EBIX Insurance No. *S200005646

AGREEMENT FOR SERVICES
BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
CLARIS STRATEGY INC.

PREAMBLE

This Agreement is made and entered into on the date last signed by the Parties ("Effective Date") between the City of Santa Clara, California, a chartered California municipal corporation (City) and Claris Strategy a California corporation, (Consultant). City and Consultant may be referred to individually as a "Party" or collectively as the "Parties."

RECITALS

A. City desires to secure the services ("Services") more fully described in this Agreement, in Exhibit A, entitled "Scope of Services";

B. Consultant represents that it, and its subcontractors, if any, have the professional qualifications, expertise, necessary licenses and desire to provide certain goods and/or required Services and goods of the quality and type which meet objectives and requirements of City; and,

C. The Parties agree that Consultant will perform the Services under the terms and conditions set forth in this Agreement.

NOW, THEREFORE, for and in consideration of the mutual promises, covenants, and conditions herein contained, the Parties hereto agree as follows:

AGREEMENT TERMS AND CONDITIONS

1. AGREEMENT DOCUMENTS

The documents forming the entire Agreement between City and Consultant shall consist of these Terms and Conditions and the following Exhibits, which are hereby incorporated into this Agreement by this reference:

Exhibit A – Scope of Services

Exhibit B – Schedule of Fees and Payment Provisions

Exhibit C – Insurance Requirements

This Agreement, including the Exhibits set forth above, contains all the agreements, representations and understandings of the Parties, and supersedes

and replaces any previous agreements, representations and understandings, whether oral or written. In the event of any inconsistency between the provisions of any of the Exhibits and the Terms and Conditions, the Terms and Conditions shall govern and control.

2. TERM OF AGREEMENT

A. Unless otherwise set forth in this Agreement or unless this paragraph is subsequently modified by written amendment to this Agreement, the term of this Agreement shall begin on August 1, 2025, and terminate on July 31, 2027 ("Initial Term").

B. After the Initial Term, City reserves the right, at its sole discretion, to extend the term of this Agreement for one (1) additional year through July 31, 2028 ("Option Periods") in such increments as determined by City. The Option Periods shall be authorized through an Amendment to this Agreement executed by the Parties. The Initial Term and Option Periods shall collectively be referred to as "Term".

3. SCOPE OF SERVICES AND PERFORMANCE SCHEDULE

Consultant shall perform those Services specified in Exhibit A within the time stated in Exhibit A. Time is of the essence.

4. WARRANTY

In addition to those warranties contained in Exhibit A, Consultant expressly warrants that all Services and materials covered by this Agreement shall be fit for the purpose intended, shall be free from defect and shall conform to the specifications, requirements and instructions applicable to this Agreement. Consultant agrees to promptly replace or correct any incomplete, inaccurate or defective Services or materials at no further cost to City when defects are due to the negligence, errors or omissions of Consultant. If Consultant fails to promptly correct or replace Services or materials, City may make corrections or replace Services or materials and charge Consultant for the cost incurred by City.

5. QUALIFICATIONS OF CONSULTANT - STANDARD OF CARE

A. Consultant represents and maintains that it is skilled in the professional calling necessary to perform the Services, including its duties and obligations, expressed and implied, contained herein. Consultant shall perform all Services under this Agreement in a skillful and competent manner, consistent with the standards generally recognized as being employed by professionals in the same discipline in the State of California. City expressly relies upon Consultant's representations regarding its skills and knowledge.

B. Consultant warrants that all employees and subcontractor, if any, shall have sufficient skill and experience to perform the Services assigned to them.

C. Consultant shall comply with all applicable federal, state and local laws in the performance of the Services; including but not limited to those of the Occupational Safety and Health Administration (OSHA) and the California Department of Industrial Relations and State Division of Industrial Safety and the professional standard of care. Where any applicable laws or ordinances conflict with the City's requirements, the more stringent requirement(s) shall be followed. Consultant's failure to be thoroughly familiarized with the provisions of any applicable federal, state, and local regulations, ordinances and codes shall not relieve Consultant from compliance with the obligations and penalties resulting therefrom.

D. Consultant represents and warrants to the City that it has, shall obtain, and shall keep in full force in effect during the Term hereof, at its sole cost and expense, all licenses, permits, qualifications, insurance and approvals of whatsoever nature that is legally required of Consultant to practice its profession and to perform Services.

6. COMPENSATION AND PAYMENT

In consideration for Consultant's complete performance of Services, City shall pay Consultant for all Services rendered and material provided by Consultant in accordance with Exhibit B, entitled "SCHEDULE OF FEES AND PAYMENT PROVISIONS." The maximum compensation of this Agreement is **TWO HUNDRED FORTY-SIX THOUSAND THREE HUNDRED FIFTY-TWO DOLLARS ($246,352),** subject to budget appropriations, which includes all payments that may be authorized for Services and for expenses, supplies, materials and equipment required to perform the Services including any taxes. All Services performed or supplies, materials and equipment provided in excess of the maximum compensation shall be at Consultant's expense. Consultant shall not be entitled to any payment above the maximum compensation under any circumstance.

7. TERMINATION

A. Termination for Convenience. City shall have the right to terminate this Agreement, without cause or penalty, by giving not less than Thirty (30) days' prior written notice to Consultant.

B. Termination for Default. For purposes of this Section 7.B., the word "Default" shall mean the failure of Consultant to perform any of Consultant's duties or obligations or the breach by Consultant of any of the terms and conditions set forth in this Agreement. In addition, Consultant shall be deemed to be in Default upon Consultant (i) applying for, consenting to, or suffering of, the appointment of a receiver, trustee or liquidator for all or a

substantial portion of its assets; (ii) making a general assignment for the benefit of creditors; (iii) being adjudged bankrupt; (iv) filing a voluntary petition or suffering an involuntary petition under any bankruptcy, arrangement, reorganization or insolvency law (unless in the case of an involuntary petition, the same is dismissed within thirty (30) days of such filing); or (v) suffering or permitting to continue unstayed and in effect for fifteen (15) consecutive days any attachment, levy, execution or seizure of all or a substantial portion of Consultant's assets or of Consultant's interests hereunder. In the event of any Default by Consultant, in addition to all other remedies provided by law, City may terminate this Agreement immediately upon written notice to Consultant.

C. Upon termination, each Party shall assist the other in arranging an orderly transfer and close-out of services. As soon as possible following the notice of termination, but no later than ten (10) days after the notice of termination, Consultant will deliver to City all City information or material that Consultant has in its possession.

D. In the event of termination under sections 7.A. or 7.B., Consultant shall have no further rights hereunder

8. ASSIGNMENT AND SUBCONTRACTING

City and Consultant bind themselves, their successors and assigns to all covenants of this Agreement. This Agreement shall not be assigned or transferred without the prior written approval of City. Consultant shall not hire subcontractors without express written permission from City.

Consultant shall be as fully responsible to City for the acts and omissions of its subcontractors, and of persons either directly or indirectly employed by them, as Consultant is for the acts and omissions of persons directly employed by it.

9. NO THIRD PARTY BENEFICIARY

This Agreement shall not be construed to be an agreement for the benefit of any third party or parties and no third party or parties shall have any claim or right of action under this Agreement for any cause whatsoever.

10. INDEPENDENT CONTRACTOR

Consultant and all person(s) employed by or contracted with Consultant to furnish labor and/or materials under this Agreement are independent contractors and do not act as agent(s) or employee(s) of City. Consultant has full rights to manage its employees in their performance of Services under this Agreement.

11. CONFIDENTIALITY OF MATERIAL

A. "Confidential Information" means, with respect to a Party hereto, all information or material which either (1) is marked or identified as "Confidential," "Restricted," or "Proprietary Information" or other similar marking or identification, or (2) the other Party knew, as recipient, or under the circumstances, should have known, was considered confidential or proprietary by the Disclosing Party (as defined below), except that this Agreement, Consultant pricing, and Consultant proposals incorporated into this Agreement shall not be deemed Confidential Information. Confidential Information shall consist of all information, whether in written, oral, electronic, or other form, furnished in connection with this Agreement by the Disclosing Party or its Representatives ("Representative" is defined as any elected and appointed officials, affiliate, director, officer, employee, agent, advisor or Consultant of a Party or any of its subsidiaries or affiliates) to the Receiving Party (as defined below) or to its Representatives, and specifically includes but is not limited to the City's individually identifiable customer information, and the City's customer usage data and financial data.

B. Consultant and the City shall each hold the other's Confidential Information in confidence. Neither Party shall make the other's Confidential Information available in any form to any third party or use the other's Confidential Information for any purpose other than as specified in this Agreement. The Party providing Confidential Information ("Disclosing Party") to the other Party ("Receiving Party") shall remain the sole owner of such information. Except as provided elsewhere within this Agreement, nothing contained in this Agreement shall be construed as granting or conferring any right or license in any Confidential Information or in any patents, copyrights, software or other technology, either expressly or by implication to the Receiving Party, or to its Representatives or to others. The term Confidential Information shall not include any of the following: (1) information already in possession of, or already known to, the Receiving Party as of the Effective Date without an obligation of confidentiality; (2) information in the public domain at the time of the disclosure, or which, after such disclosure, enters into the public domain through no breach of this Agreement by the Receiving Party or its Representative(s); (3) information lawfully furnished or disclosed to the Receiving Party by a non-party to this Agreement without any obligation of confidentiality and through no breach of this Agreement by the Receiving Party or its Representative(s); (4) information independently developed by the Receiving Party without use of any Confidential Information of the Disclosing Party; (5) information authorized in writing by the Disclosing Party to be released from the confidentiality obligations herein; or (6) this Agreement and Consultant's proposals.

