Supervisory Control and Data Acquisition Systems (SCADA) Security Assessment RFP
Solicitation Number: R-21-007-FG

ADDENDUM 1
June 30, 2021

To Respondent of Record:

RESPONSES TO QUESTIONS

1. Question: **Can companies from Outside the USA apply for this? (like, from India or Canada)**

Response: *Due to the high security nature of requested services, no data can be transferred and no work can be performed outside of the US."*

2. Question: **Do we need to come over there for meetings?**

Response: *Meetings with business units can be held via video conference.*

3. Question: **Can we perform the tasks (related to RFP) outside USA? (like, from India or Canada)**

Response: *Please see Response #1.*

4. Question: **Can we submit the proposals via email?**

Response: *Yes. See section IV. Submitting a Response, B. Submission for details on submitting your submittal.*

5. Question: **Is this going to be the first assessment done on the system or has one been done previously?**

Response: *Yes, this will be the first assessment.*

6. Question: **Is there a percentage of small business participation required?**

Response: *There is a 40% aspirational (non-mandatory) goal for Small, Minority, and Woman-owned Business participation. The SMWB goal is not a set-aside and is at the discretion of the Respondent.*

7. Question: **Can you define other wireless technologies included excepting WiFi/802.11 radios in the scope of the assessment?**

Response: *Mixture of 4.9 and 11 Ghz Microwave point-to-point and point-to-multipoint.*

8. Question: **What are the approximate number/scope of HMIs, PLCs, DCS in the scope of the assessment?**

Response: *SAWS is expecting a sample size of up to 8 PLCS, 1 HMI, 1DCS. Please note these are at different physical locations.*

9. Question: **Does an asset inventory exist of all devices in the Process Control System (PCS)?**

Response: *A partial, manual, inventory exists.*

10. Question: **Are systems backups and recovery capabilities included within the scope of the assessment? They are not noted.**

Response: *Review of existing backup and restore capabilities is in scope, but not the actual systems.*

11. Question: **Is Systems Development managed internally within SAWS & what does that entail?**

Response: *The systems themselves are not developed internally but are programmed and managed internally.*

12. Question: **Does SAWS define PLC programs and HMI applications as part of the Secure Systems Development Lifecycle?**

Response: *No.*

13. Question: **Section I, Subsection F is cited as providing the minimum submission criteria but is missing. Can you please enumerate the minimum criterion?**

Response: *See Modifications to RFP for clarification.*

14. Question: **Do you have a network architecture drawing for all systems in scope?**

Response: *Yes.*

15. **Question:** **Do you have an architecture drawing for all applications in scope?**

Response: *Yes.*

16. Question: **Do veteran-owned businesses qualify for 15 points per the scoring chart in Section II paragraph D?**

Response: *No, veteran-owned businesses do not qualify for SMWB points if that is the only certification that a business has.*

17. Question: **Which standards does SAWS want/done against? CFF, NIST 800-43 Rev 5 or NIST 800-82 Rev 2?**

Response: *NIST 800-53*

18. Question: **Where does Task order specifications #23 -NIST Assessment dated 06/17/2021 play into this?**

Response: *These are unrelated.*

19. Question: **How many Internal IP's are involved?**

Response: *Approximately 900.*

20. Question: **How many segments (e.g. vLAN's) are involved and do you want segmentation testing completed?**

Response: *7 segments. SAWS would want some segmentation testing.*

21. Question: **How many External IP's are involved?**

Response: *None external to the Internet. Approx. 12 external to the enterprise network.*

22. Question: **Is the system complete air gapped from the Internet?**

Response: *Yes.*

23. Question: **Does SAWS expect the engagement to be performed on site or can the contractor engage a mix of on-shore, on-site and 1` resources?**

Response: *SAWS expects the engagement would be a mix of on-site and off-site. No offshore resources should be used.*

24. Question: **For the risk assessment - please clarify whether a manual or tool-based assessment is preferred by SAWS.**

Response: *No preference.*

25. Question: **Can SAWS provide high level org chart of the operations organization for us to estimate the number of interviews and stakeholder engagement? If not please provide list of all designations that we are expected to interview and engage?**

Response: *There are 5 separate groups with 1-2 interviews per group.*

26. Question: **"Please clarify whether PT is allowed on production environment or if it needs to be done in a staging environment? Please share the count of various network and security devices to undergo vulnerability assessments (VA) and penetration testing (PT).**

a. Count of External devices
b. Count of internal devices
c. Total number of HMI's to be tested
d. Total number of users per HMI to be tested"

Response: *Any penetration testing needs to be done in a sandbox environment or to the SCADA DMZ.*

a-d: Please refer to Questions 8, 19, 20, 21.

