SOUTHERN CALIFORNIA PUBLIC POWER AUTHORITY

Request for Proposals for Cybersecurity Services
Issuance Date: February 8, 2019
Response Deadline: March 11, 2019

I. Introduction

The Southern California Public Power Authority (SCPPA), on behalf of its Member Utilities, is hereby soliciting competitive proposals for Cybersecurity Services, as described below in Section III.

SCPPA is interested in discovering all Respondent's capabilities related to specified Areas of Interest and associated pricing to enable informed decisions and potentially proceed to more specific negotiations on contract development with one or more qualified Respondents to this Request for Proposals (RFP).

Responses to this RFP are due on or before March 11, 2019, as described below in Sections III and V.

II. Background

SCPPA is a joint powers authority and a public entity organized under the California Joint Exercise of Power Act found in Chapter 5 of Division 7 of Title 1 of the Government Code of the State of California, and through the SCPPA Joint Powers Agreement, for the purposes of planning, financing, developing, acquiring, constructing, operating and maintaining projects for the generation or transmission of electric energy. SCPPA also facilitates joint service contracts, at the request of its members, to aggregate like project efforts among its Members for the purposes of developing energy efficiency, demand response and resource procurement Programs or Projects to improve operating efficiencies and reduce costs.

Membership of SCPPA consists of eleven cities and one irrigation district, which supply electric energy within Southern California, including the municipal utilities of the cities of Anaheim, Azusa, Banning, Burbank, Cerritos, Colton, Glendale, Los Angeles, Pasadena, Riverside, and Vernon, and the Imperial Irrigation District. SCPPA is governed by its Board of Directors, which consists of representatives from each of its Members. The management of SCPPA is under the direction of an Executive Director who is appointed by the Board.

Any service contract subsequently entered into by SCPPA pursuant to this RFP would be utilized directly by the interested Members to serve their respective utility customers' needs. The service and work products would be ordered and approved directly by SCPPA and/or the applicable Members and the billing would be administered through SCPPA.

III. Areas of Interest

Certain SCPPA Members have expressed interest in in SCPPA securing bids to perform certain services related to Cybersecurity Services to meet the needs of their municipality as outlined below. SCPPA is requesting proposals from qualified firms or individuals that will demonstrate an ability to perform such services and functions.

A. Scope of Work

The successful Respondents to this RFP shall assist member utilities in advisory, vulnerability assessment, and remediation efforts related to cybersecurity within the member utility. The consultant's services can include advisory services, vulnerability assessment services, penetration testing services, incident response services, remediation services, and training services. Services can include all program and project management functions related to these activities. The services will use a task order-based approach.

Advisory services can include identification of cybersecurity and related physical security weaknesses, identifying potential risks, and offering advice on how to safeguard information and systems related to Information Technology (IT), Operating Technology/Industrial Control Systems (OT/ICS), and Internet of Things (IoT). Focus can include people, policy and process evaluation, service provider evaluation, vulnerability management, cybersecurity resilience assessments, compliance programs, and leadership. These services focus on holistic and technical review and reporting.

Vulnerability assessment services can include holistic people, processes, and technology review of the utility's environment, which can include corporate infrastructure, control system infrastructure, cyber-related physical assessments, and external managed services evaluation. The focus of this service is to ascertain vulnerabilities in the organization's environment. People review can include cyber security awareness level, determination of staff compliance to existing security policies and procedures, and assessment of training effectiveness. Process review can include elements such as review of policies and procedures that are in place and their effectiveness in the organization, and whether the policies and procedures align to user security and business requirements. Technology review can include reviews of cyber security technologies and their effectiveness in the organization, technology configuration and deployment, and holistic maintenance effectiveness.

Penetration testing services can include utilization of knowledge, tools, and other resources to penetrate hosts and infrastructure equipment to identify vulnerabilities to both the devices and infrastructure of the organization. The intent of this service is to focus on cyber and physical posture, as well as device vulnerability from an attack vector perspective both within and the outside of the organization. This service will tend to be much more focused on a goal, rather than an accumulated list of issues.

Remediation services can include specific focused activities of remediation, such as policy and procedure development or improvement, implementation of technical controls, application or upgrade of patches to existing systems, building technical procedures, adjusting and update plans (such as Contingency, Disaster Recovery and Incident Response), or build security baseline standards. These services focus on specific operational and technical engagement activities.

