CC - Test License	11
IPS0004	I/Informer CC	1
IPS0004BCK	I/Informer CC - Backup License	1
IPS0004CAC	I/CAD Message Ste for CA State Switch CC	1
IPS0004RDT	I/Informer CC - Redundant License	1
IPS0008	I/Push To Talk NL	1
IPS0008BCK	I/Push To Talk NL - Backup License	1
IPS0008RDT	I/Push To Talk NL - Redundant License	1
IPS0009	I/Mobile Data Terminal NL	2
IPS0009BCK	I/Mobile Data Terminal NL - Backup License	2
IPS0009RDT	I/Mobile Data Terminal NL - Redundant License	2
IPS0009TRN	I/Mobile Data Terminal NL - Training License	1
IPS0009TST	I/Mobile Data Terminal NL - Test License	1
IPS0012	I/Page NL	1
IPS0012BCK	I/Page NL - Backup License	1
IPS0012RDT	I/Page NL - Redundant License	1
IPS0012TRN	I/Page NL - Training License	1
IPS0015	I/Tracker - I/CAD NL	2
IPS0015BCK	I/Tracker - I/CAD NL - Backup License	2
IPS0015RDT	I/Tracker - I/CAD NL - Redundant License	2
IPS0015TRN	I/Tracker - I/CAD NL - Training License	1
IPS0015TST	I/Tracker - I/CAD NL - Test License	1
IPS0035NC	I/Backup - (No Charge)	2
IPS0042I	I/NetViewer CC	150
IPS0042IBCK	I/NetViewer CC - Backup License	150
IPS0042ITRN	I/NetViewer CC - Training License	150
IPS0042ITST	I/NetViewer CC - Test License	150
IPS0051	I/CADLink CC	1
IPS0051BCK	I/CADLink CC - Backup License	1
IPS0051RDT	I/CADLink CC - Redundant License	1
IPS0051TST	I/CADLink CC - Test License	1
IPS0080	Mobile for Public Safety CC	400
IPS0082	Map Administration Utility CC	1

IPS1163	I/Map Editor CC	1
IPS3042	Xalt Runtime Engine NL	1
IPS3042-BCK	Xalt Runtime Engine NL - Backup License	1
IPS3042-RDT	Xalt Runtime Engine NL - Redundant License	1
IPS3042-TRN	Xalt Runtime Engine NL - Training License	1
IPS3042-TST	Xalt Runtime Engine NL - Test License	1
GSPX5007	GeoMedia Professional CC	1
IPSCUSTOM03	I/Informer to CLETS/NCIC	1
IPSCUSTOM03	Alarm Interface (I/ABL-CryWolf)	1
IPSCUSTOM03	Interface for LOI(Mobile) Requirements	1
IPSCUSTOM03	Interface for Dashboard Functionality	1
IPSCUSTOM03BCK	I/Informer to CLETS/NCIC - Backup License	1
IPSCUSTOM03BCK	Alarm Interface (I/ABL - CryWolf) - Backup License	1
IPSCUSTOM03BCK	Interface for LOI (Mobile) Requirements - Backup License	1
IPSCUSTOM03BCK	Interface for Dashboard Functionality - Backup License	1
IPSCUSTOM03RDT	I/Informer to CLETS/NCIC-Reduntant License	1
IPSCUSTOM03RDT	Alarm Interface (I/ABL - CryWolf) - Redundant License	1
IPSCUSTOM03RDT	Interface for LOI (Mobile) Requirements - Redundant License	1
IPSCUSTOM03RDT	Interface for Dashboard Functionality - Redundant License	1
IPSCUSTOM04	Auto Returns Interface	1
IPSCUSTOM04	EdgeFrontier Interface for Juvenile/Adult Missing Persons	1
PSA1026	Axon CAD EF Interface	1
EFCUSTOM16	EdgeFrontier Aero Computers Moving Map Interface	1
**EFCUSTOM16	EdgeFrontier Interface to CRMS	1
EFCUSTOM16	EdgeFrontier Omega Dashboard Interface	1
EFCUSTOM16	EdgeFrontier ARJIS Interface	1
EFCUSTOM16	EdgeFrontier GIS Data Layer Interface	1
**EFCUSTOM16	EdgeFrontier for NextGen Incident Command Sys Interface	1
EFCUSTOM16BCK	EF Aero Computers Moving Map Interface - Bckup Lic	1
EFCUSTOM16BCK	EdgeFrontier Omega Dashboard Interface - Backup License	1
EFCUSTOM16BCK	EdgeFrontier ARJIS Interface - Backup License	1
EFCUSTOM16BCK	EdgeFrontier GIS Data Layer Interface - Backup License	1
EFCUSTOM16BCK	EdgeFrontier Interface for On Body Camera Reqs -Backup Lic	1
**EFCUSTOM16BCK	EdgeFrontier for NextGen Incident Command System Interface-Bckup Lic	1
EFCUSTOM16RDT	EdgeFrontier Omega Dashboard Interface - Redundant License	1
EFCUSTOM16RDT	EdgeFrontier ARJIS Interface - Redundant License	1
EFCUSTOM16RDT	EdgeFrontier GIS Data Layer Interface - Redundant Lic	1
EFCUSTOM16RDT	EdgeFrontier Interface for On Body Camera Req - Rdnt Lic	1
**EFCUSTOM16RDT	EdgeFrontier for NextGen Incident Comm Sys Intrfce - Rdnt Lic	1
EFCUSTOM16RDT	EF Aero Computers Moving Map Interface-Rdndnt Lic	1

Third Party SW

****7NQ-00853	Microsoft SQL Server 2016 Std Edition Full-Use - 2 Core Pack	1
**IPS21179C	Intergraph Business Intelligence Direct - CAD Bundle 10 NUL	1
**IPS21006C	Intergraph Business Intelligence Direct - CAD Bundle 10 NUL	1
**IPS21006TSTC	Intergraph Business Intelligence Direct - CAD Bundle 10 NUL	1
**IPS21048C	Intergraph Business Intelligence Direct - CAD Bundle 10 NUL	1
****7LQ-00001	Microsoft SQL Server 2012 ENT Edition RUNTIME - 2 core pack	26
****7RQ-00003	Microsoft SQL Server 2012 STD Edition RUNTIME - 2 core pack	1

SCHEDULE 2

PRICING FOR ORDERS 1 (MAINTENANCE SERVICES) AND 2 (RSA SERVICES)

The following reflects the pricing for Maintenance Services for the Covered Products listed in Schedule 1 hereto except for those Software Products denoted with "**" for the following periods. The products denoted with "**" will not be included in this Order for Maintenance Services. The products denoted with "*****" will be included in this Order for Maintenance Services for Year 1 and are then intended to be upgraded to MS SQL 2019 following Year 1. Pricing for Maintenance Services is subject to change if the Customer purchases additional Software and desires to include them in the Order for Maintenance Services, updates third party software, or otherwise changes the composition of the System.