C. By virtue of this Agreement, each Party hereto may disclose to the other Party information that is Confidential Information. This Agreement does not diminish, revoke or supersede any existing confidentiality, non-disclosure or similar agreement between the Parties that does not pertain to the subject matter of this Agreement. However, any Confidential Information, whether or not previously disclosed, that pertains to the subject matter of this Agreement shall be governed by the terms of this Section 11 which shall supersede any such previous agreement with respect to such Confidential Information and any Confidential Information relating to the subject matter of this Agreement that was exchanged under such previous agreement shall be treated as though it was exchanged under this Agreement as of the date of such exchange.

D. The Receiving Party will treat all Confidential Information of the Disclosing Party, no matter written, electronic, or oral, as confidential and proprietary, and the Receiving Party shall only use such information in furtherance of this Agreement. As such, the Receiving Party shall hold in confidence the Confidential Information of the Disclosing Party and ensure that such Confidential Information is not disclosed to any other person or entity, except as expressly permitted by this Agreement or as authorized in writing by the Disclosing Party. The Receiving Party shall not disclose Confidential Information of the Disclosing Party received under this Agreement to any person other than its Representatives who require knowledge of such Confidential Information in furtherance of this Agreement. The Receiving Party shall inform its Representatives of the confidential nature of the Confidential Information of the Disclosing Party and advise such Representatives of the limitations on the use and disclosure and prohibition on making copies or summaries of such Confidential Information. The Receiving Party shall be responsible for any breach of this Agreement by its Representatives. Neither Party shall use the Confidential Information of the other Party for any commercial purpose.

E. If the Receiving Party becomes legally compelled (by oral questions, interrogatories, request for information or documents, subpoena, civil investigative demand, or similar process) to disclose any Confidential Information of the Disclosing Party or is requested Confidential Information pursuant to the California Public Records Act or similar law, the Receiving Party will provide the Disclosing Party with written notice of such an occurrence (if so permitted) as soon as possible. Thereafter, at its sole costs and expense, the Disclosing Party may seek a protective order or other appropriate remedy or waive compliance with the provisions of this Agreement. If the disclosing Party (i) waives compliance, (ii) fails to respond to the Receiving Party within five (5) business days, or (iii) after providing the notice and assistance required under this Section, the Receiving Party remains required by law to disclose any Confidential Information, the

Receiving Party shall disclose only that portion of the Confidential Information that the Receiving Party is legally required to disclose. So long as it is consistent with applicable law, the Receiving Party will not oppose action by, and the Receiving Party will cooperate with, the Disclosing Party, at the Disclosing Party's sole cost and expense, to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded the Confidential Information. If the Disclosing Party fails to obtain such protective order or other remedy, or if the Disclosing Party waives compliance with the requirements of the preceding sentence, the Receiving Party will disclose only that Confidential Information that it is legally required to disclose, and will exercise commercially reasonable efforts, at Disclosing Party's expense, to obtain reliable assurance that confidential treatment will be accorded the Confidential Information so disclosed.

F. In the event the Receiving Party discloses, disseminates or releases any Confidential Information, except as expressly permitted by this Agreement, such disclosure, dissemination or release will be deemed a material breach of this Agreement and the Disclosing Party may demand prompt return of all Confidential Information previously provided to the Receiving Party. As soon as the Receiving Party becomes aware that it has made an unauthorized disclosure of Confidential Information, the Receiving Party shall take any and all necessary actions to recover the improperly disclosed Confidential Information and immediately notify Disclosing Party regarding the nature of the unauthorized disclosure and the corrective measures being taken. Each Party agrees that any breach of their confidentiality obligations could cause irreparable harm to the other Party, the amount of which would be extremely difficult to estimate. Accordingly, it is understood and agreed that monetary damages would not be a sufficient remedy for any material breach of this Agreement and that specific performance and injunctive relief in addition to monetary damages shall be appropriate remedies for any breach or any threat of such breach. The provisions of this Paragraph are in addition to any other legal rights or remedies the Disclosing Party may have.

G. Within two (2) weeks of the termination of this Agreement, Consultant will return to the City or destroy, to the extent permitted by law, any and all Confidential Information, including all originals, copies, translations, transcriptions or any other form of material, without retaining any copy or duplicate thereof; provided that Consultant may retain Confidential Information contained on backup media created in the ordinary course of business provided further that there is no effort to access such Confidential Information and Consultant's confidential obligations with respect to such information shall continue so long as such information is retained. Consultant shall certify in writing the destruction of the Confidential

Information. The City may perform an audit of Consultant's records to confirm the return or destruction of the Confidential Information. The City shall have this audit right for two (2) years after the termination of this Agreement.

H. Notwithstanding the termination of this Agreement, this Confidentiality Section shall survive the expiration or earlier termination of this Agreement.

12. OWNERSHIP OF MATERIAL

A. City shall furnish to Consultant such documents and materials as may be relevant and pertinent to the provision of Services hereunder as City may possess or acquire.

B. All documents and materials furnished by City to Consultant, pursuant to Section 12.A., shall remain the property of City and shall be returned to City upon termination of this Agreement, for any reason. All documents or material prepared or caused to be prepared by Consultant, its officers, employees, agents and subcontractors, in the course of implementing this Agreement, shall be considered works made for hire and shall become the exclusive property of the City, and City shall have the sole right to use such documents and materials without restriction or limitation on their use in City's discretion without further compensation to Consultant or any other party. Consultant shall, at Consultant's sole cost and expense, provide such documents and material to City upon written request.

C. Documents and material prepared by Consultant, pursuant to this Agreement, are not intended or represented to be suitable for reuse by City or others on any other project. Any use of completed documents for other projects and any use of incomplete documents without specific written authorization from Consultant will be at City's sole risk and without liability to Consultant. Further, any and all liability arising out of changes made to Consultant's deliverables under this Agreement by City or persons other than Consultant, is waived against Consultant and City assumes full responsibility for such changes unless City has given Consultant prior notice and has received from Consultant written consent for such change.

13. RIGHT OF CITY TO INSPECT RECORDS OF CONSULTANT

A. City, through its authorized employees, representatives or agents shall have the right during the Term and for four (4) years from the date of final payment for Services or goods provided under this Agreement ("Audit Period"), to audit the books and records of Consultant for the purpose of verifying any and all Consultant invoices and charges.

B. Consultant shall keep records and invoices in connection with the Services for the length of the Audit Period. Consultant agrees to maintain sufficient books and records in accordance with generally accepted accounting principles to establish the correctness of all charges submitted to City.

C. Consultant shall use recognized accounting methods in preparing reports and invoices submitted to the City in connection with the Services. City reserves the right to designate its own employee representative(s) or its contracted representative(s) with a certified public accounting firm who shall have the right to audit Consultant's accounting procedures and internal controls of Consultant's financial systems and to examine any cost, revenue, payment, claim, other records or supporting documentation resulting from any items set forth in this Agreement. If Consultant fails to provide supporting documentation satisfactory to City for costs charged, then Consultant agrees to reimburse City for those costs. Any such audit(s) shall be undertaken by City or its representative(s) at reasonable times and in conformance with generally accepted auditing standards. Consultant agrees to fully cooperate with any such audit(s).

D. Consultant will be notified in writing of any exception taken as a result of an audit. Any adjustments and/or payments which must be made as a result of any such audit or inspection of Consultant's invoices and/or records shall be made within thirty (30) days from presentation of City's findings to Consultant. If Consultant fails to make such payment, Consultant agrees to pay interest, accruing monthly, at a rate of ten percent (10%) per annum unless another section of this Agreement specifies a higher rate of interest, then the higher rate will prevail. Interest will be computed from the date of written notification of exception(s) to the date Consultant reimburses City for any exception(s). If an audit inspection or examination in accordance with this Section discloses overcharges (of any nature) by Consultant to City in excess of one percent (1%) of the value of that portion of the Agreement that was audited, the actual cost of City's audit shall be reimbursed to City by Consultant.

E. Consultant shall submit to City any and all reports concerning its performance under this Agreement that may be requested by City in writing. Consultant agrees to assist City in meeting City's reporting requirements to the State and other agencies with respect to the Services.

14. HOLD HARMLESS/INDEMNIFICATION

A. To the extent permitted by law, Consultant agrees to protect, defend, hold harmless and indemnify City, its City Council, commissions, officers, employees, volunteers and agents from and against any claim, injury, liability, loss, cost, and/or expense or damage, including all costs and attorney's fees in providing a defense to any such claim or other action, and

whether sounding in law, contract, tort, or equity, in any manner arising from, or alleged to arise in whole or in part from, or in any way connected with the Services performed by Consultant pursuant to this Agreement – including claims of any kind by Consultant's employees or persons contracting with Consultant to perform any portion of the Services – and shall expressly include passive or active negligence by City connected with the Services. However, the obligation to indemnify shall not apply if such liability is ultimately adjudicated to have arisen through the sole active negligence or sole willful misconduct of City; the obligation to defend is not similarly limited.