27. Question: **About penetration testing SAWS critical infrastructure, we assume that the penetration testing will initiate from Level 4 of Purdue Model (i.e. IT Infrastructure) and it will be till Level 3.5 of Purdue model and not on an actual network and the devices below Level 3.5 of Purdue model. Please confirm.**

Response: *Yes.*

28. Question: **Please clarify the expected frequency of penetration testing. Is it expected to be a one-time activity?**

Response: *SAWS expects a one-time pen test with targeted re-tests if needed.*

29. Question: **"Please provide more details on the Number or sites/sub-sites in scope (you have mentioned 100 Remote locations). Are all in scope or only the sites from this list is in-scope?**

Response: *Sample size consists of approximately 8 locations.*

30. Question: **Can the sites be classified based on different control environment sizing or number of assets?**

Response: *Sites can be classified as either HMI or DCS site. Please refer to question 8 for the sample size expectation.*

31. Question: **Assets per site - You have given a list of assets, are those the only assets in scope and are they from one site or location? Please clarify.**

Response: *Please refer to Question 8.*

32. Question: **Are there are any pen testing tools used currently? Can the bidder re-use them for penetration testing? If yes, can you please provide tool details.**

Response: *Bidders should use their own pen-testing tools.*

33. Question: **Are the total number of internal IP address and public facing IP address are in-scope for penetration testing?**

Response: *All IP listed in Question 21 are in scope for pen-testing.*

34. Question: **Is it possible to access SAWS environment remotely for pen testing?**

Response: *No.*

35. Question: **Is the bidder expected to do pen testing on Software applications (06 nos.) also? Please clarify.**

Response: *Yes, in the sandbox environment.*

36. Question: **Can SAWS provide a high-level architecture diagram/schematics of their SCADA system without any sensitive information?**

Response: *Diagrams will be provided after the contract award.*

37. Question: **What are BCS and HCS? Abbreviations are not available.**

Response: *BCS – Backup Control System; HCS – Primary Control System*

38. Question: **Are the firewalls mentioned in the list ICS level 3 firewalls? What is average number of firewall policies (rules) in place?**

Response: *2 Firewalls are at level, the remaining are segmenting between levels 3, 2, and 1. There is an average of 60 rules per firewall.*

39. Question: **Does SAWS use any third party or cloud services for ICS environment?**

Response: *No.*

40. Question: **Please clarify what type (Black/Gray box) of pen testing is expected?**

Response: *Whitebox.*

41. Question: **What will the expected timeline be for this assessment? Any specific timelines you would like the bidder to follow?**

Response: *Assessment should be completed by end of November 2021.*

42. Question: **Please provide clarification on the required percentage of SMWVB. Page 10 of 59 states a 40% goal while on Page 24 of 59 (Exhibit B) states 20%.**

Response: *Please see Response #6 and Modifications to RFP section.*

43. Question: **RFP page 5 – II. Selection Process A. Minimum Submission Requirements. This section indicates that section I. subsection F includes the minimum requirements that vendors must meet to be responsive. The RFP does not contain a section I. subsection F. Please clarify.**

Response: *See Modifications to RFP for clarification.*

44. Question: **RFP page 7 – B. Submission 3 Are resumes and sample reports count included in the 25 page limit?**

Response: *No. Reports and Resumes do not count against the 25-page limit.*

45. Question: **RFP page 23 – Good Faith Effort Plan for Construction SUBCONTRACTS The title of the form indicates that this form is targeted for construction contractors. Does this form apply for professional services providers, as well?**

Response: *Yes.*

46. Question: **RFP page 1 – Scope of Services Please clarify whether the comprehensive penetration test includes the internal business environment in addition to the SCADA environment. Please further clarify and provide context on how the network testing involves the**

Business Connection Sewer (BCS) and House Connection Sewer (HCS), and what is involved in the test for each.