ORDER 1 MAINTENANCE SERVICES	
YEAR 1 (Nov. 1, 2020 – Oct. 31, 2021)	$596,578.56
YEAR 2 (Nov. 1, 2021 – Oct. 31, 2022)	$672,723.48
YEAR 3 (Nov. 1, 2022 – Oct. 31, 2023)	$745,907.76
YEAR 4 (Nov. 1, 2023 – Oct. 31, 2024)	$783,204.36
YEAR 5 (Nov. 1, 2024 – Oct. 31, 2025)	$822,371.88

The following reflects the pricing for RSA services as described in the SOW for RSA services.

ORDER 2 Resident System Administrator Services	
YEAR 1 (Oct 18, 2020- Oct 17, 2021)	$286,377
YEAR 2 (Oct 18, 2021- Oct 17, 2022)	$294,968
YEAR 3 (Oct 18, 2022- Oct 17, 2023)	$303,817
YEAR 4 (Oct 18, 2023- Oct 17, 2024)	$312,932
YEAR 5 (Oct 18, 2024- Oct 17, 2025)	$322,320

City of San Diego

CONTRACTOR STANDARDS

Pledge of Compliance Attachment II

The City of San Diego has adopted a Contractor Standards Ordinance (CSO) codified in section 22.3004 of the San Diego Municipal Code (SDMC). The City of San Diego uses the criteria set forth in the CSO to determine whether a contractor (bidder or proposer) has the capacity to fully perform the contract requirements and the business integrity to justify the award of public funds. This completed Pledge of Compliance signed under penalty of perjury must be submitted with each bid and proposal. If an informal solicitation process is used, the bidder must submit this completed Pledge of Compliance to the City prior to execution of the contract. All responses must be typewritten or printed in ink. If an explanation is requested or additional space is required, Contractors must provide responses on Attachment A to the Pledge of Compliance and sign each page. Failure to submit a signed and completed Pledge of Compliance may render a bid or proposal non-responsive. In the case of an informal solicitation or cooperative procurement, the contract will not be awarded unless a signed and completed Pledge of Compliance is submitted. A submitted Pledge of Compliance is a public record and information contained within will be available for public review except to the extent that such information is exempt from disclosure pursuant to applicable law.

By signing and submitting this form, the contractor is certifying, to the best of their knowledge, that the contractor and any of its Principals have not within a five (5) year period – preceding this offer, been convicted of or had a civil judgement rendered against them for commission of a fraud or a criminal offense in connection with obtaining, attempting to obtain or performing a public (Federal, State or local) contract or subcontract.

"Principal" means an officer, director, owner, partner or a person having primary management or supervisory responsibilities within the firm. The Contractor shall provide immediate written notice to the Procurement Contracting Officer handling the solicitation, at any time prior to award should they learn that this Representations and Certifications was inaccurate or incomplete.

This form contains 10 pages, additional information may be submitted as part of *Attachment A.*

A. BID/PROPOSAL/SOLICITATION TITLE:

Computer Aided Dispatch Support

B. BIDDER/PROPOSER INFORMATION:

Intergraph Corporation		Hexagon Safety & Infrastru	
Legal Name		DBA	
305 Intergraph Way	Madison	AL	35758
Street Address	City	State	Zip
Victor S. Vasile, Regional Divisional Counsel	(256) 730-1516		
Contact Person, Title	Phone	Fax	

Provide the name, identity, and precise nature of the interest* of all persons who are directly or indirectly involved** in this proposed transaction (SDMC § 21.0103). Use additional pages if necessary.

* The precise nature of the interest includes:

- the percentage ownership interest in a party to the transaction,
- the percentage ownership interest in any firm, corporation, or partnership that will receive funds from the transaction,
- the value of any financial interest in the transaction,
- any contingent interest in the transaction and the value of such interest should the contingency be satisfied, and
- any philanthropic, scientific, artistic, or property interest in the transaction.

** Directly or indirectly involved means pursuing the transaction by:

- communicating or negotiating with City officers or employees,
- submitting or preparing applications, bids, proposals or other documents for purposes of contracting with the City, or
- directing or supervising the actions of persons engaged in the above activity.

Hexagon AB	Corporation
Name	Title/Position
Stockholm, Sweden	
City and State of Residence	Employer (if different than Bidder/Proposer)
Wholly owns Intergraph Corporation	
Interest in the transaction	

Tammy Heaton	Vice President
Name	Title/Position
High Point, NC	
City and State of Residence	Employer (if different than Bidder/Proposer)
Account Management Vice President and supervisor of Daniel Tarkowski	
Interest in the transaction	

Victor Vasile	Regional Divisional Counsel
Name	Title/Position
Huntsville, AL	
City and State of Residence	Employer (if different than Bidder/Proposer)
Counsel	
Interest in the transaction	

Benjamin Ernst	Vice President and General Manager
Name	Title/Position
Columbus, OH	
City and State of Residence	Employer (if different than Bidder/Proposer)
General Manager of U.S. Public Safety and Supervisor of Tammy Heaton	
Interest in the transaction	

William Campbell	Senior Vice President, Americas
Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
SVP of North America and supervisor of Benjamin Ernst and Kristy Humaldeh	
Interest in the transaction	

Steven Cost	President
Name	Title/Position
Huntsville, AL	
City and State of Residence	Employer (if different than Bidder/Proposer)
President of Intergraph Corporation and supervisor of William Campbell	
Interest in the transaction	

Kristy Humaidah	Director
Name	Title/Position
Huntsville, AL	
City and State of Residence	Employer (if different than Bidder/Proposer)
Bids and Proposals Manager	
Interest in the transaction	

Daniel Tarkowski	Account Manager
Name	Title/Position
Huntsville, AL	
City and State of Residence	Employer (if different than Bidder/Proposer)
Account Manager for San Diego	
Interest in the transaction	

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

C. OWNERSHIP AND NAME CHANGES:

1. In the past five ten (5) years, has your firm changed its name?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to list all prior legal and DBA names, addresses, and dates each firm name was used. Explain the specific reasons for each name change.