Incident Response Services can include specific small-scale forensic analysis tasks, breach containment, and large scale cybersecurity incident management.

Training services can include broad cybersecurity training, specialty OT/ICS training, specialty IoT, specialty IT training, software and hardware technical training, vulnerability assessment and penetration test training, one-on-one operational and/or technical mentoring, as well as orchestrated laboratory engagements.

Example project deliverables may include the development of documentation and reports, management of project teams, and troubleshooting of technical problems.

SCPPA may select more than one successful Respondent to support member initiatives. SCPPA may request successful Respondents to respond to requests for task proposals. The term of master service agreements awarded could be up to five years.

B. Description of Work

The successful Respondent(s) to this RFP shall also demonstrate their experience and capabilities to provide the following:

- Capability to provide program and project management services and provide daily support and facilitate coordination among the project teams in the areas of corporate IT, operational IT, and operational OT/ICS, and IoT devices and equipment, including devices that are utilized in generation, transmission, distribution, demand response, advanced metering infrastructure control systems.
- Transfer skills and knowledge relevant to the above services to employees during the contract term through training sessions and the development of design, standards, and procedural manuals.
- Knowledge and experience in the field of cyber protection for energy utilities that incorporate IT, OT/ICS, and IoT cyber defense, as well as a cyber defense envelope that encompasses both legacy and new equipment.
- Demonstrable reputation for excellence in the field of critical infrastructure cybersecurity by providing proof of experience and understanding of the utility critical infrastructure environment.

The successful Respondent(s) to this RFP shall also demonstrate their experience and capabilities to provide following categories of services they wish to engage, especially as it relates to corporate utility, generation, transmission, sub-transmission, IT and OT cybersecurity experience:

Note: Bidders are not expected to bid on all of these items but will need to clearly identify which categories they are bidding.

1. **Advisory Services:** Develop strategic cybersecurity plans, related physical security plans, cyber technology roadmaps, business cases, implementation plans, communications and customer engagement plans, workforce transition plans, testing and commissioning plans, and organizational change management plans.
2. **Cyber Program Assessments:** Ability to effectively and methodically identify cybersecurity program elements that include people, policy and process evaluation, service provider

evaluation, vulnerability management, cybersecurity resilience assessments, compliance programs, and leadership.

3. **Cyber Posture Assessments:** Ability to effectively and methodically identify cybersecurity and related physical weaknesses and potential risks. Ability to advise on best approach on how to safeguard information and systems related to IT, OT, and IoT, using holistic and effective methodology.
4. **Vulnerability Assessments:** Ability to perform overarching, as well as focused/detailed vulnerability assessments, that can include evaluations of people, processes, and technology in a utility environment. The assessment experience should include corporate infrastructure, control system infrastructure, cyber-related physical security, and external managed services evaluations as part of the assessment capability. Demonstrated experience should reflect reviewing cyber security awareness levels, determination of staff compliance to existing security policies and procedures, and assessment of training effectiveness. Experience should demonstrate a strong process review capability that included review of policies and procedures that were in place, as well as their effectiveness in the organization, and whether the policies and procedures aligned to user security and business requirements. Experience should also include a scoped technology review, which included reviews of cyber security technologies and their effectiveness in the organization, technology configuration and deployment, and holistic maintenance effectiveness. Experience should result in demonstrable ability to present resulting materials in both a consumable and auditable fashion.
5. **Penetration Testing Services:** Ability to perform a comprehensive goal-oriented penetration into the in-scope infrastructure or host environment. The experience should effectively demonstrate both the care of and understanding of the environment that is needed to identify how an attacker would enter the environment either logically and/or physically, while not causing significant disruption to the environment. Demonstrated experience working with a wide variety of equipment, physical and logical environments, as well as sensitivity to both control systems and corporate environments. Demonstrable experience in thoroughness of approach and methodology in testing practices, including both cyber and physical elements.
6. **Remediation Services:** Ability to perform specifically scoped cybersecurity technical services. Experience should demonstrate that includes focused activities of remediation, such as policy and procedure development or improvement, implementation of specific/targeted technical controls, application or upgrade of patches to existing hosts/systems/infrastructure, building detailed technical procedures, adjusting and update operational/business plans (such as Contingency, Disaster Recovery and Incident Response) to a degree that supports multiple sizes and types of systems utilized by business and operational activities in a utility, or build security baseline standards for operational IT, OT/ICS, IoT components.
7. **Incident Response Services:** Ability to provide scalable analysis and response activities related to cyber incidents. Experience should include experience in forensic analysis of individual devices (such as mobile technology, workstations, servers, network technology network components (that can include fiber, copper, radio, and microwave infrastructures), storage technologies, OT/ICS, and IoT,) through to a large-scale infrastructure. Experience should demonstrate working with varying threat intelligence sources and ability to integrate these sources into response engagement and response methods. Ability to demonstrate capabilities to analyze the potential impact across critical infrastructure, to investigate those responsible in conjunction with threat intelligence sources, law enforcement, and to coordinate the national response agencies. Ability to demonstrate clear ability to respond promptly from a regionally-local site to the requesting utility.

