AMENDMENT NO. 1
TO THE AGREEMENT FOR THE PERFORMANCE OF SERVICES
BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA
AND
GRID SUBJECT MATTER EXPERTS, LLC

PREAMBLE

This agreement ("Amendment No. 1") is entered into between the City of Santa Clara, California, a chartered California municipal corporation (City) and Grid Subject Matter Experts, LLC a Delaware limited liability company, (Contractor). City and Contractor may be referred to individually as a "Party" or collectively as the "Parties" or the "Parties to this Agreement."

RECITALS

A. The Parties previously entered into an agreement entitled "Agreement for the Performance of Services by and Between the City of Santa Clara, California, and Grid Subject Matter Experts, Inc., dated July 26, 2018 (Agreement); and

B. The Parties entered into the Agreement for the purpose of having Contractor provide North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Compliance Program, and the Parties now wish to amend the Agreement as Amended to extend the term and increase the maximum compensation.

NOW, THEREFORE, the Parties agree as follows:

AMENDMENT TERMS AND CONDITIONS

1. Section 5 of the Agreement as Amended, entitled "TERM OF AGREEMENT" is amended to read as follows: Unless otherwise set forth in this Agreement or unless this paragraph is subsequently modified by a written amendment to this Agreement, the term of this Agreement shall begin on July 26, 2018 and expire on July 26, 2024.

   After the Initial Term, the City reserves the right, at its sole discretion, to extend the term of this Agreement for one additional three-year term through July 26, 2027 ("Option Periods"). City shall provide Contractor with no less than thirty (30) days prior written notice of its intention to exercise its option to extend the term of this Agreement. Exhibit B of the Agreement as Amended, entitled "SCHEDULE OF FEES" is amended to read as follows: In no event shall the amount billed to City by Contractor for services under this Agreement exceed three hundred thousand dollars, subject to budget appropriations.

1. Exhibit A – Scope of Services shall be deleted and replaced with the attached Exhibit A – Scope of Services – Amended July 15, 2021.
2. Exhibit B – Schedule of Fees shall be deleted and replaced with the attached Exhibit B – Compensation and Fee Schedule – Amended July 15, 2021
3. Exhibit F – Milestone Schedule shall be deleted and replaced with Exhibit F – Notice of Exercise Option to Extend Agreement

4. Except as set forth herein, all other terms and conditions of the Agreement shall remain in full force and effect. In case of a conflict in the terms of the Agreement and this Amendment No. 1, the provisions of this Amendment No. 1 shall control.

The Parties acknowledge and accept the terms and conditions of this Amendment No. 1 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: Dated: _____

BRIAN DOYLE
City Attorney

DEANNA J. SANTANA
City Manager
1500 Warburton Avenue
Santa Clara, CA 95050
Telephone: (408) 615-2210
Fax: (408) 241-6771

"CITY"

GRID SUBJECT MATTER EXPERTS, LLC
A DELAWARE LIMITED LIABILITY COMPANY

Dated: _____
By (Signature): _____
Name: _____
Title: _____
Principal Place of Business Address: (to be filled in by City staff)
Email Address: _____
Telephone: ( )
Fax: ( )

"CONTRACTOR"

AMENDMENT NO. 1
TO THE AGREEMENT FOR THE PERFORMANCE OF SERVICES
BY AND BETWEEN THE CITY OF SANTA CLARA, CALIFORNIA AND
GRID SUBJECT MATTER EXPERTS, LLC.

EXHIBIT A – SCOPE OF SERVICES – AMENDED JULY 15, 2021

Contractor will provide support services for Supervisory control and Data Acquisition (SCADA) and North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance for the City of Santa Clara Electric Utility, Silicon Valley Power (SVP) as defined below:

1. As-Needed SCADA Support and Maintenance including:

    1.1. Supporting SCADA system issues when they arise,

    1.2. Providing audit support for the new SCADA system (including baseline setup and support, patch tracking, logs, etc.), and

    1.3. Preparing the system for any new or upcoming regulatory changes.

2. CIP-004 Training Maintenance including:

    2.1. Provide as-needed training updates to support SVP's compliance with CIP-004 using SVP's emPower Learning Management System (LMS).