2. Is your firm a non-profit?
   ☐ **Yes** ☑ **No**

   If **Yes,** attach proof of status to this submission.

3. In the past five (5) years, has a firm owner, partner, or officer operated a similar business?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to list names and addresses of all businesses and the person who operated the business. Include information about a similar business only if an owner, partner, or officer of your firm holds or has held a similar position in another firm.

D. BUSINESS ORGANIZATION/STRUCTURE:

Indicate the organizational structure of your firm. Fill in only one section on this page. Use Attachment A if more space is required.

☑ **Corporation** Date Incorporated: 02/02/1969 State of Incorporation: Delaware

List corporation's current officers:
President: Steven Cost
Vice Pres: Richard Blair Jacks
Secretary: Tony Zana
Treasurer:

Type of corporation: C ☐ Subchapter S ☐

Is the corporation authorized to do business in California: ☑ **Yes** ☐ **No**

If **Yes,** after what date: 08/24/1984

Is your firm a publicly traded corporation? ☐ **Yes** ☑ **No**

If **Yes,** how and where is the stock traded? _____

If **Yes,** list the name, title and address of those who own ten percent (10 %) or more of the corporation's stocks:

_____

_____

_____

_____

Do the President, Vice President, Secretary and/or Treasurer of your corporation have a third party interest or other financial interests in a business/enterprise that performs similar work, services or provides similar goods? ☐ **Yes** ☑ **No**

If **Yes,** please use Attachment A to disclose.

Please list the following:	Authorized	Issued	Outstanding
a. Number of voting shares:	_____	_____	_____
b. Number of nonvoting shares:	_____	_____	_____
c. Number of shareholders:			_____
d. Value per share of common stock:		Par	$_____
		Book	$_____
		Market	$_____

Limited Liability Company Date formed: _____ State of formation: _____

List the name, title and address of members who own ten percent (10%) or more of the company:

_____

_____

_____

_____

☐ **Partnership** Date formed: _____ State of formation: _____

List names of all firm partners:

_____

_____

_____

_____

☐ **Sole Proprietorship** Date started: _____

List all firms you have been an owner, partner or officer with during the past five (5) years. Do not include ownership of stock in a publicly traded company:

_____

_____

_____

_____

☐ **Joint Venture** Date formed: _____

List each firm in the joint venture and its percentage of ownership:

Note: To be responsive, each member of a Joint Venture or Partnership must complete a separate *Contractor Standards form.*

E. FINANCIAL RESOURCES AND RESPONSIBILITY:

1. Is your firm preparing to be sold, in the process of being sold, or in negotiations to be sold?
   ☐ Yes ☑ No

   If **Yes**, use Attachment A to explain the circumstances, including the buyer's name and principal contact information.

2. In the past five (5) years, has your firm been denied bonding?
   ☐ Yes ☑ No

   If **Yes**, use Attachment A to explain specific circumstances; include bonding company name.

3. In the past five (5) years, has a bonding company made any payments to satisfy claims made against a bond issued on your firm's behalf or a firm where you were the principal?
   ☐ Yes ☑ No

   If **Yes**, use Attachment A to explain specific circumstances.

4. In the past five (5) years, has any insurance carrier, for any form of insurance, refused to renew the insurance policy for your firm?
   ☐ Yes ☑ No

   If **Yes**, use Attachment A to explain specific circumstances.

5. Within the last five years, has your firm filed a voluntary petition in bankruptcy, been adjudicated bankrupt, or made a general assignment for the benefit of creditors?
   ☐ Yes ☑ No

   If **Yes**, use Attachment A to explain specific circumstances.

6. Are there any claims, liens or judgements that are outstanding against your firm?
   ☐ Yes ☑ No

   If **Yes**, please use Attachment A to provide detailed information on the action.

7. Please provide the name of your principal financial institution for financial reference. By submitting a response to this Solicitation Contractor authorizes a release of credit information for verification of financial responsibility.

   Name of Bank: PNC Bank, NA

   Point of Contact: Lockbox Group, Product Client Services

   Address: Pittsburgh, PA 15222

   Phone Number: (800) 824-5001

8. By submitting a response to a City solicitation, Contractor certifies that he or she has sufficient operating capital and/or financial reserves to properly fund the requirements identified in the solicitation. At City's request, Contractor will promptly provide to City

a copy of Contractor's most recent balance sheet and/or other necessary financial statements to substantiate financial ability to perform.

9. In order to do business in the City of San Diego, a current Business Tax Certificate is required. Business Tax Certificates are issued by the City Treasurer's Office. If you do not have one at the time of submission, one must be obtained prior to award.

   Business Tax Certificate No.: B2012024460 Year Issued: 2019

F. **PERFORMANCE HISTORY:**

1. In the past five (5) years, has your firm been found civilly liable, either in a court of law or pursuant to the terms of a settlement agreement, for defaulting or breaching a contract with a government agency?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

2. In the past five (5) years, has a public entity terminated your firm's contract for cause prior to contract completion?
   ☑ **Yes** ☐ **No**

   If **Yes**, use Attachment A to explain specific circumstances and provide principal contact information.

3. In the past five (5) years, has your firm entered into any settlement agreement for any lawsuit that alleged contract default, breach of contract, or fraud with or against a public entity?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

4. Is your firm currently involved in any lawsuit with a government agency in which it is alleged that your firm has defaulted on a contract, breached a contract, or committed fraud?
   ☑ **Yes** ☐ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

5. In the past five (5) years, has your firm, or any firm with which any of your firm's owners, partners, or officers is or was associated, been debarred, disqualified, removed, or otherwise prevented from bidding on or completing any government or public agency contract for any reason?
   ☐ **Yes** ☑ **No**

   If **Yes**, use *Attachment A* to explain specific circumstances.