Response: *Penetration testing should focus on SCADA DMZ. Please refer to question 37 for the acronym definition.*

47. Question: **RFP page 2 – Project Information Are the six software applications found on the SCADA network or internal business network?**

Response: *Combination of SCADA network and SCADA DMZ.*

48. Question: **Approximately how many IPs or subnets are in scope, and how many are active?**

Response: *Please refer to Question 19 and Question 21.*

49. Question: **Does SAWS prefer (or would you welcome) the project team be on-site to deliver any or all aspects of this assessment? Is remote or onsight testing preferred?**

Response: *Please refer to Question 23.*

50. Question: **Is there a preferred duration for this effort? Is there any deadline for the completion of the effort?**

Response: *Please refer to Question 41.*

51. Question: **The Risk Assessment Report should include 'The identification of existing and proposed safeguards, and an assessment of their adequacy'. To what extent should physical security be included in this assessment, if at all?**

Response: *A high-level physical security review should be included in the assessment.*

52. Question: **For the remote locations, can you provide the sample set and types (Substations, Data Centers, etc.) of sites that will be impacted by this assessment?**

Response: *Please refer to Question 8 for sample size.*

53. Question: **How often have SCADA cybersecurity assessments been conducted in the past regarding the scope in the RFP?**

Response: *These types of assessments are carried out periodically.*

54. Question: **How many IPs are in scope for External?**

Response: *Please refer to Question 21*

55. Question: **Should we keep our focus on the internal network?**

Response: *Please refer to Questions 19, 20, 21 for details.*

56. Question: **How many IPs are in scope for Internal?**

Response: *Please refer to Question 19.*

57. Question: **Can we provide a document on IPS ranges?**

Response: *Please refer to Questions 19, 20, 21 for details.*

58. Question: **Are any other field devices (backhaul, network, or otherwise) in scope for this assessment that are not detailed in the table on Page 1 of the RFP? (see below)**

Device/Service	Approximate Count	Notes
Physical Host Servers	8	Across two VCenters
BCS Side of PCS	35 VM (Server/WkSt)	3 hosts / 1 host for Vcenter
HCS Side of PCS	68 VM (Server/WkSt)	3 hosts / 1 host for Vcenter
Software Applications	6	6 separate apps Rockwell PlantPx Emerson Ovation Office SQL Remote Desktop Server Symantec AV Netbackup (Servers only)
Desktop Computers	50	Physical Workstations
Laptops	22	Physical Laptops
Wireless Radios (PtP/PtMP)	12	
Routers/Switches	22	
Firewalls	7	
Datacenters	2	
Remote Locations	100	A sample set of sites, all within the San Antonio Metro area, is sufficient for this assessment

Response: *No.*

59. Question: **What type of documentation are you asking for?**

Response: *Provide a brief description of similar sized projects that you have worked on.*

60. Question: **Would the company name and description of services suffice, or is there something else that you are looking for?**

Response: *Company name, Industry, size of company (customers served / employees), description of the scope of work, deliverables provided, and a sample report.*

61. Question: **If they are capable of completing the project in its entirety, without assistance from a sub contractor, what is the expectation regarding this goal?**

Response: *The SMWB goal is aspirational, not mandatory, and therefore Respondents are not required to use Small, Minority, and Woman-owned Business (SMWB) subcontractors on their responses. Please be aware that SMWB points will not be assessed for submissions that do not contain SMWB participation. If you have any questions related to the Good Faith Effort Plan, including inquiring about lists of local SMWB firms for outreach purposes, please reach out to Marisol V. Robles, SMWVB Program Manager, at marisol.robles@saws.org.*

MODIFICATIONS TO RFP

1. *Replace Good Faith Effort Plan (pages 23 – 26) with the attached.*

   The SMWVB goal on this project is updated to ***40%.***

2. *Insert section "F. Minimum Submission Requirements" to Section I. Project Information.*

   F. Minimum Submission Requirements

   1. Respondent must be located in the United States;
   2. Must have experience with such projects; and
   3. Must provide all information requested in the RFP, to include references, sample reports, etc.

END OF ADDENDUM 1

This Addendum is twelve (12) pages in its entirety, with one (1) attachment.

Attachments: Good Faith Effort Plan (4 pages)

Good Faith Effort Plan for Professional Services SUB-CONSULTING for:

NOTE: Effective 1/1/17, SMWB points shall only be assessed for consultants and/or sub-consultants who are local and certified by the South Central Texas Regional Certification Agency as SBEs. MBEs and WBEs must (also) have SBE certification).