8. **Computer-Based Training Services:** Ability to manage, deliver and report on provided computer-based training on topics related to general cybersecurity, specific IT, OT, and/or IoT cybersecurity, cybersecurity-related programming, communications infrastructure technology, and other specific cybersecurity topics. Advanced topics may include items such as a Phishing Program (which could include statistics, sophistication levels, and potential added training), Social Engineering training (for targeted audiences such as Customer Service Representatives, Service Desk staff, and/or Security Officers, who all engage in telephonic support), and Physical Access Management (for Security Officers and other staff at facility entrances.)
9. **In-Person Training Services:** Ability to develop, manage, deliver and report on provided in-person classroom training for an assembly of trainees, up to 20 students. Experience in delivering on topics related to general cybersecurity, specific IT, OT/ICS, IoT cybersecurity, cybersecurity-related programming, communications infrastructure technology, and other specific cybersecurity topics.
10. **One-on-One Mentoring Services:** Ability to provide effective one-on-one cybersecurity-focused training services (i.e. side-by-side mentoring) for specific technical practices, such as applications development, application testing, network architecture/design, network diagnostics, operating system troubleshooting, OT/ICS testing, IoT, penetration testing, supply chain component testing, and other related cybersecurity functions. Ability to evaluate current individual training needs, develop specific training objectives and deliverables, and effectively deliver the components of the approved training plan.
11. **Laboratory Training Services:** Ability to develop, manage, deliver and report on provided laboratory-based training for an assembly of trainees in complex arenas that mimic critical infrastructures and in configurable environments where our utilities can test their own equipment. Demonstrated experience in delivering on topics related to red team/blue team/white team/purple team events. Demonstrated proof of delivery on topics, such as specific IT, OT/ICS, IoT infrastructure monitoring and defense, with focus on Programmable Logic Controllers, defense against cyber-attacks on complex, wide-spread systems, and sensitive infrastructures. Demonstrated proof of training delivery related to security operations centers analysts and technicians, information security professionals, field engineering staff, and electrical technicians.

C. Deliverables

Depending on the task, the project deliverables may include, but are not limited to:

1. Cybersecurity Program Documents: strategic cybersecurity plans, road maps, business case documents, implementation plans, communications plans, customer engagement plans, workforce transition plans, testing and commissioning plans, and organizational change management plans, and assessment reports.
2. Cyber Posture, Assessment, and Penetration Testing Documents: Assessment reports that focus on identification and assessment of any and all risks to scoped assessments, which include categories of risk, details of findings, demonstrable proof of findings, and actionable remediation recommendations.
3. Remediation and Incident Response Documents: Remediation reports that focus on scope of project, details of affected in-scope components, actions taken, and risk mitigated.
4. Computer and In-Person Training Documents: Training materials for students. Reporting documents on attendance and performance of training participants, as requested.
5. Mentoring Training Services: May include training materials for mentee. Training Plan documentation. Reporting documents on covered materials and performance of mentees, as requested.

6. Laboratory Training Services: Training laboratories/facilities, as requested. Training materials for students. Reporting documents on attendance and performance of training participants, as requested.
7. Project Management: Project Charters, Project Resource Plans, Stakeholder Communications Plans, Stakeholder Engagement Plans, and Organizational Change Management Plans, as needed, based on task.
8. Progress Reporting: Daily, weekly, monthly progress reporting on scoped assignments, as requested.
9. Invoices: Preparation and submittal of monthly, quarterly and annual invoices.