B. Consultant's obligation to protect, defend, indemnify, and hold harmless in full City and City's employees, shall specifically extend to any and all employment-related claims of any type brought by employees, contractors, subconsultants, subcontractors or other agents of Consultant, against City (either alone, or jointly with Consultant), regardless of venue/jurisdiction in which the claim is brought and the manner of relief sought.

C. To the extent Consultant is obligated to provide health insurance coverage to its employees pursuant to the Affordable Care Act ("Act") and/or any other similar federal or state law, Consultant warrants that it is meeting its obligations under the Act and will fully indemnify and hold harmless City for any penalties, fines, adverse rulings, or tax payments associated with Consultant's responsibilities under the Act.

15. INSURANCE REQUIREMENTS

During the Term, and for any time period set forth in Exhibit C, Consultant shall provide and maintain in full force and effect, at no cost to City, insurance policies as set forth in Exhibit C.

16. WAIVER

Consultant agrees that waiver by City of any one or more of the conditions of performance under this Agreement shall not be construed as waiver(s) of any other condition of performance under this Agreement. Neither City's review, acceptance nor payments for any of the Services required under this Agreement shall be constructed to operate as a waiver of any rights under this Agreement or of any cause of action arising out of the performance of this Agreement.

17. NOTICES

All notices to the Parties shall, unless otherwise requested in writing, be sent to City addressed as follows:

City of Santa Clara
Attention: Silicon Valley Power
1500 Warburton Avenue
Santa Clara, CA 95050
and by e-mail at svpcontracts@santaclaraca.gov and manager@santaclaraca.gov

And to Consultant addressed as follows:

Claris Strategy Inc.
Attn: William Lim
1111 Drake Road
Arcadia, CA 91007
and by e-mail at wlim@clarisstrategy.com

The workday the e-mail was sent shall control the date notice was deemed given. An e-mail transmitted after 1:00 p.m. on a Friday shall be deemed to have been transmitted on the following business day.

18. COMPLIANCE WITH LAWS

Consultant shall comply with all applicable laws and regulations of the federal, state and local government, including but not limited to "The Code of the City of Santa Clara, California" ("SCCC"). In particular, Consultant's attention is called to the regulations regarding Campaign Contributions (SCCC Chapter 2.130), Lobbying (SCCC Chapter 2.155), Minimum Wage (SCCC Chapter 3.20), Business Tax Certificate (SCCC section 3.40.060), and Food and Beverage Service Worker Retention (SCCC Chapter 9.60), as such Chapters or Sections may be amended from time to time or renumbered. Additionally Consultant has read and agrees to comply with City's Ethical Standards (http://santaclaraca.gov/home/showdocument?id=58299).

19. CONFLICTS OF INTEREST

Consultant certifies that to the best of its knowledge, no City officer, employee or authorized representative has any financial interest in the business of Consultant and that no person associated with Consultant has any interest, direct or indirect, which could conflict with the faithful performance of this Agreement. Consultant is familiar with the provisions of California Government Code section 87100 and

following, and certifies that it does not know of any facts which would violate these code provisions. Consultant will advise City if a conflict arises.

20. FAIR EMPLOYMENT

Consultant shall not discriminate against any employee or applicant for employment because of race, sex, color, religion, religious creed, national origin, ancestry, age, gender, marital status, physical disability, mental disability, medical condition, genetic information, sexual orientation, gender expression, gender identity, military and veteran status, or ethnic background, in violation of federal, state or local law.

21. NO USE OF CITY NAME OR EMBLEM

Consultant shall not use City's name, insignia, or emblem, or distribute any information related to Services under this Agreement in any magazine, trade paper, newspaper or other medium without express written consent of City.

22. GOVERNING LAW AND VENUE

This Agreement shall be governed and construed in accordance with the statutes and laws of the State of California. The venue of any suit filed by either Party shall be vested in the state courts of the County of Santa Clara, or if appropriate, in the United States District Court, Northern District of California, San Jose, California.

23. SEVERABILITY CLAUSE

In case any one or more of the provisions in this Agreement shall, for any reason, be held invalid, illegal or unenforceable in any respect, it shall not affect the validity of the other provisions, which shall remain in full force and effect.

24. AMENDMENTS

This Agreement may only be modified by a written amendment duly authorized and executed by the Parties.

25. COUNTERPARTS

This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but both of which shall constitute one and the same instrument.

SIGNATURES ON NEXT PAGE

The Parties acknowledge and accept the terms and conditions of this Agreement as evidenced by the following signatures of their duly authorized representatives.

CITY OF SANTA CLARA, CALIFORNIA
a chartered California municipal corporation

Approved as to Form:

GLEN R. GOOGINS
City Attorney

Dated: July 28, 2025

JŌVAN D. GROGAN
City Manager
City of Santa Clara
1500 Warburton Avenue
Santa Clara, CA 95050
Telephone: (408) 615-2210
Fax: (408) 241-6771

"CITY"

CLARIS STRATEGY
*choose one: a California corporation

Dated: July 10, 2025
By (Signature):
Name: William Lim
Title: CEO/President
Principal Place of Business Address: 1111 Drake Rd. Arcadia, CA 91007
Email Address: wlim@clarisstrategy.com
Telephone: (626-437-4365

"CONSULTANT"

EXHIBIT A
SCOPE OF SERVICES

SECTION 1. GENERAL

1.1 Consultant shall provide comprehensive professional services to prepare the following for the City's Electric Utility Department, Silicon Valley Power (SVP):

1.1.1 A threat and vulnerability assessment (TVA) report for a total of thirty-nine (39) unique sites, including:

1.1.1.1 Thirty-five (35) City substations

1.1.1.2 One (1) switching station

1.1.1.3 Donald Von Raesfeld Power Plant (DVR)

1.1.1.4 Gianera Generating Station (Gianera)

1.1.1.5 Natural Gas Pipeline & Natural Gas Compressor Station

1.1.2 Standard plans, details, and specifications for physical and operational security of future substations yet to be constructed.

1.1.3 Update to 2021 Utility Security Plan

1.2 The terms "City" and "SVP," are used interchangeably.

SECTION 2. SPECIFIC WORK REQUIREMENTS

2.1 **Threat and Vulnerability Assessment Report.** Consultant will prepare a report that will (a) identify critical assets at each facility, (b) identify mitigation, protection, prevention, and resiliency efforts to address security and reduce the potential of long-term outage, and (c) provide a prioritization of the overall needs for City's consideration. Consultant shall provide recommendations of required and desirable improvements at each facility with cost estimates. Consultant shall comprehensively identify optimal physical and operational security for each facility and may focus on the following areas for each facility:

2.1.1 Parking/Delivery/Standoff

2.1.2 Security Force Profile

2.1.3 Barriers

2.1.4 Electronic security systems

2.1.5 Dependencies (Electric Power)

2.1.6 Dependencies (Information Technology)

2.2 **Standard Plans, Details, and Specifications for Physical and Operational Security of Future Substations.** Consultant shall provide recommendations, standard plans, details, and specifications for optimal physical and operational security for future substations yet to be constructed, to improve public safety and deter sabotage, theft, and vandalism that includes, but is not limited to, the following:

2.2.1 Access control system that consists of access control panel, auxiliary power supply, card readers at all doors, magnetic door contacts, and wire and other related accessories.

2.2.2 Perimeter fence/wall, equipment and communication line protection, gate security and access control, intrusion alarm, video cameras, and biometric identification systems.

2.2.3 Consultant shall evaluate the City's current access control system software for two separate systems: SVP's main system and SVP's isolated system, both subject to federal regulatory compliance requirements, including the North American Electric Reliability Corporation (NERC). If Consultant recommends new software, Consultant shall provide a comprehensive report containing a cost-benefit, resource analysis, and impact analyses, along with an estimated timeline and other considerations identified by Consultant. If the City chooses to replace the systems, the City may request Additional Services (as defined in Section 7) pursuant to Section 7 from Consultant, such as but not limited to:

2.2.3.1 Assisting the City in facilitating the Request for Proposals (RFP) including the development of solicitation documents, assistance with responding to vendor questions, and participation in the evaluation process and contract negotiations.

2.2.3.2 Providing services to maintain current system functionality.

2.3 2021 Utility Security Plan Update

2.3.1 Consultant shall provide:

2.3.1.1 A detailed narrative explaining how SVP can take steps to implement a preventative maintenance plan for security equipment to ensure that mitigation measures are functional and performing adequately.

2.3.1.2 A description of distribution and/or security control center roles and actions related to distribution system physical security.

2.3.2 Consultant shall identify and recommend firms, utilities, or municipalities capable of conducting an independent review of the updated Utility Security Plan delivered by Consultant to City.

