San Antonio Water System

OVERARCHING SECURITY CONSULTING SERVICES
SAWS Solicitation No. R-18-001-JAM

ADDENDUM NO. 1
February 28, 2018

To Respondent of Record:

This addendum, applicable to project referenced above, is an amendment to the RFP and as such will be a part of and included in the Contract Documents. Acknowledge receipt of this addendum by entering the Addendum number and issue date on the space provided in submitted copies of the Respondent Questionnaire.

RESPONSES TO SUBMITTED QUESTIONS

1. QUESTION: This RFP does not have a dollar value stated anywhere. Does that mean that the San Antonio Water System (SAWS) and the selected contractor will negotiate a budget for the scope of work? The hourly rates requested in Exhibit D should not incorporate other direct costs correct? Those will be addressed separately during contract negotiation?

   ANSWER: ***SAWS will create a work order contract to use as needed. Other direct costs would be addressed separately per work order.***

2. QUESTION: Is this a continuation of the previously released solicitation or is this a new one?

   ANSWER: ***This is a new solicitation, not a continuation of a previous project or other current solicitations.***

3. QUESTION: In addition, could we get information about the following solicitation: Information Technology Consulting and Technical Support Services Task Order Contracts?

   ANSWER: ***Please refer to the solicitation website for that project at the following web address: http://www.saws.org/business_center/contractsol/Drill.cfm?id=2121&View=Yes***

4. QUESTION: One of the requirements is for the vendor to be a Certified Incident Handler (CIH). Can a Respondent submit a proposal as a "sole" vendor without this requirement?

   ANSWER: ***All firms are encouraged to submit regardless if the Respondent has a certified incident handler on staff. SAWS may consider vendors without the incident certifications.***

5. QUESTION: Can you please prioritize the list of IT security projects from the most important to the least important?

   ANSWER: ***Road mapping the SAWS NIST compliance would be our priority on this contract.***

6. QUESTION: Which do you hope to have completed within the 1st year of the contract period?

   ANSWER: ***Because this contract will be utilized on an as needed-basis, there are no defined expectations of what may or may not be done in the first year. This contract could have all areas used or just a few, depending on SAWS' needs.***

7. QUESTION: Would SAWS be willing to extend the due date for the RFP response beyond March 8th?

   ANSWER: ***Yes. Please refer to the Clarifications section in this Addendum.***

8. QUESTION: Can you please list how many applications you would like security tested and how many of each type of app you have, based off the matrix below?

Application Includes one or more of	Static	Basic	Portal	Advanced	Custom
Static Content	✓	✓	✓	✓	✓
Dynamic pages	✓	✓	✓	✓	✓
Database backend	✓	✓	✓	✓	✓
Login/accounts		✓	✓	✓	✓
Search function		✓	✓	✓	✓
HTML forms		✓	✓	✓	✓
File upload/download			✓	✓	✓
Forums			✓	✓	✓
Credit card payments				✓	✓
Shopping cart				✓	✓
Content Management (CMS)				✓	✓
AJAX					✓
JSON					✓
Flash					✓
Silverlight					✓
COTS (SP, SAP, Lotus, etc.)					✓

ANSWER: ***These would be on an as needed basis. SAWS does not have anything in the queue at this time. Total external applications currently is between five to ten (5-10).***

9. QUESTION: How many wireless Access Points do you have?
ANSWER: ***SAWS has approximately two hundred access points (~200); however, not all wireless would be tested each year.***

10. QUESTION: How many campuses would you like to test?
ANSWER: ***SAWS is requesting to test three to five (3-5) campuses per year once testing is available.***

11. QUESTION: How many active, external IP addresses do you have for external network penetration test?
ANSWER: ***SAWS has approximately fifty (50) external IP addresses that may require external network penetration tests.***

12. QUESTION: How many internal IP addresses do you have for internal network penetration test?
ANSWER: ***SAWS has approximately one thousand (1000) in datacenter and three thousand (3000) endpoints.***

13. QUESTION: How many policies would you like reviewed?
ANSWER: ***Currently SAWS has ten (10) policies/standards available for review.***

14. QUESTION: How many policies do you want drafted?
ANSWER: ***SAWS is currently developing five to ten (5-10) new policies/standards.***

15. QUESTION: How many staff does SAWS have today dedicated today on IT or Security?
ANSWER: ***SAWS currently employs two (2) security engineers.***

16. QUESTION: Is SAWS currently implementing any solutions that are not yet live that will need to be part of the assessment?

ANSWER: ***Not at this time.***

17. QUESTION: Under Section VII. Other Requirements, Section B. Disclosure of Interested Parties (Form 1295), it states that this form will need to be provided before entering into a contract with SAWS. Does SAWS want this form included as part of the formal response?

ANSWER: ***This form will be requested from the awarded Respondent prior to contract award. It does not need to be included as part of this formal response.***

18. QUESTION: Exhibit C, Conflict of Interest Questionnaire, Question 3 states, "Name of local government officer about whom the information is being disclosed." What/whose name should be entered here?