Successful bidder(s) must to adhere to North American Electric Reliability Corporation (NERC) and all other Regulatory Federal/State/Local regulations. Delivered report standards must adhere to and be presentable to an auditing organization, such a Western Energy Coordinating Council (WECC) requirements.

Please note that all activities conducted under this RFP will be performed onsite at the requesting utility, without exception.

Timeline / Schedule*

SCPPA RFP for Cybersecurity Services Selection Process	
Schedule of Requirements	**Target Date(s)**
Issue RFP	February 8, 2019
Question Cutoff Date	February 25, 2019
Responses Due	March 11, 2019
Review of Responses	March 25, 2019
Interviews (if necessary)	March 26-29, 2019
Selection of Respondent(s)	April, 2019

*Timeline/Schedule is subject to change.

IV. Proposal Submission Required Elements

1. Transmittal Letter Content:

a. A brief statement of the Respondent's understanding of the work to be done and commitment to perform the work as scheduled, including:
   i) areas of the Description of Work (Section 3, subsection B) that you are bidding;
   ii) statement of work specifications; and
   iii) reference to any proposed contractual terms and conditions required by the Respondent; and
   iv) a summary of exceptions taken to the RFP requirements; and
   v) any and all expectations from SCPPA including, but not limited to: requirements definitions, strategy refinement, and staffing requirements to support the proposed project or program implementation.

b. An officer authorized to bind must sign the proposal on behalf of the Respondent and must include the following declarations on the transmittal letter:

> "This proposal is genuine, and not sham or collusive, nor made in the interest or in behalf of any person not herein named; the Respondent has not directly or indirectly induced or solicited any other Respondent to put in a sham bid, or any other person, firm or corporation to refrain from submitting a proposal; and the Respondent has not in any manner sought by collusion to secure for themselves an advantage over any other Respondent."

2. **Respondent Information**: Provide legal name of Company or Individual, physical street address, the name(s) and title(s) of the individual(s) authorized to represent the Respondent, including telephone number(s) and email address(es).

3. **Proposal:** Proposals must include a description of the proposed project or program, how it meets (or does not meet) each of the objectives of this RFP, and a detailed description addressing all of the Areas of Interest. Respondents may also include additional services, products, tasks, task elements and/or functions that may not be part of or included in the RFP but are deemed by the Respondent to be pertinent and potentially valuable to SCPPA or its Members. SCPPA will have full discretionary authority to consider, accept and/or reject without cause such supplemental information that is not directly requested, included in or made part of the RFP.

4. **Fees:** Pricing in all Proposals should be made based on good faith estimates of the requirements defined in this RFP. Please include all necessary details of specific examples or estimates of the fees, labor rates and service charges. Describe how the fees, rates or charges will be determined. Respondents shall also be prepared to provide a breakdown of the applicable overheads and fringe benefit costs that are part of any labor rates and other direct costs associated with the services to be performed.

5. **Experience:** Respondent shall clearly identify project participants and management team, including:

   a. Describe your firm's experience as may be applicable to this RFP, your organizational structure, management qualifications, and other contract related qualifications, including number of years firm has been in business. This response should be no more than four pages per category the responder is bidding.

   b. Specify key employees and describe their qualifications, experience and duties related to this RFP, including the office location(s) where work will be performed, in addition to the physical street address referenced above.

   c. Provide a commitment statement for the retention and use of key employees as proposed, their availability to initiate and sustain the proposal, as well as planned supplemental employees if key personnel are not available to assure project delivery.

   d. State whether Respondent will use subcontractors to perform services pursuant to the contract. Should the use of subcontractors be offered, the Respondent shall provide the same assurances of competence for the subcontractor, plus the demonstrated ability to manage and supervise the subcontracted work. Subcontractors shall not be allowed to further subcontract with others for work.

The provisions of any contract resulting from this RFP shall apply to all subcontractors in the same manner as to the Respondent.

e. Respondent shall indicate any and all pending litigation that could affect the viability of Respondent's proposal, continuance of existing contracts, operation or financial stability.