NAME OF PROJECT: SCADA Security Assessment

SECTION A - PRIME CONSULTANT INFORMATION

Legal Name of Firm, including "doing business as" if applicable: _____

Address of Office to Perform Project Work: _____

City: _____ **State:** _____ **Zip Code:** _____

Telephone: _____ **Fax:** _____

Contact Person: _____

Email Address: _____ **Is your firm Certified as an SMWVB?** **Yes:** _____ **No:** _____

If "Yes", Certification Agency that granted SMWVB designation: _____

Type/s of Certification: **SBE:** _____ **MBE:** _____ **VBE:** _____ **WBE:** _____

Prime Consultant's Percentage of Participation: (Ex: 100% is the total value of the contract) _____%

1. List ALL SUB-CONSULTANTS/SUPPLIERS that will be utilized on this project/contract. (SMWB AND Non-SMWB)

	Legal Name of Sub-consultant/Supplier (including "doing business as", if applicable).	Address of Office Location to Perform Project Work or Provide Supplies:	Scope of Work/Supplies to be Performed/Provided by Firm:	Estimated Percentage of Participation on this Project:	Certification Type & Certification Agency:
1					
2					
3					
4					

5					

SECTION B. – SMWB COMMITMENTS

The SMWB goal on this project is 40%

1. The undersigned proposer has satisfied the requirements of the PROPOSAL specification in the following manner (please check the appropriate space):

_____The proposer is committed to a minimum of 40 % SMWB utilization on this contract.

The proposer, (if unable to meet the SMWVB goal of 40%), is committed to a minimum of % SMWB utilization on this contract.
_____(If contractor is unable to meet the goal, please fill out Section C and submit documentation demonstrating good faith efforts).

2. Name and phone number of person appointed to coordinate and administer the SMWB requirements on this project.

Name: _____
Title: _____
Phone Number: _____
Email Address: _____

IF THE SMWB GOAL WAS MET, PROCEED TO AFFIRMATION AND SIGN THE GFEP. IF GOAL WAS NOT MET, PROCEED TO SECTION C.

SECTION C – GOOD FAITH EFFORTS (Fill out only if the SMWB goal was not achieved).

1. On a separate sheet of paper, list and attach to this Good Faith Effort Plan written, posted, or published notification to all firms you contacted with sub-consulting/supply opportunities for this project that will not be utilized for the contract by choice of the proposer, sub-consultant, or supplier. Notices to firms contacted by the proposer for specific scopes of work identified for sub-consulting/supply opportunities must be provided to sub-consultant/supplier ***not less than five (5) business days prior to proposal due date***. This information is required for all firms that were contacted of sub-consulting/supply opportunities.

Copies of said notices must be provided to the SMWB Program Manager at the time the response is due. Such notices shall include information on the plans, specifications, and scope of work.

2. Did you attend the pre-submittal conference scheduled for this project? _____Yes _____No

3. List all SMWB listings or directories, contractor associations, and/or any other associations utilized to solicit SMWB sub-consultants/suppliers:

_____

4. Discuss efforts made to identify elements of the work to be performed by SMWBs in order to increase the likelihood of achieving the goal:

_____

_____

5. Indicate advertisement mediums used for soliciting SMWBs. (Please attach a copy of the advertisement(s):

_____

_____

AFFIRMATION

I hereby affirm that the above information is true and complete to the best of my knowledge. I further understand and agree that, this document shall be attached thereto and become a binding part of the contract.

Name and Title of Authorized Official:

Name: _____

Title: _____

Signature: _____

Date: _____

NOTE:

This Good Faith Effort Plan is reviewed by SAWS Contracting Department. For questions and/or clarifications, please contact Marisol V. Robles, SMWVB Program Manager, at 210-233-3420 or marisol.robles@saws.org.

DEFINITIONS

Note: To be eligible for participation in the SAWS Small, Minority, Woman, and Veteran-owned Business Program, a firm must have an established place of business in the San Antonio Metropolitan Statistical Area, and must be certified as a Small Business Enterprise (SBE). This includes firms certified as Minority and/or Woman-owned Business Enterprises (MBEs and WBEs). SAWS tracks Veteran-owned Business Enterprises (VBEs) for statistical purposes, but does not award points for VBE participation.