6. In the past five (5) years, has your firm received a notice to cure or a notice of default on a contract with any public agency?

   ☑ **Yes** ☐ **No**

   If **Yes**, use Attachment A to explain specific circumstances and how the matter resolved.

7. Performance References:

Please provide a minimum of three (3) references familiar with work performed by your firm which was of a similar size and nature to the subject solicitation within the last five (5) years.

Please note that any references required as part of your bid/proposal submittal are in addition to those references required as part of this form.

Company Name: South Sound 911

Contact Name and Phone Number: Tim Hannah (253) 798-6213

Contact Email: tim.hannah@southsound911.org

Address: 945 Tacoma Ave S Tacoma, WA 98402

Contract Date: February 26, 2014

Contract Amount: $4,572,386.00

Requirements of Contract: Implementation and support of I/CAD

Company Name: Washington D.C Office of Unified Communications

Contact Name and Phone Number: Teddy Kavaleri (202) 714-3701

Contact Email: teddy.kavaleri@dc.gov

Address: 2720 Martin Luther King Jr. Ave, Washington D.C. 20032

Contract Date: June 11, 2019

Contract Amount: $3,529,836.40

Requirements of Contract: Support for I/CAD

Company Name: San Jose, CA

Contact Name and Phone Number: Judith Torrico (408) 537-1745

Contact Email: Judith.torrico@sanjoseca.gov

Address: 855 N. San Pedro St, San Jose CA 95100

Contract Date: June 28, 2016

Contract Amount: $3,541,593.32

Requirements of Contract: Support and services for I/CAD

G. COMPLIANCE:

1. In the past five (5) years, has your firm or any firm owner, partner, officer, executive, or manager been criminally penalized or found civilly liable, either in a court of law or pursuant to the terms of a settlement agreement, for violating any federal, state, or local law in performance of a contract, including but not limited to, laws regarding health and safety, labor and employment, permitting, and licensing laws?
   ☐Yes ☑No

   If **Yes**, use Attachment A to explain specific circumstances surrounding each instance. Include the name of the entity involved, the specific infraction(s) or violation(s), dates of instances, and outcome with current status.

2. In the past five (5) years, has your firm been determined to be non-responsible by a public entity?
   ☐**Yes** ☑**No**

If **Yes**, use Attachment A to explain specific circumstances of each instance. Include the name of the entity involved, the specific infraction, dates, and outcome.

H. BUSINESS INTEGRITY:

1. In the past five (5) years, has your firm been convicted of or found liable in a civil suit for making a false claim or material misrepresentation to a private or public entity?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance. Include the entity involved, specific violation(s), dates, outcome and current status.

2. In the past five (5) years, has your firm or any of its executives, management personnel, or owners been convicted of a crime, including misdemeanors, or been found liable in a civil suit involving the bidding, awarding, or performance of a government contract?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance; include the entity involved, specific infraction(s), dates, outcome and current status.

3. In the past five (5) years, has your firm or any of its executives, management personnel, or owners been convicted of a federal, state, or local crime of fraud, theft, or any other act of dishonesty?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance; include the entity involved, specific infraction(s), dates, outcome and current status.

4. Do any of the Principals of your firm have relatives that are either currently employed by the City or were employed by the City in the past five (5) years?

   ☐**Yes** ☑**No**

   If **Yes**, please disclose the names of those relatives in Attachment A.

I. BUSINESS REPRESENTATION:

1. Are you a local business with a physical address within the County of San Diego?
☐**Yes** ☑**No**

2. Are you a certified Small and Local Business Enterprise certified by the City of San Diego?
☐**Yes** ☑**No**

   Certification #_____

3. Are you certified as any of the following:
   a. Disabled Veteran Business Enterprise Certification #_____
   b. Woman or Minority Owned Business Enterprise Certification #_____
   c. Disadvantaged Business Enterprise Certification #_____

J. WAGE COMPLIANCE:

In the past five (5)years, has your firm been required to pay back wages or penalties for failure to comply with the federal, state or local **prevailing, minimum, or living wage laws?** ☐**Yes** ☑**No** If **Yes**, use Attachment A to explain the specific circumstances of each instance. Include the entity involved, the specific infraction(s), dates, outcome, and current status.

By signing this Pledge of Compliance, your firm is certifying to the City that you will comply with the requirements of the Equal Pay Ordinance set forth in SDMC sections 22.4801 through 22.4809.

K. STATEMENT OF SUBCONTRACTORS & SUPPLIERS:

Please provide the names and information for all subcontractors and suppliers used in the performance of the proposed contract, and what portion of work will be assigned to each subcontractor. Subcontractors may not be substituted without the written consent of the City. Use Attachment A if additional pages are necessary. If no subcontractors or suppliers will be used, please write "Not Applicable."

Company Name: SDI Presence, LLC

Address: 200 East Randolph, Suite 3550

Contact Name: Sharee Wolff Phone: (312) 580-7521 Email: swolff@sdipresnce.com

Contractor License No.: _____ DIR Registration No.: _____

Sub-Contract Dollar Amount: $_____ (per year) $_____ (total contract term)

Scope of work subcontractor will perform: Resident System Administrator

Identify whether company is a subcontractor or supplier: Subcontractor

Certification type (check all that apply):☐DBE ☐DVBE ☐ELBE ☐MBE ☐SLBE☐WBE ☐Not Certified

Contractor must provide valid proof of certification with the response to the bid or proposal to receive participation credit.

Company Name: _____

Address: _____

Contact Name: _____ Phone: _____ Email: _____

Contractor License No.: _____ DIR Registration No.: _____

Sub-Contract Dollar Amount: $_____ (per year) $_____ (total contract term)

Scope of work subcontractor will perform: _____

Identify whether company is a subcontractor or supplier: _____

Certification type (check all that apply):☐DBE ☐DVBE ☐ELBE ☐MBE ☐SLBE☐WBE ☐Not Certified

Contractor must provide valid proof of certification with the response to the bid or proposal to receive participation credit.