6. References:

a. Describe whether the Respondent has, within the last five (5) years, rendered any service to SCPPA or to any of SCPPA's Members, either as a contractor or subcontractor, either under the current Respondent's name or any other name or organization. If so, please provide details (status as prime or subcontractor, brief description of the contract, contract start and end date, the contract administrator name, and total actual contract expenditures).

b. If the Respondent has not rendered any service within the last five (5) years to SCPPA or to any of SCPPA's Members, then please provide references over that period with the details described above including the counterparty for which services were provided.

c. Identify existing related or relevant projects or programs which Respondent developed and/or operates that would demonstrate Respondent's capabilities in this area.

d. Describe relevant program development and implementation experience, approach, and provide a list of references for similar projects completed.

V. Proposal Submission Delivery Requirements

One (1) electronic copy of your proposal must be emailed to CybersecurityServicesRFP@scppa.org or delivered on a CD or USB flash drive to the address below by no later than 4:00 pm PST on March 11, 2019:

Southern California Public Power Authority
Attention: Cybersecurity Services RFP
1160 Nicole Court
Glendora, California 91740

No contact should be made with the Board of Directors, committees or working group representatives, or SCPPA Members concerning this RFP.

Clarification questions regarding this RFP may be addressed to CybersecurityServicesRFP@scppa.org, no later than the questions cutoff deadline.

All information received by SCPPA in response to this RFP is subject to the California Public Records Act and may be subject to the California Brown Act and all submissions may be subject to review in the event of an audit.

VI. Terms and Conditions

1. SCPPA reserves the right to cancel this RFP at any time, reject any and all proposals and to waive irregularities.

2. SCPPA shall determine at its sole discretion the value of any and/or all proposals including price and non-price attributes.

3. Proposals may be sub-divided or combined with other proposals, at SCPPA's sole discretion.

4. SCPPA shall perform an initial screening evaluation to identify and eliminate any proposals that are, for example, not responsive to the RFP, do not meet the minimum requirements set forth in the RFP, are not economically competitive with other proposals, or are submitted by Respondents that lack appropriate creditworthiness, sufficient financial resources, or qualifications to provide dependable and reliable services for this RFP.

5. SCPPA reserves the right to submit follow up questions or inquiries to request clarification of information submitted and to request additional information from any one or more of the Respondents.

6. SCPPA reserves the right, without qualification and in its sole discretion, to accept or reject any or all proposals for any reason without explanation to the Respondent, or to make any award to that Respondent, who, in the opinion of SCPPA, will provide the most value to SCPPA and its Members.

7. SCPPA may decline to enter into any potential engagement agreement or contract with any Respondent, terminate negotiations with any Respondent, or to abandon the request for proposal process in its entirety.

8. SCPPA reserves the right to make an award, at its sole discretion, irrespective of price or technical ability, if SCPPA determines that to do so would result in the greatest value to SCPPA and its Members.

9. Those Respondents who submit proposals agree to do so without legal recourse against SCPPA, its Members, their directors, officers, employees and agents for rejection of their proposal(s) or for failure to execute or act on their proposal for any reason.

10. SCPPA shall not be liable to any Respondent or party in law or equity for any reason whatsoever for any acts or omissions arising out of or in connection with this RFP.

11. SCPPA shall not be liable for any costs incurred by any Respondents in preparing any information for submission in connection with this RFP process or any and all costs resulting from responding to this RFP. Any and all such costs whatsoever shall remain the sole responsibility of the Respondent.

12. SCPPA may require certain performance assurances from Respondents prior to entering into negotiations for work that may result from this RFP. Such assurances may potentially include a requirement that Respondents provide some form of performance security.

13. Prior to contract award, the successful Respondent shall supply a detailed breakdown of the applicable overheads and fringe benefit costs that are part of the labor rates and other direct costs associated with the services to be performed.

14. SCPPA Members, either collectively or individually may contact Respondents to discuss or enter into negotiations regarding a proposal. SCPPA is not responsible or liable for individual Members interactions with the Respondent which are not entirely conducted through SCPPA or at SCPPA's option or election to engage the Respondent as defined within the RFP.

15. Submission of a Proposal constitutes acknowledgement that the Respondent has read and agrees to be bound by the terms and specifications of this RFP and any addenda subsequently issued by SCPPA.