2.3.3 Consultant shall provide recommendations that support and integrate with SVP's resiliency plans and activities.

2.3.4 Consultant shall review and update the 2021 Utility Security Plan to include up to six (6) of the thirty-nine (39) sites identified in Section 1.1. Consultant shall submit an updated plan that complies with the requirements of the California Public Utilities Commission (CPUC) Decision 19-01-018. The report shall include, but not be limited to, the following:

2.3.4.1 Overview

2.3.4.2 Background

2.3.4.3 Plan Development Process

2.3.4.4 Identification of Covered Distribution Facilities

2.3.4.5 Risk Assessment per Site

2.3.4.6 Covered Distribution Facility Mitigation Plans per Site

2.3.4.7 Independent Evaluation and Response

2.3.4.8 Validation

2.3.4.9 Narrative Descriptions for Utility Security Plan

2.4 Project Management/Communication

2.4.1 Consultant shall communicate and coordinate with the City's designated project manager and project team.

2.4.2 Consultant shall conduct meetings with the City, third-party contractors or consultants, vendors, and other design consultants as necessary. These meetings may be conducted in person or virtually.

2.4.3 Through the project manager designated by City, Consultant shall coordinate with SVP Divisions including Planning, Fiber, Protection, Substation, Systems Support, Operations, Engineering Records Retention,

Electrical Control Center, and management. Such coordination shall be incorporated into the fixed price defined in Exhibit B.

2.4.4 Consultant will be provided access to and is expected to use the City's project management tool, e-Builder, further described in Section 6 for managing schedules, action items, and invoicing. All other files, such as reports, plans, and deliverables, must be submitted to a City-controlled Secure File Transfer Protocol (SFTP) site separate from e-builder.

2.4.5 Consultant is responsible for providing all staff and materials to complete the project.

2.4.6 Consultant shall perform the required services at their own offices.

2.4.7 Consultant is required to conduct site or field visits to support their work.

2.4.8 Consultant must ensure the information security of all City-owned data in its possession, including any data or materials generated by the Consultant and its affiliates, subcontractors, and service providers in connection with the work for the City. This includes implementing specific methods for storage, handling, and transmittal of the data or materials. Consultant shall be compliant with System and Organization Control (SOC or SOC2) and work within a Federal Risk and Authorization Management Program (FedRAMP) security framework.

SECTION 3. PROJECT WORK PLAN

3.1 Task 1 – Project Start Up

3.1.1 **Request for Background Materials**. Consultant shall submit a data request(s) to City for information needed to perform services. All data shall be exchanged through SFTP site provided by City. The requested information may include, but not be limited to:

3.1.1.1 City and/or SVP goals and policies.

3.1.1.2 Regulatory requirements.

3.1.1.3 Previous threat and vulnerability assessments.

3.1.1.4 Previous physical security assessments.

3.1.1.5 Security plans including 2021 Utility Security Plan.

3.1.1.6 Emergency response plans.

3.1.1.7 Security system information, such as:

3.1.1.7.1 As-built floor plans with layout of rooms, cable paths, architectural features, and security devices.

3.1.1.7.2 System block diagrams illustrating the overall architecture and components of the electronic security systems and interconnections between different devices.

3.1.1.7.3 Wiring diagrams depicting the electrical connections between different components of the security system.

3.1.1.7.4 Elevation Drawings with a vertical view of specific areas, such as the exterior walls where security devices are placed.

3.1.1.7.5 Integration Design Documents: a comprehensive and detailed blueprint for the integration of disparate systems, applications, or components within a larger software or IT infrastructure. This document outlines the architecture, data flow, interfaces, protocols, and communication mechanisms.

3.1.1.8 City Policies regarding:

3.1.1.8.1 How video can be used in the city.

3.1.1.8.2 Exporting and sharing recorded video.

3.1.1.8.3 Configuration of video cameras (resolution, framerate, codec, compression, etc.).

3.1.1.8.4 Design standards or design criteria for security systems.

3.1.1.8.5 User accounts and access rights for various security systems.

3.1.1.9 Standard Operating Procedures.

3.1.1.9.1 Response to access control alarms (e.g. door held open, door forced open) to include alarmed gates and roll-up doors.

3.1.1.9.2 Response to duress alarm.

3.1.1.9.3 Procedures for exporting and sharing recorded video.

3.1.1.9.4 Procedures for viewing live video.

3.1.1.10 After-Action Reports and Improvement Plans.

3.1.1.11 Site maps and facility plans of facilities to be assessed.

3.1.1.12 Customer and staff data regarding safety and security issues.

3.1.1.13 Specific safety and security standard operating procedures (SOPs).

3.1.1.14 Organization charts.

3.1.1.15 Previous related studies and reports.

3.1.2 Project Kick-Off Meeting

Consultant shall schedule a kick-off meeting with SVP personnel. The kick-off meeting shall be virtual, unless SVP requests the meeting to be onsite to coincide with the scheduled site visits. The meeting agenda shall include:

3.1.2.1 Review of project goals and assumptions.

3.1.2.2 Review project scope and work plan.

3.1.2.3 Establishment of a schedule for delivering (a) the Threat and Vulnerability Assessment Report; (b) the Standard Plans, Details, and Specifications for Physical and Operational Security of Future Substations; and (c) the Utility Security Plan.

3.1.2.4 Identification of City staff and Consultant's team members roles and responsibilities.

3.1.2.5 Confirmation the facilities to be assessed.

3.1.2.6 Data collection methods to be used.

3.1.2.7 Discussion of preliminary set of assessment criteria.

3.1.2.8 Discussion of risk methodology use for risk assessment.

3.1.2.9 Establishment of communication channels.

3.1.2.10 Confirmation of key project dates and deliverables.

3.1.2.11 Discussion and confirmation of dates for site walk.

3.1.2.12 Development of initial list of stakeholders.

3.1.2.13 Project team discussion.

3.2 Task 2 – Data Collection

3.2.1 Site and Facilities to Assess

3.2.1.1 Consultant to conduct site visits to assess thirty-nine (39) SVP sites including:

3.2.1.1.1 Thirty-five (35) City substations.

3.2.1.1.2 Switching Station.

3.2.1.1.3 Donald Von Raesfeld Power Plant.

3.2.1.1.4 Gianera Generating Station.

3.2.1.1.5 Natural Gas Pipeline and Natural Gas Compressor Station.

3.2.2 Site and Facility Walks

3.2.2.1 Consultant shall use the site and facility walks to evaluate potential threats, to document the security measures in place, to assess any vulnerabilities, to identify any opportunities for improvement, and gather any other data required for Consultant to perform Services.

3.2.2.2 Consultant will be accompanied at all times by SVP staff and may only photograph with consent from SVP staff.

3.2.2.3 Consultant shall document the site and facilities through photographs and notes, focusing on an assessment criteria checklist previously developed and agreed upon by Parties. These will include

3.2.2.3.1 Site and facilities physical security including use of entrances and exits for vehicles and persons, lighting, fences, walls, gates, guard rails, bollards, secured doors and locking systems, screening centers and equipment and guard posts.

3.2.2.3.2 Intrusion and egress vulnerabilities to the threats such as terrorist attack, active shooter, and criminal behavior.

3.2.2.3.3 Video surveillance systems (CCTV).

3.2.2.3.4 Access control systems.

3.2.2.3.5 Intrusion detection systems.

3.2.2.3.6 Communication systems dependencies.

3.2.2.3.7 Electric power dependencies.

3.2.2.3.8 Information technology systems dependencies.

3.2.2.4 During the facility walks, Consultant shall evaluate the following with respect to the security systems at the facilities:

3.2.2.4.1 Coverage: Evaluate the system's coverage and ensure that all critical areas, such as entry and exit points, perimeters of buildings, areas critical to operations, and public spaces are adequately covered by cameras.

3.2.2.4.2 Quality: The quality of the video footage is essential for identifying people and events accurately. Every camera should have a specific objective and purpose (detection, observation, recognition, identification). Some cameras will be used for general observation of a space while other cameras should provide high- resolution video that can capture details such as faces, license plates, and other identifying features.

3.2.2.4.3 Storage: The system should have sufficient storage capacity to retain video footage for an extended period. Depending on the City's requirements, the storage capacity should be able to retain video footage for a specified amount of time.

3.2.2.4.4 Integration: The video surveillance system could be integrated with other security systems, such as access control and alarm systems. Integration ensures that the video footage can be used in conjunction with other security measures to enhance

the overall security of the city. Integrations will be evaluated and considered in the process.

3.2.2.4.5 Maintenance: The system should be easy to maintain, and regular maintenance should be performed to ensure optimal performance. Maintenance and support options will be considered with any recommendations.

3.2.3 Key Stakeholder Interviews

3.2.3.1 Consultant will conduct interviews (up to eight interviews) with key City staff. Each interview will be approximately sixty minutes in length. Interviews may be held virtually or, if possible, be held on site during the site walks. The interviews will:

3.2.3.1.1 Identify the key stakeholders responsible for security at the sites to be assessed.

3.2.3.1.2 Include meetings with key stakeholders, including Planning, Fiber, Protection, Substation, Systems Support, Operations, Engineering Records Retention, Electrical Control Center, and management to discuss any security concerns, past incidents, challenges, lessons learned and opportunities.

3.2.3.1.3 Develop an understanding of the processes and procedures in place to monitor, patrol, report, notify and respond to security incidents.