ANSWER: ***Should a business relationship exist between your firm and a local government entity, this question requires the name of the officer of said entity with which the relationship exists. If no business relationship exists between your firm and a local government entity, then no name is required in this section.***

19. QUESTION: SAWS states that there should only be one (1) file with all required response information submitted; however, Exhibit D Compensation Proposal, states "To Be Submitted Separately from RFP Response." Does SAWS want this included in the 1 complete PDF file, or submitted as a separate PDF file for a total of two (2) files submitted?

ANSWER: ***Please submit Exhibit D as a separate file attachment but within the same email submittal with the total response. Two (2) separate files are requested.***

20. QUESTION: Will organizations who intend to sell hardware to SAWS be precluded from providing a response to this RFP which includes consulting on that related equipment?

ANSWER: ***A Respondent intending to sell hardware will not be excluded from submitting a proposal to this project.***

21. QUESTION: In regards to estimated number of NIST System Specific controls to test, is Authorization to Operate (ATO) part of this?

ANSWER: ***SAWS has not gotten to the actual implementation of NIST controls at this time. This is currently being processed for control and auditing. SAWS will not be doing ATO.***

22. QUESTION: Is SAWS handling data from or accessing federal information systems? Can contractual or other specific legal requirements be provided?

ANSWER: ***SAWS is not handling or accessing federal systems.***

23. QUESTION: Are annual controls testing a factor? If so, how?

ANSWER: ***SAWS is not currently ready for any control testing. Currently, SAWS is identifying NIST controls to apply to systems.***

24. QUESTION: Has a self-assessment been performed?

ANSWER: ***Yes, a self-assessment has been performed.***

25. QUESTION: How many System Security Plans are involved?

ANSWER: ***Two (2) plans are involved.***

26. QUESTION: Is SAWS expected to comply with the guidance in NIST 800-125A?

ANSWER: ***No. Currently NIST compliance is voluntary.***

27. QUESTION: What is the estimated percentage of systems virtualized versus not in terms of NIST compliance?

ANSWER: ***Approximately 98-99% are virtualized but SAWS has not looked at any of these as NIST compliant at this time.***

28. QUESTION: What languages are the custom codes in?

ANSWER: ***The languages are:* .net, sql, python, UI/UX front end – bootstrap, jqueryt, html 5, and react.**

29. QUESTION: What frequency does SAWS expect for Vulnerability Assessments in IT during the contract term?

ANSWER: ***SAWS expects the penetration test annually.***

30. QUESTION: In Industrial?

ANSWER: ***SAWS expects this test bi-annually.***

31. QUESTION: Has SAWS considered the use of cyber incident insurance for incident response? Would you like more details on that option?

ANSWER: ***Yes, that information would go to the SAWS Risk Management division.***

32. QUESTION: If the awarded Respondent makes recommendations as the result of an assessment, will the Respondent be excluded from providing those products/services?

ANSWER: ***No, the Respondent would not be excluded from providing those products/services.***

33. QUESTION: Will the customer purchase the Data Loss Prevention (DLP) solution or is the product part of the expected service delivery?

ANSWER: ***The customer, SAWS, will purchase the DLP solution.***

34. QUESTION: Will SAWS consider extending the submission due date for this RFP?

ANSWER: ***Yes. Please refer to the Clarifications section in this Addendum.***

35. QUESTION: Would SAWS be open to the idea of leveraging a mix of US and offshore resources?

ANSWER: ***SAWS prefers not to use offshore resources.***

36. QUESTION: What is the scope of email server scan, archived emails on the server, or emails sent and received by users on a daily basis?

ANSWER: ***The scope of work is an audit on archived and sent emails.***

37. QUESTION: Does SAWS have existing tools for DLP scans and OCR scans? If it does, how are the tools currently used? Does SAWS have sufficient DLP hardware components in place to perform the requested scans? If the existing DLP tool doesn't have the functionality to perform OCR scans, is SAWS planning to upgrade the tool, purchase another tool, or integrate the existing tool with OCR technologies?

ANSWER: ***SAWS has had a DLP at rest and in motion but we do not have the capability to identify sensitive information moving via email at this time. OCR is a requirement in the RFP.***

38. QUESTION: Is SAWS looking to perform one time scan of all structured and unstructured data sources?

ANSWER: ***SAWS' preference is to perform an annual or bi-annual scan.***

39. QUESTION: Are databases included in the 700 internal servers mentioned?

ANSWER: ***Yes, the databases are included.***

40. QUESTION: Is the IT Disaster Recovery/Continuity Planning scope limited to recovering IT functionality, across people, process and technology? For instance, on page 5 of the RFP, SAWS requests “Develop a cost effective recovery solution for the top 5 most likely scenarios.” and “Create a master plan for implementing business continuity planning”. Is the scope limited to recovering the IT functionality provided to the business? To helping make the requisite IT technologies, IT people and IT processes available at the appropriate times in the recovery cycle? Such as providing for rapid recovery of critical databases, email and telephone system failover, data center recovery. Or will the master plan referred to in this section also need to provide for non-IT, business recovery? Such as business unit leadership succession plans, alternate work locations for office staff, etc.