    2.2. Keep the training up to date and relevant to SVP's operations including ongoing updates related to items identified through Contractors support of SVP's SCADA system.

3. New 2021 CIP Compliance Requirement Implementation:

    3.1. Contractor's GridSecurity and Compliance teams will work together to support the preparation and implementation of SVP's SCADA system and compliance program in response to any new CIP Standards or Requirements such as the transition from v3 to v5 recently supported by Contractor

    3.2. Provide a team available to help SVP remain compliant with any new CIP Standards that become enforceable.

4. Periodic Vulnerability Assessment:

    4.1. Upon request of SVP, Contractor will provide SVP with a cyber-vulnerability assessment.

    4.2. The proposed assessment is focused on cyber-security best practices and takes into account NERC CIP requirements and also evaluates the other important cyber systems that relied on by SVP.

    4.3. In this assessment, Contractor will focus first on the cyber systems physically located at SVP's control center, as well as assess any cyber systems that

directly interact with the control center to the extent those systems could impact the control center.

4.4. Preparation for assessment:

4.4.1. In order to understand the network topology, verify the initial list of in-scope devices, and better focus the efforts of the vulnerability assessment, Contractor will review technical CIP documentation of the control center. City shall make any required documents available to contractor to support the assessment. The following list is a sample of needed documents. Prior to an assessment, Contractor shall provide a list of documents needed and City shall provide documents in a timely manner.

4.4.1.1. CIP-002 Asset.device lists

4.4.1.2. CIP-004 Access management lists

4.4.1.3. CIP-005 Network diagrams

4.4.1.4. CIP-007 Ports and services evidence

4.4.1.5. CIP-007 Logging evidence

4.4.1.6. Patch management evidence

4.4.1.7. Known default accounts

4.4.1.8. Configuration baselines

4.4.1.9. Vulnerability assessment results

4.4.2. As part of the preparation phase, Contractor will coordinate with SVP staff to identify and establish out-of-scope systems, optimal scanning times, communication points-of-contact, and access rights. Whenever possible, SVP shall administrative access to systems so that credentialed scans are able to identify critical vulnerabilities that are otherwise not discoverable by non- intrusive testing.

4.5. Technical:

4.5.1. Passive Scanning: In order to validate the network topology information obtained from network diagrams, asset lists, etc., Contractor performs passive scanning techniques.

If requested, Contractor will continuously monitor network traffic in order to automatically discover users, unpatched assets, and other potential vulnerabilities. This requires a SPAN or mirrored port to be configured by City.

4.5.2. Active Scanning: During this stage, Contractor uses network scanning tools to identify vulnerable hosts on the network.

4.5.2.1. Contractor scans firmware versions, applications, and configurations for potential attack vectors. While these are not actual intrusion attempts, active scanning may cause undesired operation in older equipment—Contractor will configure the scan parameters in order to reduce the risk of this occurring.

4.5.2.2. Additionally, any potential vulnerabilities identified during the passive scans are investigated further using active scanning techniques.

4.5.3. As part of the onsite assessment, Contractor will evaluate SVP's physical security posture

4.6. Evaluation

4.6.1. Contractor will evaluates the information obtained during the active and passive scans especially reviewing vulnerabilities identified by the software tools and removing false positives or vulnerabilities that are not applicable to the SVP environment.

4.6.2. Contractor compares in detail the findings of the assessment and the CIP evidence provided during the preparation phase.

4.6.3. Contractor summarizes results in a "punch-list" report. The punch list report details the results of the assessment and any identified vulnerabilities, including but not limited to the following:

4.6.3.1. Configuration evaluation such as, but not limited to overly permissive firewall rules, broadcast domains or VLANs trunked to untrusted devices, default passwords, or reduced security posture

4.6.3.2. Passive scan results such as, but not limited to hosts not documented in network diagrams/asset lists

4.6.3.3. Active scan results such as, but not limited to configuration vulnerabilities, missing patches, known vulnerabilities, available attack vectors

4.6.3.4. Active scan results such as, but not limited to configuration vulnerabilities, missing patches, known vulnerabilities, available attack vectors

4.6.3.5. Discrepancies between CIP evidence and findings

4.6.4. Contractor will prioritize each identified based on the risk that vulnerability poses to SVP. Additionally, for each finding, Contractor shall document an action plan for handling the risk associated with the vulnerability including estimated costs and level of effort. The action plan proposes the technical and procedural measures for eliminating or mitigating the risk.