3.2.3.1.4 Meetings with law enforcement and security staff to discuss security issues such as criminal activity, incident reports, and community and social concerns which could impact the potential threats and vulnerabilities surrounding the sites.

3.2.4 Document Review

Consultant shall review the background material received in detail to develop an understanding of the current state of the safety and security of the facilities.

3.2.5 Research

3.2.5.1 Threat Analysis Based on Local and National Research. Consultant shall perform research on the following threat areas:

3.2.5.1.1 Terrorist threat. Consultant shall regularly update the threat profile for various types of terrorist threats to critical infrastructure utilizing our sources and contacts at applicable security organizations such as the Federal Bureau of Investigation (FBI), Department of U. S. Department of Homeland Security (DHS), Joint Terrorist Task Force (JTTF), Infragard, Federal Emergency Management Agency (FEMA), local law enforcement and American Society for Industrial Safety (ASIS) to identify the current best practices to harden high target facilities.

3.2.5.1.2 Criminal Statistics. Consultant shall provide three (3) years of crime statistics for each facility location. Analysis will include current, real-time, and historical data by utilization of the Federal Bureau of Investigation Uniform Crime Report (UCR) systems as well as Automated Regional Justice Information Systems (ARJIS) to target Part 1 violent crimes, Part 1 property crimes, and Part 2 offenses.

3.3 Task 3 Findings Summary and Risk Analysis

Consultant shall perform the following actions in Task 3:

3.3.1 **Findings.** Consultant shall produce and discuss an initial set of findings that will include:

3.3.1.1 A summary of the information collected, using a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis for each facility.

3.3.1.2 Identification of locations necessitating the construction, or addition of physical deterrents.

3.3.1.3 Risk analysis with prioritization of areas requiring mitigation.

3.3.1.4 Identification of rough order of magnitude costs.

3.3.2 **Findings Meeting.** Consultant shall host a virtual meeting with City's project staff to review Consultant's findings. This meeting shall include a review of the SWOT analysis, and City will provide direction to Consultant identifying which mitigation strategies to focus on for the final report.

3.3.3 **Risk Assessment**. Consultant shall use the information collected to develop a risk assessment based on the assets to be protected, relevant

threats and vulnerabilities identified. Consultant shall use the U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) methodology for the risk assessment:

Risk (R) = Threat (T) x Vulnerability (V) x Consequence (C)

3.3.3.1 **Threat Assessment.** Based on the research, Consultant will identify the relevant threats to each facility. Consultant will rate relevant threats for a facility on a scale of 1 (Very Low) to 10 (Very High). At a minimum, Consultant will consider the following threats and hazards:

3.3.3.1.1 Terrorist attack: Vehicle borne bomb, person borne bomb, vehicle ramming, drone attach, active shooter, firearms to grid components, generation lines, fuel tanks, sabotage, chemical, biological, radiological, and nuclear and explosives (CBRNE) attack.

3.3.3.1.2 Criminal activity: Active shooter, firearms to grid components, generation lines, fuel tanks, trespassing, assault, theft or diversion, robbery, rape, arson, vandalism, and insider threat.

3.3.3.2 **Vulnerability Assessment**. In the vulnerability assessment, Consultant will include an in-depth analysis of the facilities' functions, systems, and site characteristics to identify building weaknesses and identifying mitigations or corrective actions that can be designed and/or implemented to reduce the vulnerabilities. Consultant will rate each relevant vulnerability on the scale of 1 (Very Low) to 10 (Very High).

At a minimum, Consultant will consider, the following components in the vulnerability assessment for each facility:

3.3.3.2.1 Fencing/gates.

3.3.3.2.2 Security lighting.

3.3.3.2.3 Security signage.

3.3.3.2.4 Vehicle bollards.

3.3.3.2.5 Door and gate locks.

3.3.3.2.6 Blast resistance/standoff distances.

3.3.3.2.7 Panic buttons.

3.3.3.2.8 Security systems: video surveillance, access control, intrusion detection, system monitoring.

3.3.3.2.9 Security/emergency communications

3.3.3.2.10 Electric power and information technology dependencies

3.3.3.3 **Consequences.** Consultant shall use the DHS/FEMA threat and vulnerability assessment methodology to quantify the potential losses. For each facility, Consultant will rate each consequence on a scale of 1 (Very Low) to 10 (Very High) in the following four categories.

3.3.3.3.1 Human Impact. Effects on human life and physical wellbeing (e.g. fatalities, injuries).

3.3.3.3.2 Economic Impact. Direct and indirect effects on the economy with respect to the buildings and its functions.

3.3.3.3.3 Public Confidence. Effect on the public confidence in the organization to deliver service. This shall encompass those changes in perception emerging from a significant incident that affect the public's sense of safety and wellbeing.

3.3.3.3.4 Business Functionality. Effect on the business's ability to continue operations to delivery serve.

3.3.3.4 Risk Analysis

Using the confirmed threat, asset and vulnerability assessments, Consultant shall quantify the level of risk for each facility against each primary threat using the risk equation below. Consultant will tabulate an overall risk rating for each facility. The risks will be ranked high, medium and low.

	Low Risk	Medium Risk	High Risk
Risk Factors Total	1-60	61-175	>175

3.3.4 Recommendations

From the risk analysis, Consultant will develop a set of recommendations, prioritized by risk, for mitigating the vulnerabilities and enhancing the physical security measures and security systems.

3.3.5 Risk Assessment Workshop

Contactor shall schedule and conduct a virtual workshop with City's project team and key stakeholders to review and discuss the risk assessment and initial recommendations.

3.3.6 Task 4 Cost Analysis

Consultant will review the prioritized recommendations and develop a rough order of magnitude (ROM) cost estimate, divided into short and long-term costs. Consultant will use historic data, current market pricing and in some cases direct vendor estimates to prepare the cost estimates for the physical deterrents and security system improvements. Consultant will break down the cost estimate for each facility.

3.4 TASK 4 FINAL REPORT

Consultant's final report will include a threat and vulnerability assessment report; standard plans, details, and specifications for physical and operational security of substations yet to be completed; and an updated Utility Security Plan.

3.4.1 Threat and Vulnerability Assessment Draft Report

Consultant shall develop a draft report for SVP review. The draft report will include content developed during the previous tasks with the final content, recommendations, and appendices finalized in the draft report. The preliminary table of contents for the draft report will include:

3.4.1.1 An executive summary

3.4.1.2 An introduction with project scope, methodology and assumptions.

3.4.1.3 A findings summary with SWOT analysis.

3.4.1.4 A threat analysis.

3.4.1.5 A vulnerability assessment

3.4.1.6 A consequence analysis

3.4.1.7 A risk assessment summary

3.4.1.8 An evaluation matrix ranking risk based on threat vulnerability and consequence.

3.4.1.9 A prioritized set of recommendations with a focus on the security systems.

3.4.1.10 Rough-Order-of-Magnitude costs for the recommendations.

3.4.1.11 A summary report of each identified facility which may include:

3.4.1.11.1 A description of the facility and its key functions

3.4.1.11.2 A threat analysis

3.4.1.11.3 A vulnerability assessment of each site

3.4.1.11.4 A consequence analysis

3.4.1.11.5 A risk assessment matrix

3.4.1.11.6 Site-specific recommendations for mitigation

3.4.1.12 A set of appendices that includes a glossary and detailed crime statistics.

3.4.2 Consultant shall present the key elements of the Draft Threat and Vulnerability Assessment Report to SVP (and other stakeholders) at a virtual meeting.

3.4.3 After SVP review of the draft report, Consultant shall incorporate any changes recommended by SVP into the final report. Consultant will submit the Threat and Vulnerability Assessment Final Report to City staff for approval.

3.4.4 Standard Plans, Details and Specifications for Physical Security and Operational Security of Future Substations.

3.4.4.1 Upon completion of the Threat and Vulnerability Assessment Final Report, Consultant shall develop a base plan for a substation; design physical security components including perimeter fence/wall, equipment and communication line protection, gate security and access control, intrusion alarm, video cameras, and biometric identification systems. Consultant shall produce details and develop specifications for City's use.

3.4.4.2 Consultant shall include an evaluation of the City's current access control software for the two separate systems in its evaluation.

Consultant will make recommendations for new software if Consultant determines new software is warranted.

3.4.4.3 If Consultant determines new access control software is recommended, Consultant shall provide a comprehensive report supporting such recommendation. The comprehensive report will contain a cost benefit analysis, a resource analysis, and an impact analysis, along with an estimated timeline and other considerations.

3.4.5 Utility Security Plan Update

After completion of the Threat and Vulnerability Assessment Final Report, Consultant shall prepare an update to SVP's 2021 Utility Security Plan. This update shall, at minimum, include:

3.4.5.1 A detailed narrative explaining how SVP can take steps to implement a preventative maintenance plan for security equipment to ensure that mitigation measures are functional and performing adequately.

3.4.5.2 A description of Distribution and/or Security Control Center roles and actions related to distribution system physical security.