L. STATEMENT OF AVAILABLE EQUIPMENT:

A full inventoried list of all necessary equipment to complete the work specified may be a requirement of the bid/proposal submission.

By signing and submitting this form, the Contractor certifies that all required equipment included in this bid or proposal will be made available one week (7 days) before work shall commence. In instances where the required equipment is not owned by the Contractor, Contractor shall explain how the equipment will be made available before the commencement of work. The City of San

Diego reserves the right to reject any response, in its opinion, if the Contractor has not demonstrated he or she will be properly equipped to perform the work in an efficient, effective matter for the duration of the contract period.

M. **TYPE OF SUBMISSION:** This document is submitted as:

☐ Initial submission of *Contractor Standards Pledge of Compliance*

☐ Initial submission of *Contractor Standards Pledge of Compliance* as part of a Cooperative agreement

☐ Initial submission of *Contractor Standards Pledge of Compliance* as part of a Sole Source agreement

☑ Update of prior *Contractor Standards Pledge of Compliance* dated 02/14/2019.

Complete all questions and sign below.

Under penalty of perjury under the laws of the State of California, I certify that I have read and understand the questions contained in this Pledge of Compliance, that I am responsible for completeness and accuracy of the responses contained herein, and that all information provided is true, full and complete to the best of my knowledge and belief. I agree to provide written notice to the Purchasing Agent within five (5) business days if, at any time, I learn that any portion of this Pledge of Compliance is inaccurate. Failure to timely provide the Purchasing Agent with written notice is grounds for Contract termination.

I, on behalf of the firm, further certify that I and my firm will comply with the following provisions of SDMC section 22.3004:

(a) I and my firm will comply with all applicable local, State and Federal laws, including health and safety, labor and employment, and licensing laws that affect the employees, worksite or performance of the contract.

(b) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of receiving notice that a government agency has begun an investigation of me or my firm that may result in a finding that I or my firm is or was not in compliance with laws stated in paragraph (a).

(c) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of a finding by a government agency or court of competent jurisdiction of a violation by the Contractor of laws stated in paragraph (a).

(d) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of becoming aware of an investigation or finding by a government agency or court of competent jurisdiction of a violation by a subcontractor of laws stated in paragraph (a).

(e) I and my firm will cooperate fully with the City during any investigation and to respond to a request for information within ten (10) working days.

Failure to sign and submit this form with the bid/proposal shall make the bid/proposal non-responsive. In the case of an informal solicitation, the contract will not be awarded unless a signed and completed *Pledge of Compliance* is submitted.

Victor S. Vasile, Regional Divisional Counsel	V. S. V.	8/5/20
Name and Title	Signature	Date

City of San Diego
CONTRACTOR STANDARDS
Attachment "A"

Provide additional information in space below. Use additional Attachment "A" pages as needed. Each page must be signed. Print in ink or type responses and indicate question being answered.

With respect to:
Question F.2:
Intergraph's contracts with Howard County, City of Elk Grove, and Louisville/Jefferson County Metro Government were terminated in the manner described in the question. Hexagon disputes the basis for the terminations. Those customers continue to use Hexagon CAD and RMS software despite their actions. Due to confidentiality provisions included within those contracts, Intergraph is not in a position to provide additional details.

Question F.6
In addition to the circumstances listed above, Intergraph has received a notice of default and cure from the City of Westminster, Colorado; the City of Huntsville, Alabama; Fairfax County, Virginia; City of Elk Grove in relation to projects to implement WebRMS. Those projects ended for each party's convenience. The customers continue to use Intergraph's ILEADS RMS and CAD. Intergraph Corporation received notices to cure from the City of Glendale, Arizona in relation to a contract to implement WebRMS. That project was ultimately completed and the Customer uses the software. The City of Tucson issued a notice to cure in relation to a completed project to implement ILEADS RMS and CAD. The City took no further action and the City remains an Intergraph customer for CAD and ILEADS. The City of Louisville has issued a notice of default in relation to its project to implement WebRMS. Due to confidentiality provisions in those contracts and other contracts between it and its customer, Intergraph is not in a position to provide additional details.

I have read the matters and statements made in this Contractor Standards Pledge of Compliance and attachments thereto and I know the same to be true of my own knowledge, except as to those matters stated upon information or belief and as to such matters, I believe the same to be true. I certify under penalty of perjury that the foregoing is true and correct.

Victor S. Vasile, Regional Divisional Counsel		8/5/20
Print Name, Title	Signature	Date

The City of
SAN DIEGO

EQUAL OPPORTUNITY CONTRACTING (EOC)

1200 Third Avenue, Suite 200 · San Diego, CA 92101
Phone: (619) 236-6000 · Fax: (619) 236-5904

Attachment III
WORK FORCE REPORT

The objective of the *Equal Employment Opportunity Outreach Program*, San Diego Municipal Code Sections 22.3501 through 22.3517, is to ensure that contractors doing business with the City, or receiving funds from the City, do not engage in unlawful discriminatory employment practices prohibited by State and Federal law. Such employment practices include, but are not limited to unlawful discrimination in the following: employment, promotion or upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rate of pay or other forms of compensation, and selection for training, including apprenticeship. Contractors are required to provide a completed *Work Force Report (WFR).*

NO OTHER FORMS WILL BE ACCEPTED

CONTRACTOR IDENTIFICATION

Type of Contractor: ☐ Construction ■ Vendor/Supplier ☐ Financial Institution ☐ Lessee/Lessor
☐ Consultant ☐ Grant Recipient ☐ Insurance Company ☐ Other

Name of Company: Intergraph Corporation

ADA/DBA: Hexagon Safety & Infrastructure

Address (Corporate Headquarters, where applicable): 305 Intergraph Way

City: Madison County: Madison State: Alabama Zip: 35758

Telephone Number: 256-730-2000 Fax Number: _____

Name of Company CEO: Steven Cost

Address(es), phone and fax number(s) of company facilities located in San Diego County **(if different from above):**

Address: N/A

City: _____ County: _____ State: _____ Zip: _____

Telephone Number: _____ Fax Number: _____ Email: _____

Type of Business: Corporation Type of License: _____

The Company has appointed: Jay Cobb

As its Equal Employment Opportunity Officer (EEOO). The EEOO has been given authority to establish, disseminate and enforce equal employment and affirmative action policies of this company. The EEOO may be contacted at:

Address: 305 Intergraph Way, Madison, Alabama 35758

Telephone Number: 256 730-2000 Fax Number: _____ Email: jay.cobb@hexagonsi.com

---

☐ One San Diego County (or Most Local County) Work Force - Mandatory
☐ Branch Work Force *
■ Managing Office Work Force

Check the box above that applies to this WFR.

