REQUEST FOR INFORMATION

1.0 Description

1.1 Silicon Valley Clean Energy Authority (SVCEA) in support of the Finance and Administration Department is seeking information on how an interested consultant could identify cybersecurity risks and access cybersecurity preparedness in the community choice aggregation sector.

1.2 THIS IS A REQUEST FOR INFORMATION (RFI) ONLY. This RFI is issued solely for information and planning purposes – it does not constitute a Request for Proposal (RFP) or a promise to issue an RFP in the future. This request for information does not commit SVCEA to contract for any supply or service whatsoever. Further, SVCEA is not at this time seeking proposals and will not accept unsolicited proposals. Responders are advised that SVCEA will not pay for any information or administrative costs incurred in response to this RFI, all costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future RFP, if any is issued. If a solicitation is released, it will be posted on the SVCEA website at https://svcleanenergy.org. It is the responsibility of the potential offerors to monitor these sites for additional information pertaining to this requirement.

2.0 Background

2.1 SVCEA is a community choice aggregator (CCA) formed in March 2016 as a Joint Powers Authority serving most of Santa Clara County with carbon free electricity. SVCEA is a public agency with a thirteen (13) member Board of Directors representing each community that we serve. SVCEA partners with Pacific Gas and Electric (PG&E) as PG&E operates the transmission and distribution systems to deliver the electricity that SVCEA procures.

As the CCA sector continues to evolve and mature, the importance of cybersecurity to the integrity of grid reliability and customer data protection has been underscored by SVCEA senior management and board directors.

3.0 Requested Information

3.1 In order to promote better compliance practices and inform staff and board directors understanding of cybersecurity preparedness, this RFI will focus on the following areas:

3.1.1 Governance and Risk Assessment: Responders should provide information regarding best practices for firms evaluating cybersecurity risks and what controls and risk assessment processes are recommended specifically for the Electric Utility and/or CCA type business. Responders may comment on the level of communication to, and involvement of, senior management and board of directors.

3.1.2 Access Right and Controls: SVCEA may be particularly at risk of a data breach from a failure to implement basic controls to prevent unauthorized access to systems of information. Responders may comment on how firms control access to various systems and data via management or user credentials, authentication, and authorization methods. Comments may include a review of controls associated with remote access, passwords, network segmentation and tiered access.

3.1.3 Data Loss Prevention: Some data breaches may have resulted from the absence of robust controls in the areas of patch management and system configuration. Responders may comment on how firms monitor the volume of content transferred outside of the agency by its employees or through third parties, such as email attachments or uploads. Responders may also comment how firms monitor potentially unauthorized data transfers and may comment how firms verify the authenticity of a customer request to transfer funds.

3.1.4 Vendor Management: Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms. As a result, responders should focus on SVCEA practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring, and oversight of vendors, and contract terms. responders may comment on assessment of how vendor relationships are considered as part of SVCEA's ongoing risk assessment process as well as how SVCEA determines appropriate level of due diligence to conduct on a vendor.

3.1.5 Training: Without proper training, employees and vendors may put SVCEA's data at risk. Some data breaches may result from unintentional employee actions such as a misplaced laptop, accessing data through an unsecured internet connection, or opening messages or downloading attachments from an unknown source. With proper training, however, employees and vendors can be the agency's first line of defense, such as by alerting IT to suspicious activity and understanding and following agency protocols with respect to technology. Responders may focus on how training is tailored to specific job functions and how training is designed to encourage responsible employee and vendor behavior.

Responders may comment how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training.

3.1.6 Incident/Management Response: responders may comment on best practices for established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events. Comments may include which SVCEA data, assets, and services warrant most protection to help prevent attacks from causing significant harm.

3.1.7 Responders may comment on additional areas of cybersecurity-related risks.

3.1.8 Security Policies: Development and maintenance.

3.1.9 Security Framework: containing standards, procedures, measurement.

3.1.10 Vulnerability Management: monitoring, alerting and remediation.

3.1.11 Privacy: As new regulations emerge, there are opportunities for integrating best practices around personal data & information security. Provide a framework for creating transparency and an essential Cybersecurity roadmap for building and leveraging current attention and focus.

4.0 Responses

4.1 Interested parties are requested to respond to this RFI with a white paper.

4.2 White papers in Microsoft Word for Office 2010 compatible format are due no later than **March 31 2019, 5:00 PM PST**. Responses shall be limited to 25 pages for Section 3 and submitted via email only to svceRMIrequests@svcleanenergy.org. Proprietary information, if any, should be minimized and MUST BE CLEARLY MARKED. To aid SVCEA, please segregate proprietary information. Please be advised that all submissions become SVCEA property and will not be returned.

4.3 Section 1 of the white paper shall provide administrative information, and shall include the following as a minimum:

4.3.1 Name, mailing address, overnight delivery address (if different from mailing address), phone number, fax number (if applicable), and e-mail of designated point of contact

4.3.2 Recommended consulting strategy.

4.3.3 Either 1) copy of executed non-disclosure agreement (NDA) with SVCEA or 2) a statement that the responder will not allow SVCEA to release its proprietary data to SVCEA support consultants.

The number of pages in Section 1 of the white paper shall not be included in the 25 page limitation, i.e., the 25 page limitation applies only to Section 3 of the white paper.

5.0 Sector Discussions

5.1 SVCEA representatives may or may not choose to meet with potential offerors. Such discussions would only be intended to get further clarification of potential capability to meet the requirements, especially any development and certification risks.

6.0 Questions

6.1 Questions regarding this announcement shall be submitted in writing by e-mail to the Management Analyst, svceRMIrequests@svcleanenergy.org. Verbal questions will NOT be accepted. Questions will be answered by posting answers to the SVCEA Cybersecurity FAQ. Accordingly, questions shall NOT contain proprietary or classified information. SVCEA does not guarantee that questions received after March 15, 2019 will be answered.

7.0 Summary

7.1 THIS IS A REQUEST FOR INFORMATION (RFI) ONLY to identify sources that can provide cybersecurity services. The information provided in the RFI is subject to change and is not binding on SVCEA. SVCEA had not made a commitment to procure any of the items discussed, and release of this RFI should not be construed as such a commitment or as authorization to incur cost for which reimbursement would be required or sought. All submissions become SVCEA property and will not be returned.