5. Contractor shall comply with all provisions of Exhibit A1 – Special Requirements.

AMENDMENT NO. 1
TO THE AGREEMENT FOR THE PERFORMANCE OF SERVICES
BY AND BETWEEN THE CITY OF SANTA CLARA, CALIFORNIA AND
GRID SUBJECT MATTER EXPERTS, LLC.

EXHIBIT A1 – SPECIAL REQUIREMENTS

1. Definitions

1.1. Security Incident: A Security Incident is defined as any breach event or known vulnerability or potential security flaw in the product delivered, or proposed to be delivered, to City. Any event perpetrated, or attempted, by any employee, contractor, or other provider working on behalf of Contractor delivering services to City. This shall include, but is not limited to, unauthorized disclosure of non-public information, unauthorized remote or local use of subject product, unauthorized changes to product or to any other City system, product crashing due to third-party interference, embedded malware, or opening of unauthorized/undisclosed communication channels.

1.2. Banned Vendors or Product: 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

2. Contractor Notification of Security Incident

2.1. Contractor agrees to notify City immediately by email, whenever a Security Incident occurs.

2.2. Anytime Contractor becomes aware of a Security Incident, Contractor must provide notice by email to City contact person identified in this Agreement and the SVP CIP Sr. Manager, as soon as possible, 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.

2.3. Contractor 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. Contractor shall cooperate with City in

City's efforts to determine the risk, if any, to the Bulk Electric System (BES) posed by the Security Incident, including providing additional information regarding the Security Incident upon request from City.

2.4. Contractor shall ensure a confirmation of receipt is received for all initial and follow-up communication regarding the Security Incident.

3. Contractor Coordination of Responses related to Security Incident

3.1. Development and Implementation of a Security Incident Response Plan: To the extent practicable, Contractor 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. Contractor shall provide City access to inspect its Response Plan, if available. 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 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.

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 Contractor, Contractor shall notify City of that implementation by contacting the CIP Senior Manager, at jipsaro@SantaClaraCA.gov, and SVP Systems Support at SVPsupport@SantaClaraCA.gov].

3.2. Prevention of Recurrence: As soon as practicable, understanding time is of the essence, Contractor 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.

3.3. Notification to Affected Parties: Contractor 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 Contractor-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.

4. Verification of Software Integrity and Authenticity of Patches

4.1. Hardware, Firmware, Software, and Patch Integrity and Authenticity: Contractor shall comply with SVP''s 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.

4.2. Viruses, Firmware and Malware:

4.2.1 Contractor will make commercially reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to City.

4.2.2 Contractor warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Contractor 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.

4.2.3 If a virus or other malware is found to have been coded or otherwise introduced as a result of Contractor's product, service, actions, or negligence, Contractor 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. Controls for Remote Access

Contractors that directly, or through any of their affiliates, subcontractors or service providers, connect to City's systems or networks agree to comply with the following protective measures:

5.1. In the course of furnishing products and services to City under this Agreement, Contractor shall not access, and shall not permit Contractor 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 Contractor 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 with notice to the Contractor.

5.2. Contractor shall demonstrate 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.

5.3. Prior to using any virtual private network or other device to simultaneously connect machines on any City system or network to any machines on any Contractor or third-party systems, Contractor shall:

5.3.1. Provide City 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

5.3.2. Agree that any computer used by Contractor 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.

5.4. Contractor shall ensure that City-issued credentials issued to Contractor Personnel for accessing City networks are not shared between Contractor Personnel.

5.5. Contractor 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. Contractor Cybersecurity Policy: Contractor will provide to City the Contractor's cybersecurity policy, and agrees to implement and comply with that cybersecurity policy.