**Submit a separate Work Force Report for all participating branches. Combine WFRs if more than one branch per county.*

I, the undersigned representative of Intergraph Corporation
(Firm Name)

Madison *(County)*, Alabama *(State)* hereby certify that information provided herein is true and correct. This document was executed on this 11th day of June, 20 20

(Authorized Signature)

VICTOR S. VASICE
(Print Authorized Signature Name)

WORK FORCE REPORT – Page 2

NAME OF FIRM: Intergraph Corporalton DATE: _____

OFFICE(S) or BRANCH(ES): Madison, Alabama COUNTY: Madison

INSTRUCTIONS: For each occupational category, indicate number of males and females in every ethnic group. Total columns in row provided. Sum of all totals should be equal to your total work force. Include all those employed by your company on either a full or part-time basis. The following groups are to be included in ethnic categories listed in columns below:

(1) Black or African-American
(2) Hispanic or Latino
(3) Asian
(4) American Indian or Alaska Native
(5) Native Hawaiian or Pacific Islander
(6) White
(7) Other race/ethnicity; not falling into other groups

Definitions of the race and ethnicity categories can be found on Page 4

ADMINISTRATION OCCUPATIONAL CATEGORY	(1) Black or African American		(2) Hispanic or Latino		(3) Asian		(4) American Indian/ Nat. Alaskan		(5) Pacific Islander		(6) White		(7) Other Race/ Ethnicity	
	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)
Management & Financial	2	0	1	0	3	0	0	0	0	0	50	38	0	1
Professional	6	8	4	2	14	8	0	2	0	0	123	88	1	0
A&E, Science, Computer	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Technical	1	1	0	1	0	0	0	0	0	0	17	6	0	0
Sales	0	0	0	0	0	0	0	0	0	0	3	0	0	0
Administrative Support	0	0	0	0	0	0	0	0	0	0	0	4	0	1
Services	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Crafts	0	0	0	0	0	0	0	0	0	0	6	1	0	0
Operative Workers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Transportation	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Laborers*	0	0	0	0	0	0	0	0	0	0	0	0	0	0

*Construction laborers and other field employees are not to be included on this page

Totals Each Column	9	9	5	3	17	8	0	2	0	0	199	137	1	2

Grand Total All Employees	392

Indicate by Gender and Ethnicity the Number of Above Employees Who Are Disabled:

Disabled	0	0	0	0	0	0	0	0	0	0	8	5	0	0

Non-Profit Organizations Only:

Board of Directors														
Volunteers			N/A											
Artists														

WORK FORCE REPORT ~ Page 3

NAME OF FIRM: Intergraph Corporation DATE: _____

OFFICE(S) or BRANCH(ES): _____ COUNTY: Madison

INSTRUCTIONS: For each occupational category, indicate number of males and females in every ethnic group. Total columns in row provided. Sum of all totals should be equal to your total work force. Include all those employed by your company on either a full or part-time basis. The following groups are to be included in ethnic categories listed in columns below:

(1) Black or African-American
(2) Hispanic or Latino
(3) Asian
(4) American Indian or Alaska Native
(5) Native Hawaiian or Pacific Islander
(6) White
(7) Other race/ethnicity; not falling into other groups

Definitions of the race and ethnicity categories can be found on Page 4

TRADE OCCUPATIONAL CATEGORY	(1) Black or African American		(2) Hispanic or Latino		(3) Asian		(4) American Indian/ Nat. Alaskan		(5) Pacific Islander		(6) White		(7) Other Race/ Ethnicity	
	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)
Brick, Block or Stone Masons														
Carpenters														
Carpet, Floor & Tile Installers Finishers														
Cement Masons, Concrete Finishers														
Construction Laborers														
Drywall Installers, Ceiling Tile Inst														
Electricians														
Elevator Installers														
First-Line Supervisors/Managers														
Glaziers														
Helpers; Construction Trade														
Millwrights														
Misc. Const. Equipment Operators														
Painters, Const. & Maintenance														
Pipelayers, Plumbers, Pipe & Steam Fitters														
Plasterers & Stucco Masons														
Roofers														
Security Guards & Surveillance Officers														
Sheet Metal Workers														
Structural Metal Fabricators & Fitters														
Welding, Soldering & Brazing Workers														
Workers, Extractive Crafts, Miners														
Totals Each Column														

NONE

Grand Total All Employees 0

Indicate By Gender and Ethnicity the Number of Above Employees Who Are Disabled:

Disabled														

The City of SAN DIEGO

Work Force Report

History

The Work Force Report (WFR) is the document that allows the City of San Diego to analyze the work forces of all firms wishing to do business with the City. We are able to compare the firm's work force data to County Labor Force Availability (CLFA) data derived from the United States Census. CLFA data is a compilation of lists of occupations and includes the percentage of each ethnicity we track (American Indian or Alaska Native, Asian, Black or African-American, Native Hawaiian or Pacific Islander, White, and Other) for each occupation. Currently, our CLFA data is taken from the 2010 Census. In order to compare one firm to another, it is important that the data we receive from the consultant firm is accurate and organized in the manner that allows for this fair comparison.

Work Force & Branch Work Force Reports

When submitting a WFR, especially if the WFR is for a specific project or activity, we would like to have information about the firm's work force that is actually participating in the project or activity. That is, if the project is in San Diego and the work force is from San Diego, we want a San Diego County Work Force Report[1]. By the same token, if the project is in San Diego, but the work force is from another county, such as Orange or Riverside County, we want a Work Force Report from that county[2]. If participation in a San Diego project is by work forces from San Diego County and, for example, from Los Angeles County and from Sacramento County, we ask for separate Work Force Reports representing your firm from each of the three counties.

