San Antonio Water System

REQUEST FOR PROPOSALS
MANAGED CYBER SECURITY SERVICES

BID NO: 19-19023

Addendum No. 1
April 3, 2019

This Addendum changes the RFP due date and provides part one of two of the responses to questions regarding the referenced RFP. A second addendum will be posted with part two of two of the responses to questions.

RFP Due Date

The proposal due date of April 10, 2019 is changed to ***April 17, 2019*** no later than 3:00 PM Central Time.

Questions and Answers

1. **Question:** Can a logical network diagram be shared?

   Response: *Not relevant to engagement.*

2. **Question:** What currently existing security technologies are present that would be monitored or managed? i.e. EDR, AV, IPS, SIEM, etc.

   Response: *AV, EDR, IPS, Firewall(s), Web Proxy, Email Metadata, Vulnerability Scans Reports, and any future data sources. All of these would centrally be monitored through the security information and event management (SIEM).*

3. **Question:** Please innumerate all perimeter firewalls and include:
   a. Make:
   b. Maximum throughput:
   c. Configuration: (HA/standalone/etc.)
   d. Are the firewalls next-generation, meaning, do they have IDS/IPS enabled?

   Response: *Firewalls will not be managed. SIEM shall analyze Internet traffic.*

4. **Question:** How many servers?
   a. How many of each: Windows/Linux/Mac/etc.

   Response: *There are approximately 450 servers. However, servers will not be managed. SIEM receives events from servers.*

5. **Question:** How many laptop/desktops?

   Response: *We have approximately 2,600 clients. However, the clients will not be managed.*

6. **Question:** How many employees?

   Response: *Approximately 1,800.*

7. **Question:** Would SAWS like the provider to both manage & monitor your firewalls?

   Response: *No. Only manage the SIEM.*

8. **Question:** Is SAWS interested in having the service provider also provide IDS/IPS as a fully managed service?

   Response: *No. Only assist with correlation of IDS/IPS alerts and with other events reported to SIEM.*

9. **Question:** Based on the checklist for Exhibit "A", it appears they want a copy of our certificate, but the RFP says NOT to send one until the contract is awarded. Please tell us exactly what is required.

   Response: *Per Section IV. Submitting a Response, C. Response Format, #9 Exhibit A, the respondent shall submit a copy of a certificate of insurance giving evidence of the various lines of the respondent's commercial insurance coverage currently in force; and a letter on the respondent's company stationary stating their commitment to provide the various lines of insurance coverage required if awarded a contract under this RFP.*

   Exhibit A provides the detailed information on coverages and amounts that shall be required upon award of a contract.

10. **Question:** The doc is locked. Can I get an editable version for our template response?

    Response: *Per this request an unlocked PDF version of the bid has been posted to the SAWS website. https://www.saws.org/business_center/ProcBids/Drill.cfm?id=3456&View=Yes*

11. **Question:** Is it SAWS' intention to continue using the existing SIEM solution (Splunk) or are you open to moving to a different tool?

    Response: *We are not open to moving to a different tool at this time.*

12. **Question:** What version of Splunk is currently in place? When does the current license for Splunk expire?

    Response: *We have Splunk 7.1.0. The licensing is perpetual. Maintenance is due on a yearly basis.*

13. **Question:** Is Splunk currently hosted on-prem or in the cloud? If on-prem, is the existing SIEM located only at the primary data center, or is there a backup/failover SIEM at the secondary data center?

    Response: *It is hosted on-premise. We do have high-availability for receiving logs, but there are some components that are not redundant. We are open to improve the current architecture.*

14. **Question:** What are the current number of Events Per Second (EPS) (messages / logs per second) for the Splunk platform?

    Response: *There are 11,000 EPS.*

15. **Question:** What is the total size of logs (in Gb/day) for the Splunk platform?

    Response: *40 Gb.*

16. **Question:** Can you provide details on the devices currently feeding into the SIEM? (e.g. # Windows Servers/Desktops, # of networking devices, # of databases, # of field devices, # and type of cloud sources, etc.)

    Response: *SIEM is not fully deployed, however, the majority of the data sources are ready. Please review the previous answers for device numbers.*

17. **Question:** Provide details and the number of use cases currently configured and triggering events.

    Response: *We are currently receiving alerts for locked accounts, malware, untrusted software, new vulnerabilities, expiring certificates, intrusion detection system (IDS), and email threats that were allowed.*

18. **Question:** What is the number of alerts/events investigated in the preceding year?

    Response: *7,300 alerts.*

19. **Question:** What is the number of incidents investigating in the preceding year?

    Response: *1,460 incidents.*

20. **Question:** What is the estimated number of SIEM to be configured and tuned in SAWS?

    Response: *One.*

21. **Question:** What are the specification of vendor SOC?

    Response:
    - *It is not required to be housed in a Sensitive Compartmentalized Information Facility, but have proper assurances in place for keeping customer information protected.*
    - *Be able to deliver on availability requirements for Service Level Agreement.*
    - *Be able to deliver services by being experienced with deployment/maintenance of Splunk Enterprise Security, having adequate staffing, and staff that is knowledgeable of current threats.*

22. **Question:** Please clarify if the SIEM logs are from SAWS IT Infrastructure, SAWS OT Infrastructure (e.g., Ovation DCS), or both.

    Response: *Currently it is only SAWS IT Infrastructure, but we are adding Intrusion Detection for the SAWS OT Infrastructure.*

23. **Question:** Please clarify the number of separate facilities/sites to be monitored

    Response: *There is one SIEM instance being used to monitor devices scattered among several facilities, but one logical network.*

24. **Question:** Can we please request an extension of time to respond?

    Response: *Yes, the due date has been extended. Please see date change above.*

End of Questions and Answers

ACKNOWLEDGEMENT BY RESPONDENT

Each Respondent shall acknowledge receipt of this Addendum No. 1 by noting such and signing below.

This undersigned acknowledges receipt of this Addendum No. 1 and the bid proposal submitted herewith is in accordance with the information and stipulations set forth.

______________________________ __________________________________

Date Signature of Respondent

End of Addendum