16. Information in this RFP is accurate to the best of SCPPA's and its Members' knowledge but is not guaranteed to be correct. Respondents are expected to complete all of their due diligence activities prior to entering into any final contract negotiations with SCPPA.

17. SCPPA reserves the right to reject any Proposal for any reason without cause. SCPPA reserves the right to enter into relationships with more than one Respondent, can choose not to proceed with any Respondent with respect to one or more categories of services, and can choose to suspend this RFP or to issue a new RFP that would supersede and replace this RFP.

VII. Additional Requirements for Proposal

1. **Consideration of Responses:** Submitted proposals should be prepared simply and economically, without the inclusion of unnecessary promotional materials. Proposals should be submitted on recycled paper that has a minimum of thirty percent (30%) post-consumer recycled content and duplex copied (double-sided pages) where possible.

2. **Insurance, Licensing, or other Certification:** If selected, the Respondent will be required to maintain sufficient insurance, licenses, or other required certifications for the type of work being performed. SCPPA or its Members may require specific insurance coverage to be established and maintained during the course of work and as a condition of award or continuation of contract.

3. **Non-Discrimination/Equal Employment Practices/Affirmative Action Plan:** If selected, the Respondent and each of its known subcontractors may be required to complete and file an acceptable Affirmative Action Plan. The Affirmative Action Plan may be set forth in the form required as a business practice by the Department of Water and Power of the City of Los Angeles which is SCPPA's largest Member.

4. **Living Wage Ordinance:** If selected, the Respondent may be required to comply with the applicable provisions of the City of Los Angles Living Wage Ordinance and the City of Los Angeles Service Contract Workers Retention Ordinance. The Living Wage Ordinance provisions are found in Section 10.36 of the Los Angeles City Administrative Code; and the Service Contract Workers Retention Ordinance are found in Section 10.37 of the Los Angeles Administrative Code (SCWRO/LW0).

5. **Prevailing Wage Rates:** If selected, the Respondent will be required to conform to prevailing wage rates applicable to the location(s) where any work is being performed. Workers shall be paid not less than prevailing wages pursuant to determinations of the Director of Industrial Relations as applicable in

accordance with the California Labor Code. To access the most current information on effective determination rates, Respondent shall contact:

Department of Industrial Relations
Division of Labor Statistics and Research
PO Box 420603, San Francisco, CA 94142-0603
Division Office Telephone: (415) 703-4780
Prevailing Wage Unit Telephone: (415) 703-4774
Web: http://www.dir.ca.gov/dlsr/DPreWageDetermination.htm

6. **Child Support Policy:** If selected, Respondent may be required to comply with the City of Los Angeles Ordinance No. 172401, which requires all contractors and subcontractors performing work to comply with all reporting requirements and wage earning assignments and wage earning assignments relative to court ordered child support.

7. **Supplier Diversity:** Respondents shall take reasonable steps to ensure that all available business enterprises, including Small Business Enterprises (SBEs), Disadvantaged Business Enterprises (DBEs), Women-Owned Business Enterprises (WBEs), Minority-Owned Business Enterprises (MBEs), Disabled Veteran Business Enterprises (DVBEs), and other Business Enterprises (OBEs), have an equal opportunity to compete for and participate in the work being requested by this RFP. Efforts to obtain participation of these business enterprises may reasonably be expected to produce a twenty-five percent (25%) participation goal for SBEs. For the purpose of this RFP, SCPPA's Supplier Diversity program is modeled after that of the Los Angeles Department of Water and Power. Further information concerning the Supplier Diversity Program may be obtained from the Supply Chain Services Division of the Los Angeles Department of Water and Power.

8. **SCPPA-Furnished Property:** SCPPA or a Member's utility drawings, specifications, and other media furnished for the Respondent's use shall not be furnished to others without written authorization from SCPPA or the applicable Member(s).

9. **Contractor-Furnished Property**: Upon completion of all work under any agreement developed as a result of this RFP, ownership and title to reports, documents, drawings, specifications, estimates, and any other document produced as a result of the agreement shall automatically be vested to SCPPA and no further agreement will be necessary for the transfer of ownership to SCPPA. SCPPA has the sole right to distribute, reproduce, publish, license, or grant permission to use all or a portion of the deliverable documentation, work product or presentations as it determines in its sole discretion.