ANSWER: ***In the context for this RFP Disaster Recovery (DR) is for IT only; no non-IT business development will be performed or requested on this contract.***

41. QUESTION: The page 5 “IT Disaster Recovery / Continuity Planning: Solution Design” details seem to indicate a desire for the development of recovery plans, more than a strategy. It appears SAWS would like plans written that detail how to establish command and control, maintain communications, assemble teams, on the day of disaster. Is that accurate?

ANSWER: ***Yes, that is accurate.***

42. QUESTION: For purposes of Business Impact Analysis, how many functional business units, roughly, will need to be engaged?

ANSWER: ***For purposes of Business Impact Analysis, approximately six to seven (6-7) business units will be involved.***

43. QUESTION: In terms of rough orders of magnitude, how many systems and applications are in scope for cataloging?

ANSWER: ***SAWS has approximately one thousand (~1000) servers and approximately three thousand (~3000) endpoints; and for ICS the total is unknown currently at this time. For applications there are five to ten (5-10).***

44. QUESTION: What is the expected level of detail of the system and application cataloging? For instance, does discovery on a SCADA system stop at the supervisory systems, or drive down to individual PLU’s?

ANSWER: ***The desired details include system name, applications on the system, location, ip. SAW’s goal is eventually get down to PLC on SCADA/ICS, but currently stop at supervisory systems.***

45. QUESTION: Although it doesn’t appear to be in scope, does the system and application cataloging include the development of a service catalog?

ANSWER: ***Service catalog is not in the scope of this contract.***

46. QUESTION: Does the request to “Create a master plan for implementing business continuity planning”, entail creating a multi-year roadmap for a program to use in developing SAWS’ recovery capability. Will this include or exclude some level of cost analysis?

ANSWER: ***SAWS prefers a roadmap. A rough cost analysis is desired.***

47. QUESTION: How many groups are involved in the maintenance of the systems and applications?

ANSWER: ***There are three to four (3-4) groups depending on the systems and applications.***

48. QUESTION: What is the rough structure (mainframe, 3-tier, ERP, cloud, etc) and composition of the critical servers and systems hosting the applications?

ANSWER: ***The most critical servers are 3-tier at this time. These servers are mainly windows with three to five percent (3-5%) Linux.***

49. QUESTION: Roughly, how large is the overall IT environment, in terms of IT people and data centers / data center square footage?

ANSWER: ***SAWS' Information Systems (IS) Department is about one hundred (100) people, with two (2) datacenters, and square footage is approximately two thousand (~2000 sqft.).***

50. QUESTION: Roughly, how large is the overall business environment, in terms of people and locations?

ANSWER: ***SAWS has are approximately one thousand six hundred fifty (1650) employees and approximately eighty (80) locations, with fifteen to twenty (15-20) locations permanently manned.***

51. QUESTION: How many internal and external applications will be in scope for vulnerability assessments / penetration testing?

ANSWER: ***External applications is five to ten (5-10). Internal applications are not be included.***

52. QUESTION: Apart from the assets listed in the Scope of Services for DLP, how many additional internal / external IPs will be in scope for vulnerability assessments / penetration testing?

ANSWER: ***Approximately fifty (50) external IP addresses. Approximately one thousand (1000) in datacenter and three thousand (3000) endpoints.***

53. QUESTION: Which in-scope IP-addresses are third party owned? Do you have authorization to test those third party owned IP addresses?

ANSWER: ***No IP-addresses are third party owned.***

54. QUESTION: Does vulnerability assessment / penetration testing only include the IT assets or does it also include OT / SCADA systems?

ANSWER: ***This only includes IT assets.***

55. QUESTION: In addition to including a copy of our current Certificate of Liability Insurance in the proposal, are we to also abide by the instructions on page 23, Exhibit A, Item 2 j. 1 and 2 and send a copy by email to saws@ebix.com and the original to SAWS Contract Administration office?

ANSWER: ***A copy of current insurance coverage should be included in the proposal. The requirement in the instructions on Exhibit A will be required of the awarded Respondent once notified with the intent to award the contract.***

55. QUESTION: Are we to include Exhibit A in our response or just the Certification of Insurance?

ANSWER: ***Certification of insurance is required for the submitted response. Exhibit A is presented for reference of the insurance requirements for the awarded contract.***

55. QUESTION: Is Exhibit "F" – Sample Contract (along with its associated Exhibits) for review purposes only?

ANSWER: ***The Sample Contract is included for review purposes only.***

CLARIFICATIONS

1. The bid submission time will be moved to a later date. On Page 4, Section I. C. Estimated Timeline, remove the proposal due date line and replace with the following:

   March 15, 2018 by 2:00 p.m... Proposals Due

   The remainder of this section will remain unchanged.

END ADDENDUM 1

This Addendum, is seven (7) pages in its entirety. There are no attachments.