3.4.5.3 Recommendations that support and integrate with SVP's resiliency plans and activities.

3.4.5.4 Analysis of up to six (6) sites of the thirty-nine (39) sites identified in Section 1.1.

3.4.5.5 Sections for each of the following:

3.4.5.5.1 Overview

3.4.5.5.2 Background

3.4.5.5.3 Plan Development Process

3.4.5.5.4 Identification of Covered Distribution Facilities

3.4.5.5.5 Risk Assessment of Each Site

3.4.5.5.6 Covered Distribution Facility Mitigation Plans per Site

3.4.5.5.7 Independent Evaluation and Response

3.4.5.5.8 Validation

3.4.5.5.9 Narrative Descriptions for Utility Security Plan

SECTION 4. PROJECT SCHEDULE AND DELIVERABLES

4.1 Task 1. Project Start-Up

4.1.1 **Request for Background Material.** Consultant shall submit request for background material to City within the first two weeks after project start.

4.1.2 **Project Kick-Off Meeting.** Consultant shall schedule the project kick-off meeting no later than 2 weeks after submittal of request for background material.

4.2 Task 2. Data Collection and Evaluation

4.2.1 Within sixty (60) calendar days of project start, Consultant shall complete the following:

4.2.1.1 Site visits and facility walks

4.2.1.2 Key stakeholder interviews

4.2.1.3 Document review

4.2.1.4 Local and national research for threat analysis

4.3 Task 3. Findings Summary and Risk Analysis

4.3.1 **Findings Summary and Findings Meeting with City**. Within thirty (30) calendar days of completion of Task 2, Consultant shall produce a summary of findings and present the findings to the City for discussion.

4.3.2 **Risk Analysis.** Within thirty (30) calendar days of the findings meeting, Consultant shall:

4.3.2.1 Conduct the threat and vulnerability assessments

4.3.2.2 Prepare the initial risk analysis

4.3.2.3 Prepare initial recommendations based on the risk analysis

4.3.3 **Risk Assessment Workshop.** Within forty-five (45) calendar days after the findings meeting, Consultant shall conduct a risk assessment workshop with City.

4.3.4 **Cost Analysis.** Within fifteen (15) calendar days of the risk assessment workshop, Consultant shall complete the cost analysis.

4.4 Task 4. Final Reports.

4.4.1 **Threat and Vulnerability Assessment Report**.

4.4.1.1 Within forty-five (45) calendar days of the risk assessment workshop, Consultant shall complete the draft report and meet with City to discuss the draft report.

4.4.1.2 City shall review the draft report and provide comments to Consultant within fifteen (15) calendar days of the meeting.

4.4.1.3 Within fifteen (15) calendar days of receiving the City's comments on the draft report, Consultant shall submit the final report to the City.

4.4.2 **Substation Plans, Details, and Specifications.** Within sixty (60) calendar days after submittal of the final Threat and Vulnerability Assessment Report, Consultant shall provide City with the substation plans, details and specifications.

4.4.3 **2021 Utility Security Plan Update.**

4.4.3.1 Within forty-five (45) calendar days after the Consultant submits the Threat and Vulnerability Assessment Final Report to City, Consultant shall submit the draft Utility Security Plan Update to City for review.

4.4.3.2 City shall review draft Utility Security Plan Update and provide comments to Consultant within fifteen (15) calendar days.

4.4.3.3 Within seven (7) calendar days of receiving City's comments, Consultant shall submit to City the final Utility Security Plan Update.

4.5 Submission of Final Reports. Consultant will deliver three (3) hard copies of the final Threat and Vulnerability Assessment Report, Substation Plans, Details and Specifications, and the updated Utility Security Plan to the City and upload the digital format (pdf) of each report to the City's SFTP site.

SECTION 5. SPECIAL REQUIREMENTS

In accordance with SVP's CIP-013 Supply Chain Risk Management Program, the Consultant is required to complete a Vendor Risk Assessment and Attestation. In

delivering the services under this agreement, Consultant must adhere to SVP's Security Incident Response Plan outlined below

5.1 Definitions

5.1.1 Security Incident: A Security Incident is defined as (a) any breach event or known vulnerability or potential security flaw in the product delivered by Consultant to City and (b) any event perpetrated, or attempted, by Consultant, employee of Consultant, affiliate, subcontractor, or service provider working on behalf of Consultant providing services to City, including, but not limited to, unauthorized disclosure of non-public information, unauthorized remote or local use of data or materials, unauthorized access or change to any City system, product crashing due to third-party interference, embedded malware, or opening of unauthorized/undisclosed communication channels.

5.1.2 Banned Vendors or Products: Banned vendors or products are deemed to pose a threat to the U.S. bulk power system (BPS) or bulk electric system (BES) and are identified in U.S. executive orders or by federal government agencies including, but not limited to, the Department of Defense, Department of Energy, the Department of Homeland Security, the Federal Energy Regulatory Commission, or the North American Electric Reliability Corporation.

5.2 Notification of Security Incident

5.2.1 Consultant shall notify City immediately by email to designated SVP representative whenever a Security Incident occurs.

5.2.2 Anytime Consultant becomes aware of a Security Incident, Consultant must provide notice by email to the City contact identified in the Agreement and the SVP Project Manager, in the most expedient time possible and without unreasonable delay, but no more than five (5) business days after discovery. The notice shall include the date and time of the Security Incident occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of (a) how the Security Incident occurred (e.g., a precise description of the reason for the system failure (root cause analysis) to the extent known – interim reports are allowable), (b) the nature, type, and scope of the Security Incident including which products or system(s) that may be impacted, (c) the scope of City information known or reasonably believed to have been disclosed, and (d) the measures taken or planned to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

5.2.3 Consultant shall provide written updates of the notice to City addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those

new facts and circumstances. Consultant shall cooperate with City in City's efforts to determine the risk, if any, to the BES posed by the Security Incident, including providing additional information regarding the Security Incident upon request from City.

5.2.4 Consultant shall ensure a confirmation of receipt is received by the City for all initial and follow-up communication regarding the Security Incident.

5.3 Coordination of Responses Related to Security Incident

5.3.1 Development and Implementation of a Security Incident Response Plan.

5.3.1.1 To the extent practicable, Consultant shall share any documentation (policies, plan, and procedures), and any updates to such documentation, to address Security Incidents ("Response Plan") in place to mitigate the harmful effects of Security Incidents and addressing and remedying the occurrence to prevent the recurrence of Security Incidents in the future.

5.3.1.2 Consultant shall provide City access to inspect its Response Plan. The Response Plan should align with the best practices consistent with the contingency planning requirements of National Institute of Standards and Technology (NIST) Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 (and NIST SP 800-61 Rev. 3 upon its promulgation), and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended from time to time. In the event of a conflict between NIST and NERC, NERC will control.

5.3.1.3 As soon as practicable, understanding time is of the essence, upon learning of a Security Incident related to the products and services provided to City by Consultant, Consultant shall notify City of that implementation by contacting the designated SVP representative(s).

5.3.2 Prevention of Recurrence: As soon as practicable, understanding time is of the essence, Consultant shall provide recommendations, action plans, and/or mitigating controls to City on actions that City may take to assist in the prevention of recurrence, as applicable or appropriate.

5.3.3 Notification to Affected Parties: Consultant will, at its sole cost and expense, assist and cooperate with City with respect to any investigation of a Security Incident, to the extent the Security Incident involves or arises from Consultant-provided products or services, disclosures to affected parties, and other remedial measures as requested by City in connection with a Security Incident

or required under any applicable laws related to a Security Incident, to the extent necessary.

5.4 Verification of Software Integrity and Authenticity of Patches

5.4.1 Hardware, Firmware, Software, and Patch Integrity and Authenticity: Consultant shall comply with SVP's NERC CIP-010 Policy and Procedure regarding the verification of the identity of the patch source and the integrity of the software obtained from the source.

5.4.2 Computer Viruses and Malware: Consultant shall warrant that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Consultant will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

5.4.3 Remedies: If a virus or other malware is found to have been coded or otherwise introduced as a result of Consultant's product, service, actions, or negligence, Consultant shall immediately, and at its own cost take all necessary remedial action and provide assistance to City to eliminate the virus or other malware throughout City's information networks, computer systems, and information systems, regardless of whether such systems or networks are operated by or on behalf of City; and restoring previous functionality of the affected device, system, or product.

5.5 Controls for Remote Access

5.5.1 In the course of furnishing products and services to City under the Agreement, Consultant, or through any of their affiliates, subcontractors or service providers, shall not access, and shall not permit Consultant personnel to access City property, systems, or networks or City information without City's prior express written authorization. Such written authorization may subsequently be revoked by City at any time in City's sole discretion. Further, any Consultant personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by City. All City authorized connectivity or attempted connectivity to City's systems or networks shall be in conformity with City's security policies, including, but not limited to, those policies used to address the NERC CIP reliability standards, as may be amended from time to time.

5.5.2 Consultant shall maintain controls designed to protect City-issued credentials and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of City-issued credentials.

5.5.3 Prior to using any virtual private network (VPN) or other device to simultaneously connect machines on any City system or network to any machines on any Consultant or third-party systems, Consultant shall:

5.5.3.1 Complete and provide an SVP VPN request form with the full name of each individual who uses any such remote access method and the phone number and email address at which the individual may be reached while using the remote access method, and

5.5.3.2 Agree that any computer used by Consultant personnel to remotely access any City system or network will not simultaneously access the Internet or any other third-party system or network while logged on to City systems or networks.