Managing Office Work Force

Equal Opportunity Contracting may occasionally ask for a Managing Office Work Force (MOWF) Report. This may occur in an instance where the firm involved is a large national or international firm but the San Diego or other local work force is very small. In this case, we may ask for both a local and a MOWF Report[1, 3]. In another case, when work is done only by the Managing Office, only the MOWF Report may be necessary.[3]

Types of Work Force Reports:

Please note, throughout the preceding text of this page, the superscript numbers one [1], two [2] & three [3]. These numbers coincide with the types of work force report required in the example. See below:

[1] One San Diego County (or Most Local County) Work Force – Mandatory in most cases

[2] Branch Work Force *

[3] Managing Office Work Force

**Submit a separate Work Force Report for all participating branches. Combine WFRs if more than one branch per county.*

RACE/ETHNICY CATEGORIES

American Indian or Alaska Native – A person having origins in any of the peoples of North and South America (including Central America) and who maintains tribal affiliation or community attachment.

Asian – A person having origins in any of the peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.

Black or African American – A person having origins in any of the Black racial groups of Africa.

Native Hawaiian or Pacific Islander – A person having origins in any of the peoples of Hawaii, Guam, Samoa, or other Pacific Islands.

White – A person having origins in any of the peoples of Europe, the Middle East, or North Africa.

Hispanic or Latino – A person of Cuban, Mexican, Puerto Rican, South or Central American, or other Spanish culture or origin.

Exhibit A: Work Force Report Job Categories – Administration

Refer to this table when completing your firm's Work Force Report form(s).

Management & Financial
Advertising, Marketing, Promotions, Public Relations, and Sales Managers
Business Operations Specialists
Financial Specialists
Operations Specialties Managers
Other Management Occupations
Top Executives

Professional
Art and Design Workers
Counselors, Social Workers, and Other Community and Social Service Specialists
Entertainers and Performers, Sports and Related Workers
Health Diagnosing and Treating Practitioners
Lawyers, Judges, and Related Workers
Librarians, Curators, and Archivists
Life Scientists
Media and Communication Workers
Other Teachers and Instructors
Postsecondary Teachers
Primary, Secondary, and Special Education School Teachers
Religious Workers
Social Scientists and Related Workers

Architecture & Engineering, Science, Computer
Architects, Surveyors, and Cartographers
Computer Specialists
Engineers
Mathematical Science Occupations
Physical Scientists

Technical
Drafters, Engineering, and Mapping Technicians
Health Technologists and Technicians
Life, Physical, and Social Science Technicians
Media and Communication Equipment Workers

Sales
Other Sales and Related Workers
Retail Sales Workers
Sales Representatives, Services
Sales Representatives, Wholesale and Manufacturing
Supervisors, Sales Workers

Administrative Support
Financial Clerks
Information and Record Clerks
Legal Support Workers
Material Recording, Scheduling, Dispatching, and Distributing Workers
Other Education, Training, and Library Occupations
Other Office and Administrative Support Workers
Secretaries and Administrative Assistants
Supervisors, Office and Administrative Support Workers

Services
Building Cleaning and Pest Control Workers
Cooks and Food Preparation Workers
Entertainment Attendants and Related Workers
Fire Fighting and Prevention Workers
First-Line Supervisors/Managers, Protective Service Workers
Food and Beverage Serving Workers
Funeral Service Workers
Law Enforcement Workers
Nursing, Psychiatric, and Home Health Aides
Occupational and Physical Therapist Assistants and Aides
Other Food Preparation and Serving Related Workers
Other Healthcare Support Occupations
Other Personal Care and Service Workers
Other Protective Service Workers
Personal Appearance Workers
Supervisors, Food Preparation and Serving Workers
Supervisors, Personal Care and Service Workers
Transportation, Tourism, and Lodging Attendants

Crafts
Construction Trades Workers
Electrical and Electronic Equipment Mechanics, Installers, and Repairers
Extraction Workers
Material Moving Workers
Other Construction and Related Workers
Other Installation, Maintenance, and Repair Occupations
Plant and System Operators
Supervisors of Installation, Maintenance, and Repair Workers
Supervisors, Construction and Extraction Workers
Vehicle and Mobile Equipment Mechanics,

Installers, and Repairers
Woodworkers

Operative Workers
Assemblers and Fabricators
Communications Equipment Operators
Food Processing Workers
Metal Workers and Plastic Workers
Motor Vehicle Operators
Other Production Occupations
Printing Workers
Supervisors, Production Workers
Textile, Apparel, and Furnishings Workers

Transportation
Air Transportation Workers
Other Transportation Workers
Rail Transportation Workers
Supervisors, Transportation and Material Moving Workers
Water Transportation Workers

Laborers
Agricultural Workers
Animal Care and Service Workers
Fishing and Hunting Workers
Forest, Conservation, and Logging Workers
Grounds Maintenance Workers
Helpers, Construction Trades
Supervisors, Building and Grounds Cleaning and Maintenance Workers
Supervisors, Farming, Fishing, and Forestry Workers

Exhibit B: Work Force Report Job Categories-Trade

Brick, Block or Stone Masons
Brickmasons and Blockmasons
Stonemasons

Carpenters

Carpet, floor and Tile Installers and Finishers
Carpet Installers
Floor Layers, except Carpet, Wood and Hard Tiles
Floor Sanders and Finishers
Tile and Marble Setters

Cement Masons, Concrete Finishers
Cement Masons and Concrete Finishers
Terrazzo Workers and Finishers

Construction Laborers

Drywall Installers, Ceiling Tile Inst
Drywall and Ceiling Tile Installers
Tapers

Electricians

Elevator Installers and Repairers

First-Line Supervisors/Managers
First-line Supervisors/Managers of Construction Trades and Extraction Workers

Glaziers

Helpers, Construction Trade
Brickmasons, Blockmasons, and Tile and Marble Setters
Carpenters
Electricians
Painters, Paperhangers, Plasterers and Stucco
Pipelayers, Plumbers, Pipefitters and Steamfitters
Roofers
All other Construction Trades