African American Business Enterprise (AABE): A business structure that is Certified by the Texas Historically Underutilized Business (HUB) Program or the South Central Texas Regional Certification Agency as being 51% owned, operated and controlled by African American minority group member(s) who are legally residing in or are citizens of the United States.

Local: A business located in the San Antonio Metropolitan Statistical Area (SAMSA) , which includes the counties of Atascosa, Bandera, Bexar, Comal, Frio, Guadalupe, Kendall, Kerr, McMullen, Medina, Uvalde and Wilson. A business's presence in the SAMSA that consists solely of a P.O. box, a mail drop, or a telephone message center does not count as being local.

Prime Consultant/Contractor: Any person, firm partnership, corporation, association or joint venture which has been awarded a San Antonio Water System contract.

Sub-consultants/contractor: Any named person, firm partnership, corporation, association or joint venture identified as providing work, labor, services, supplies, equipment, materials or any combination of the foregoing under contract with a prime consultant/contractor on a San Antonio Water System contract.

Small, Minority, and Woman-owned Business (SMWB): All business structures Certified by the Texas Historically Underutilized Business (HUB) Program or the South Central Texas Regional Certification Agency that are 51% owned, operated, and controlled by a Small Business Enterprise, a Minority Business Enterprise, or a Woman-owned Business Enterprise.

Small Business Enterprise (SBE): A business structure that is Certified by the South Central Texas Regional Certification Agency as being 51% owned, operated and controlled by someone who is legally residing in or a citizen of the United States, and the business structure meets the U.S. Small Business Administration's (SBA) size standard for a small business within the appropriate industry category, as determined by the South Central Texas Regional Certification Agency.

Minority Business Enterprise (MBE): A business structure that is Certified by the Texas Historically Underutilized Business (HUB) Program or the South Central Texas Regional Certification Agency as being 51% owned, operated, and controlled by an ethnic minority group member(s) who is legally residing in or a citizen of the United States. For purposes of the SMWB program, the following are recognized as minority groups:

a. **African American** – Persons having origins in any of the black racial groups of Africa.

b. **Hispanic American** – Persons of Mexican, Puerto Rican, Cuban, Spanish or Central or South American origin.

c. **Asian-Pacific American** – Persons having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent or the Pacific Islands.

d. **Asian-Indian American** – Persons whose origins are from India, Pakistan, Bangladesh or Sri Lanka.

e. **American Indian/Native American** – Persons having no less than 1/16 percentage origin in any of the American Indian Tribes, as recognized by the U.S. Department of the Interior's Bureau of Indian Affairs and as demonstrated by possession of personal tribal role documents.

San Antonio Metropolitan Statistical Area (SAMSA). Also known as the Relevant Marketplace, the geographic market area from which the prior Disparity Study analyzed contract utilization and availability data for disparity (currently including the counties of Atascosa, Bandera, Bexar, Comal, Frio, Guadalupe, Kendall, Kerr, McMullen, Medina, Uvalde and Wilson).

Woman-owned Business Enterprise (WBE): A business structure that is Certified by the Texas Historically Underutilized Business (HUB) Program or the South Central Texas Regional Certification Agency as being 51% owned, operated and controlled by a woman or women who are legally residing in or citizens of the United States.

Veteran-Owned Business Enterprise (VBE): A business structure that is certified by the South Central Texas Regional Certification Agency, and is at least 51% owned, operated and controlled by an individual who served in the United States Armed Forces, and who was discharged or released under conditions other than dishonorable. Please note: This certification type should not be confused with the Service Disabled Veteran designation available through the Small Business Administration.

Web Submittal of Sub-consultant/Supplier Payment Reports:
The Consultant will be required to electronically report the actual payments to all sub-consultants and suppliers utilizing the Subcontractor Payment and Utilization Reporting (S.P.U.R.) System, beginning with the first SAWS payment for services under the contract, and with every payment thereafter (for the duration of the contract). Electronic submittal of monthly subcontractor payment information will be accessed through a link on SAWS' "Business Center" web page. This information will be utilized for subcontractor participation tracking purposes. Any unjustified failure to comply with the committed SMWB levels may be considered breach of contract.

The Contractor and all subcontractors will be provided a unique log-in credential and password to access the SAWS subcontractor payment reporting system. The link may also be accessed through the following internet address: https://saws.smwbe.com/