5.5.3.3 Not be allowed to connect any of Consultant's computers to any of City system or network directly.

5.5.4 Consultant shall ensure that City-issued credentials issued to Consultant personnel for accessing City networks are not shared between Consultant personnel.

5.5.5 Consultant shall recommend any additional protective measures to address the security of remote and onsite access to City Information, City systems and networks, and City property.

5.6 Consultant Notification of Remote or Onsite Access Revocation

5.6.1 Consultant shall immediately take all steps necessary to remove Consultant personnel's access to any City Information, systems, networks, or property at such time when:

5.6.1.1 Any Consultant personnel no longer requires such access in order to furnish the services or products provided by Consultant under the Agreement,

5.6.1.2 Any Consultant personnel is terminated or suspended or his or her employment otherwise ends; or

5.6.1.3 Consultant reasonably believes any Consultant personnel poses a threat to the safe working environment at or to any City property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or employee or City Information.

5.6.2 Consultant shall notify City, no later than close of business on the same day as the day termination or change set forth in this section, occurs. Additionally, Consultant will notify City by contacting the SVP designated representative(s)

upon removal of access to City Information as well as City property, systems, and networks.

5.7 Consultant Cybersecurity Policy:

Consultant shall provide to City its cybersecurity policy and shall implement and comply with said cybersecurity policy.

5.8 Regulatory Examinations

5.8.1 Consultant agrees that any regulator or other governmental entity with jurisdiction over City and its affiliates, including but not limited to the North American Electric Reliability Corporation (NERC) and Western Electricity Coordinating Council (WECC), may examine Consultant's activities relating to the performance of its obligations under this Agreement to the extent such authority is granted to such entities under the law.

5.8.2 Consultant shall promptly cooperate with and provide all information reasonably requested by the regulator or other governmental entity in connection with any such examination and provide reasonable assistance and access to all equipment, records, networks, and systems requested by the regulator or other governmental entity.

5.8.3 Consultant shall comply with all reasonable recommendations that result from such regulatory examinations within reasonable timeframes at Consultant's sole cost and expense. The foregoing cooperation and assistance will be rendered at Consultant's then- current time and materials rates, subject to City's prior written authorization.

SECTION 6. E-BUILDER

6.1 Use of e-Builder. When required by City, Consultant shall use e-Builder for managing schedules, action items, and invoicing throughout the Term. e-Builder is a web-based construction management application hosted by e-Builder, Inc. For schedules, action items, and invoicing, e-Builder shall be the primary means of project information submission and management. Consultant shall not use e-builder for any confidential data including reports, plans, and deliverables which Contractor must submit to a City-controlled Secure File Transfer Protocol (SFTP) site provided by City.

6.2 Access to e-Builder. The City will establish the Consultant's access to e-Builder by providing licenses to Consultant's personnel at City's cost. The Consultant's designated users will be required to set up their computers/systems to use e-Builder in accordance with the e-Builder User Training Guide. The City reserves the right to limit the licenses issued to Consultant at any time.

6.3 E-builder Training. Consultant is required to obtain all necessary training to use the e-builder software. Consultant must participate in at least one classroom training or a web-based seminar as determined by City.

6.4 Connectivity to e-Builder. e-Builder is a web-based environment and therefore it is subject to the inherent speed and connectivity limitations of the Internet. Consultant is responsible for its own connectivity to the Internet. e-Builder's response time is dependent on the Consultant's equipment, including processor speed, Internet access speed, etc., and current traffic on the Internet. The City will not be liable for any delays associated with Consultant's use of e-Builder including, but not limited to slow response time, downtime periods, connectivity problems, or loss of information. The Consultant shall ensure connectivity to the e-Builder system whether at the home office or job site. Under no circumstances will Consultant's use of e-Builder be grounds for a time extension or cost adjustment to the Services.

6.5 Acceptance of Information. Data entered in a collaborative mode (entered with the intent to share as determined by permissions and workflows within the e-Builder system) by the City and the Consultant will be jointly owned. Consultant is responsible for managing, tracking, and documenting the Services provided and to comply with the requirements of this Agreement. The City's acceptance of documentation in e-builder via automated system notifications or audit logs extends only to the face value of the submitted documentation and does not constitute validation of the Consultant's submitted information.

6.6 Format of Project Documents. In addition to submittal of documents through e-Builder, at the City's sole discretion, the City may require Consultant to submit documents in hard copy format, or both electronic and hard copy format.

6.7 Project Communication. While regular email may still be used for communication, when requested by City, e-Builder shall be used as much as possible in connection with schedules, action items, and invoicing required in the performance of Services where City has directed the use of e-Builder. Where applicable, Consultant shall be responsible for scanning or otherwise converting to electronic format all schedules, action items, and invoicing documents, and uploading them to the e-Builder website. Consultant shall be responsible for the validity of its information placed in e-Builder. Consultant shall use the existing forms and processes in e-Builder to the maximum extent possible. If a required form does not exist in e-Builder, Consultant may include a form of its own or one provided by the City (if available) as an attachment to a submittal or process.

6.8 Archive Copies. When requested by City, Consultant shall keep an archive copy of all digital data created by Consultant, or submitted to Consultant via e-mail, or resident on e-Builder for the duration of the Agreement. Such data shall be available to City, and authorities with the jurisdiction (including funding agencies or representatives) on demand.

6.9 Should the City replace e-Builder with a different project management tool, Consultant, and subcontractors shall be required to use the new project management tool selected by the City.

SECTION 7. ADDITIONAL SERVICES

7.1 Additional Services are tasks or deliverables not outlined in Exhibit A, including services requested by the City beyond the agreed scope. Prior to commencing any Additional Services requested by City, Consultant shall submit a proposal outlining the Additional Services to be provided and the proposed price. If Additional Services are authorized, the Parties will execute an amendment to this Agreement which may require approval by the Santa Clara City Council.

EXHIBIT B
SCHEDULE OF FEES AND PAYMENT PROVISIONS

SECTION 1. MAXIMUM COMPENSATION

The maximum compensation payable to Consultant during the Term shall not exceed the amount in Section 6 of this Agreement.

SECTION 2. FIXED FEE FOR SCOPE OF SERVICES

Except for reimbursable expenses which are subject to the provisions of Section 3 of this Exhibit, compensation under this Agreement shall be a fixed fee in accordance with the fees outlined in Table B1 below. The fixed fees represent the total compensation for the scope of services outlined in Exhibit A. Payments for this fixed fee will be made according to the Payment Provisions in Section 5 below.

TABLE B1

Services/Task	Description	Fixed Fee
Task 0	Project Management	$ 13,500
Task 1	Project Startup	$ 8,100
Task 2	Data Collection	$ 57,960
Task 3	Risk Analysis	$ 84,970
Task 4	Final Reports: Threat and Vulnerability Assessment Report, Substation Plans, Details and Specifications, and Updated Utility Security Plan	$ 56,880
Optional Item	Comprehensive Report to support recommendation for new control access software described in Section 2.2.3	$ 12,600
Reimbursable Expenses – Not to Exceed		
Reimbursable Expenses	Printing and travel related costs – Pursuant to Section 3 of this Exhibit B	$ 12,342

Services/Task	Description	Fixed Fee
Total		$ 246,352

SECTION 3. REIMBURSABLE EXPENSES

3.1 Reimbursable Expenses. Contractor may pass through costs such as, but not limited to printing, materials, equipment, and travel as listed in the Reimbursable Expenses Schedule in this Section. Any and all reimbursable expenses related the Services shall be reimbursable only to the extent that (1) Consultant submits sufficient documentation to City that the expenses were directly incurred in providing the required Services, (2) Consultant demonstrates that such expenses aren't included in the hourly rate where applicable, (3) such expenses were approved in advance, (4) Consultant submits receipts, invoices, or other supporting documentation demonstrating that such reimbursable costs were incurred, and (5) any Mark Up conforms with the Reimbursable Expense Schedule below.

	Reimbursable Expense Schedule	Mark Up
1.	The cost of mailing, shipping and/or delivery of any documents or materials.	No Markup
2.	The cost of photographing, printing, reproducing and/or copying any documents or materials.	No Markup
3.	Costs for outside services (including subcontractor fees, equipment, materials, and facilities not furnished directly by Consultant).	Not to exceed 10%
4.	Consultant may charge allowable mileage at the prevailing IRS rate per mile. Mileage is not applicable to rental cars. Rental cars are reimbursed at actual fuel cost only.	No Markup
5.	Unless approved in writing (e-mail acceptable) in advance, reimbursement to Consultant (and any subconsultants or subcontractors) for meals, lodging, and related per diem will not exceed the rates outlined by United States General Services Administration (GSA). https://www.gsa.gov/travel-resources. Airfare or rental car, where applicable shall be at economy rates.	No Markup
6.	Other reimbursable expenses with prior written approval from the City.	No Markup

SECTION 4. RATE ADJUSTMENTS

4.1 In the event that Services extend beyond two years from the Effective Date, Consultant may propose an adjustment to the fees in Table B1.

4.2 Consultant shall notify the City ninety (90) days in advance of any proposed adjustment to fees. Consultant must be able to substantiate such adjustments to the satisfaction of the City.