5.7. Return or Destruction of City Information: Upon completion of the delivery of the products and services to be provided under this Agreement, or at any time upon City's request, Contractor will return to City all hardware and removable media provided by City containing City Information. If the hardware or removable media containing City Information is owned by Contractor or a third-party, a statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction will be sent to a designated City security representative within fifteen (15) calendar days after completion of the delivery of the products and services to be provided under this Agreement, or at any time upon City's request.

5.8. Audit Rights: City or its third-party designee may, but is not obligated to, perform audits and security tests of Contractor's IT or systems environment and procedural controls to determine Contractor's compliance with the system, network, data, and information security requirements of this Agreement. Contractor shall provide all information reasonably requested by City in connection with any such audits and shall provide reasonable access and assistance to City upon request. Contractor will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits.

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

6. Contractor Notification of Remote or Onsite Access Revocation

6.1. Revocation: Contractor will immediately take all steps necessary to remove Contractor Personnel's access to any City Information, systems, networks, or property at such time when:

6.1.1. any Contractor Personnel no longer requires such access in order to furnish the services or products provided by Contractor under this Agreement;

6.1.2. any Contractor Personnel is terminated or suspended or his or her employment otherwise ends; or

6.1.3. Contractor reasonably believes any Contractor 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.

6.2. Notification: Contractor will notify City, no later than close of business on the same day as the day termination or change set forth this section, occurs. Additionally, Contractor will notify City by contacting the CIP Senior Manager, at jipsaro@SantaClaraCA.gov, and SVP Systems Support at SVPsupport@SantaClaraCA.gov, upon removal of access to City Information as well as City property, systems, and networks.

AMENDMENT NO. 1 TO THE AGREEMENT FOR THE PERFORMANCE OF SERVICES BY AND BETWEEN THE CITY OF SANTA CLARA, CALIFORNIA AND GRID SUBJECT MATTER EXPERTS, LLC.

EXHIBIT B – COMPENSATION AND FEE SCHEDULE – AMENDED JULY 15, 2021

1. MAXIMUM COMPENSATION

1.1. The maximum amount of compensation to be paid to Contractor during the Initial Term shall not exceed three hundred thousand dollars ($300,000.00). City does not guarantee any minimum compensation under this Agreement.

1.2. Any work or materials requested by the City that exceeds the Maximum Compensation shall require the execution of an amendment to this Agreement before the commencement of work.

2. RATES:

City shall pay Contractor in accordance with the rates listed in the following table:

Position	Hourly Rates
Executive or Vice President	$250.00
Director, Principal Consultant, or Principal Security Architect	$225.00
Consultant or Technical Expert	$200.00
Specialist or Technical Analyst	$175.00
Associate Specialist or Associate Technical Analyst	$150.00
Staff Analyst, Technical Writer, or Project Manager/Administrator	$125.00

3. REIMBURSABLE EXPENSES

3.1. Pass-Through Costs:

3.1.1. In some cases, Contractor may pass-through costs such as, but not limited to, subcontracted activities or materials.

3.1.2. When these Pass-Through Costs occur, Contractor will invoice City for these costs without markup.

3.1.3. Contractor shall provide supporting documentation such as invoices or receipts for all Pass-Through costs.

3.1.4. Except in the case of emergency, Contractor will notify the City in advance when these costs are anticipated.

3.2. Reimbursement of expenses is subject to the following conditions.

3.2.1. Expenses shall be reimbursable only to the extent that the Contractor submits sufficient documentation to the City that the

expenses were directly incurred in providing the requested services and that such costs are not already included in the fee or hourly rate.

3.2.2. Travel-related expenses (mileage, lodging, meals, etc.).

3.2.2.1. Unless approved in writing (e-mail acceptable) in advance, meals, lodging, and related Per Diem shall not exceed the rates outlined by United States General Services Administration (GSA).

https://www.gsa.gov/travel-resources

3.2.2.2. The City shall not reimburse local travel (within Santa Clara County).

4. PAYMENT PROVISIONS

Contractor will bill City on a monthly basis for Services provided by Contractor during the preceding month on an invoice and in a format approved by City and subject to verification and approval by City. City will pay Contractor within thirty (30) days of City's receipt of an approved invoice.