Millwrights
Heating, Air Conditioning and Refrigeration Mechanics and Installers
Mechanical Door Repairers
Control and Valve Installers and Repairers
Other Installation, Maintenance and Repair Occupations

Misc. Const. Equipment Operators
Paving, Surfacing and Tamping Equipment Operators
Pile-Driver Operators
Operating Engineers and Other Construction Equipment Operators

Painters, Const. Maintenance
Painters, Construction and Maintenance
Paperhangers

Pipelayers and Plumbers
Pipelayers
Plumbers, Pipefitters and Steamfitters

Plasterers and Stucco Masons

Roofers

Security Guards & Surveillance Officers

Sheet Metal Workers

Structural Iron and Steel Workers

Welding, Soldering and Brazing Workers
Welders, Cutter, Solderers and Brazers
Welding, Soldering and Brazing Machine Setter, Operators and Tenders

Workers, Extractive Crafts, Miners

Item 334
9/29/2020

(R-2021-106)

RESOLUTION NUMBER R- 313223

DATE OF FINAL PASSAGE OCT 02 2020

A RESOLUTION OF THE COUNCIL OF THE CITY OF SAN DIEGO APPROVING AN AGREEMENT BETWEEN THE CITY OF SAN DIEGO AND INTERGRAPH CORPORATION, d/b/a HEXAGON SAFETY & INFRASTRUCTOR CORPORATION FOR THE COMPUTER AIDED DISPATCH SYSTEM.

WHEREAS, in December of 2015, by Resolution (R-310149) the City Council authorized the award and execution of an agreement with Intergraph Corporation d/b/a Hexagon Safety & Infrastructure Corporation (Contractor) for the purchase, implementation, design, and maintenance of a new Computer Aided Dispatch (CAD) system RFP 10047867-15-E; and

WHEREAS, implementation of the CAD system is complete, and the contract expires in October of 2020; and

WHEREAS, for the Police Department to continue using the CAD system, the City wishes to enter into a Master Agreement (Agreement) with Contractor for ongoing annual maintenance, proprietary software licensing, and resident systems administrator services; and

WHEREAS, the Agreement will allow the Police Department to continue to use the system, and perform necessary software upgrades and change orders to ensure the system continues to provide critical dispatching functions; and

WHEREAS, the Agreement is for a three (3) year term with two (2) additional one (1) year options to extend the Agreement for a total term of five (5) years for an amount not to exceed $5,878,244.48; and

WHEREAS, the Agreement meets the sole source requirements set forth in San Diego Municipal Code section 22.3016; NOW, THEREFORE

BE IT RESOLVED, by the City Council of the City of San Diego, that the Mayor or his designee is authorized to execute the Agreement with Contractor for CAD system services, including software upgrades and change orders, with a contract duration of three (3) years with the option to exercise two (2) one (1) year optional to extend the Agreement for a total term of five (5) years under the terms and conditions set forth in the Agreement on file in the Office of the City Clerk as Document No. RR- 313223.

BE IT FURTHER RESOLVED, that the Chief Financial Officer is authorized to expend an amount not to exceed $5,878,244.48 over the full term of the Agreement, including any option terms and as needed change orders, contingent upon the adoption of the Annual Appropriation Ordinance for the applicable fiscal year, and contingent upon the Chief Financial Officer first furnishing one or more certificates certifying that funds necessary for expenditure are, or will be, on deposit with the City Treasurer.

APPROVED: MARA W. ELLIOTT, City Attorney

/s/ Paige E. Folkman
Paige E. Folkman
Chief Deputy City Attorney

PEF:hm
August 28, 2020
Or.Dept:PSE
Doc. No.: 2464264

I certify that the foregoing Resolution was passed by the Council of the City of San Diego, at this meeting of 9/29/2020.

ELIZABETH S. MALAND
City Clerk

By /s/ Matthew R. Hilario
Deputy City Clerk

Approved: 10/2/2020
(date)

KEVIN L. FAULCONER, Mayor

Vetoed: _____
(date)

KEVIN L. FAULCONER, Mayor

Passed by the Council of The City of San Diego on SEP 29 2020, by the following vote:

Councilmembers	Yeas	Nays	Not Present	Recused
Barbara Bry	☒	☐	☐	☐
Jennifer Campbell	☒	☐	☐	☐
Chris Ward	☒	☐	☐	☐
Monica Montgomery	☒	☐	☐	☐
Mark Kersey	☒	☐	☐	☐
Chris Cate	☒	☐	☐	☐
Scott Sherman	☒	☐	☐	☐
Vivian Moreno	☒	☐	☐	☐
Georgette Gómez	☒	☐	☐	☐

Date of final passage OCT 02 2020.

(Please note: When a resolution is approved by the Mayor, the date of final passage is the date the approved resolution was returned to the Office of the City Clerk.)

AUTHENTICATED BY:

KEVIN L. FAULCONER
Mayor of The City of San Diego, California.

(Seal)

ELIZABETH S. MALAND
City Clerk of The City of San Diego, California.

By Connie Patterson, Deputy
for Matthews Hilario

Office of the City Clerk, San Diego, California

Resolution Number R- 313223

Passed by the Council of The City of San Diego on September 29, 2020, by the following vote:

YEAS:	**BRY, CAMPBELL, WARD, MONTGOMERY, KERSEY, CATE, SHERMAN, MORENO & GÓMEZ.**
NAYS:	**NONE.**
NOT PRESENT:	**NONE.**
RECUSED:	**NONE.**

AUTHENTICATED BY:

KEVIN L. FAULCONER

Mayor of The City of San Diego, California

ELIZABETH S. MALAND

City Clerk of The City of San Diego, California

(Seal)

By: **Connie Patterson**, Deputy

I HEREBY CERTIFY that the above and foregoing is a full, true, and correct copy of RESOLUTION NO. **R-313223**, approved on **September 29, 2020**. The date of final passage is **October 2, 2020**.

ELIZABETH S. MALAND

City Clerk of the City of San Diego, California

(Seal)

By: Connie Patterson, Deputy