4.3 If accepted, all adjustments to Table B1 must be approved by the City by executing an amendment to this Agreement.

SECTION 5. PAYMENT PROVISIONS

5.1 Payment Schedule for Scope of Services (Fixed Fee):

5.1.1 Consultant shall provide a monthly invoice for the percentage of the services completed in the preceding month, provided that the total amount billed for each task does not exceed the amounts as outlined in Table B1. Each invoice must include the following information:

5.1.1.1 Invoice Number and Invoice Period.

5.1.1.2 Current amount due for each task.

5.1.1.3 Sufficient detail for City to verify the fixed fees in Table B1 have not been exceeded.

5.2 Pre-Payment. City shall not be required to pay a deposit or any other form of pre-payment prior to Consultant beginning the Services.

5.3 Payment Limited to Satisfactory Work. Consultant is not entitled to any payments until the City concludes that the Services and/or any furnished deliverables have been satisfactorily performed.

5.4 Accurate Invoice. If the invoice submitted by Consultant is not accurate, the invoice will be returned to Consultant to correct and resubmit before payment can be processed.

5.5 Payment. If there are no discrepancies or deficiencies in the submitted invoice and Consultant has submitted all required documentation, City shall process the invoice for payment.

5.6 Confidential. Invoices are not confidential even if marked as confidential when submitted.

EXHIBIT C
INSURANCE REQUIREMENTS

Without limiting the Consultant's indemnification of the City, and prior to commencing any of the Services required under this Agreement, the Consultant shall provide and maintain in full force and effect during the period of performance of the Agreement and for twenty-four (24) months following acceptance by the City, at its sole cost and expense, the following insurance policies from insurance companies authorized to do business in the State of California. These policies shall be primary insurance as to the City of Santa Clara so that any other coverage held by the City shall not contribute to any loss under Consultant's insurance. The minimum coverages, provisions and endorsements are as follows:

A. COMMERCIAL GENERAL LIABILITY INSURANCE

1. Commercial General Liability Insurance policy which provides coverage at least as broad as Insurance Services Office form CG 00 01. Policy limits are subject to review, but shall in no event be less than, the following:

   $1,000,000 Each Occurrence
   $2,000,000 General Aggregate
   $2,000,000 Products/Completed Operations Aggregate
   $1,000,000 Personal Injury

2. Exact structure and layering of the coverage shall be left to the discretion of Consultant; however, any excess or umbrella policies used to meet the required limits shall be at least as broad as the underlying coverage and shall otherwise follow form.

3. The following provisions shall apply to the Commercial Liability policy as well as any umbrella policy maintained by the Consultant to comply with the insurance requirements of this Agreement:

   a. Coverage shall be on a "pay on behalf" basis with defense costs payable in addition to policy limits;

   b. There shall be no cross liability exclusion which precludes coverage for claims or suits by one insured against another; and

   c. Coverage shall apply separately to each insured against whom a claim is made or a suit is brought, except with respect to the limits of liability.

B. BUSINESS AUTOMOBILE LIABILITY INSURANCE

Business automobile liability insurance policy which provides coverage at least as broad as ISO form CA 00 01 with policy limits a minimum limit of not less than one million dollars ($1,000,000) each accident using, or providing coverage at least as broad as, Insurance Services Office form CA 00 01. Liability coverage shall apply to all owned (if any), non-owned and hired autos.

C. WORKERS' COMPENSATION

1. Workers' Compensation Insurance Policy as required by statute and employer's liability with limits of at least one million dollars ($1,000,000) policy limit Bodily Injury by disease, one million dollars ($1,000,000) each accident/Bodily Injury and one million dollars ($1,000,000) each employee Bodily Injury by disease.

2. The indemnification and hold harmless obligations of Consultant included in this Agreement shall not be limited in any way by any limitation on the amount or type of damage, compensation or benefit payable by or for Consultant or any subconsultant under any Workers' Compensation Act(s), Disability Benefits Act(s) or other employee benefits act(s).

3. This policy must include a Waiver of Subrogation in favor of the City of Santa Clara, its City Council, commissions, officers, employees, volunteers and agents.

D. PROFESSIONAL LIABILITY

Professional Liability or Errors and Omissions Insurance as appropriate shall be written on a policy form coverage specifically designed to protect against negligent acts, errors or omissions of the Consultant. Covered services as designated in the policy must specifically include work performed under this agreement. Coverage shall be in an amount of not less than one million dollars ($1,000,000) per claim or two million dollars ($2,000,000) aggregate. Any coverage containing a deductible or self-retention must first be approved in writing by the City Attorney's Office.

E. COMPLIANCE WITH REQUIREMENTS

All of the following clauses and/or endorsements, or similar provisions, must be part of each commercial general liability policy, and each umbrella or excess policy.

1. Additional Insureds. City of Santa Clara, its City Council, commissions, officers, employees, volunteers and agents are hereby added as additional insureds in respect to liability arising out of Consultant's work for City, using

Insurance Services Office (ISO) Endorsement CG 20 10 11 85, or the combination of CG 20 10 03 97 and CG 20 37 10 01, or its equivalent.

2. Primary and non-contributing. Each insurance policy provided by Consultant shall contain language or be endorsed to contain wording making it primary insurance as respects to, and not requiring contribution from, any other insurance which the indemnities may possess, including any self-insurance or self-insured retention they may have. Any other insurance indemnities may possess shall be considered excess insurance only and shall not be called upon to contribute with Consultant's insurance.

3. Cancellation.

   a. Each insurance policy shall contain language or be endorsed to reflect that no cancellation or modification of the coverage provided due to non-payment of premiums shall be effective until written notice has been given to City at least ten (10) days prior to the effective date of such modification or cancellation. In the event of non-renewal, written notice shall be given at least ten (10) days prior to the effective date of non-renewal.

   b. Each insurance policy shall contain language or be endorsed to reflect that no cancellation or modification of the coverage provided for any cause save and except non-payment of premiums shall be effective until written notice has been given to City at least thirty (30) days prior to the effective date of such modification or cancellation. In the event of non-renewal, written notice shall be given at least thirty (30) days prior to the effective date of non-renewal.

4. Other Endorsements. Other endorsements may be required for policies other than the commercial general liability policy if specified in the description of required insurance set forth in Sections A through E of this Exhibit C, above.

F. ADDITIONAL INSURANCE RELATED PROVISIONS

Consultant and City agree as follows:

1. Consultant agrees to ensure that subconsultants, and any other party involved with the Services, who is brought onto or involved in the performance of the Services by Consultant, provide the same minimum insurance coverage required of Consultant, except as with respect to limits. Consultant agrees to monitor and review all such coverage and assumes all responsibility for ensuring that such coverage is provided in conformity with the requirements of this Agreement. Consultant agrees that upon

request by City, all agreements with, and insurance compliance documents provided by, such subconsultants and others engaged in the project will be submitted to City for review.

2. Consultant agrees to be responsible for ensuring that no contract used by any party involved in any way with the project reserves the right to charge City or Consultant for the cost of additional insurance coverage required by this Agreement. Any such provisions are to be deleted with reference to City. It is not the intent of City to reimburse any third party for the cost of complying with these requirements. There shall be no recourse against City for payment of premiums or other amounts with respect thereto.

3. The City reserves the right to withhold payments from the Consultant in the event of material noncompliance with the insurance requirements set forth in this Agreement.

G. EVIDENCE OF COVERAGE

Prior to commencement of any Services under this Agreement, Consultant, and each and every subconsultant (of every tier) shall, at its sole cost and expense, provide and maintain not less than the minimum insurance coverage with the endorsements and deductibles indicated in this Agreement. Such insurance coverage shall be maintained with insurers, and under forms of policies, satisfactory to City and as described in this Agreement. Consultant shall file with the City all certificates and endorsements for the required insurance policies for City's approval as to adequacy of the insurance protection.

H. EVIDENCE OF COMPLIANCE

Consultant or its insurance broker shall provide the required proof of insurance compliance, consisting of Insurance Services Office (ISO) endorsement forms or their equivalent and the ACORD form 25-S certificate of insurance (or its equivalent), evidencing all required coverage shall be delivered to City, or its representative as set forth below, at or prior to execution of this Agreement. Upon City's request, Consultant shall submit to City copies of the actual insurance policies or renewals or replacements. Unless otherwise required by the terms of this Agreement, all certificates, endorsements, coverage verifications and other items required to be delivered to City pursuant to this Agreement shall be emailed to ctsantaclara@ebix.com, or by mail to:

EBIX Inc.
City of Santa Clara – Silicon Valley Power
P.O. Box 100085 – S2
Duluth, GA 30096

Telephone number: 951-766-2280

Fax number: 770-325-0409

I. QUALIFYING INSURERS

ALL OF THE INSURANCE COMPANIES PROVIDING INSURANCE FOR CONSULTANT SHALL HAVE, AND PROVIDE WRITTEN PROOF OF, AN A. M. BEST RATING OF AT LEAST A MINUS 6 (A- VI) OR SHALL BE AN INSURANCE COMPANY OF EQUAL FINANCIAL STABILITY THAT IS APPROVED BY THE CITY OR ITS INSURANCE COMPLIANCE REPRESENTATIVES.