REQUEST FOR PROPOSALS

PURCHASE OF NETWORK ANOMALY DETECTION SOLUTION
BID NO: 17-17089

ADDENDUM I

BIDS DUE: September 22, 2017 @ 3:00 PM Central Time

To report suspected ethics violations impacting the San Antonio Water System, please call 1-800-687-1918.

***** This **Addendum I** is issued to make the following changes.

Article I. Project Information, section C. Scope of Services, item 1. e., "Information regarding Vendor's ability to meet SAWS, local, state, and federal regulatory requirements including applicable licenses", removed in its entirety.

***** Addendum I is issued to provide the questions asked and the responses to those questions.

1. **Question:** SAWS provides the number users in their enterprise. How many Active Directory accounts does SAWS want to monitor with this solution?

   Answer: Between 2200-2500

2. **Question:** Could SAWS define their needs around "unsupervised machine learning"? What capabilities does SAWS expect to gain from "unsupervised machine learning"?

   Answer: The system must be able to learn without me defining what is an anomaly. I shouldn't have to monitor the output to determine if it's bad or not and feed it back into the system

3. **Question:** What is the retention policy of the data sources? How long do you need to be able to search historically? Is it the same for all data sources?

   Answer: 30 days of data would be ideal but it depends on the hardware and costing.

4. **Question:** Are there specific data sources that are required to create the network baseline?

   Answer: Not specifically, we will provide all network flow data and the system should be able to baseline from that.

5. **Question:** What are the other important data sources besides Span/Tap & NetFlow?

   Answer: Could include syslog, manual file upload, etc.

6. **Question:** How many NetFlow devices will be sending NetFlow data? What version(s) of NetFlow do they support? How many Span/Tap ports are you expecting to provide? How much data are you expecting to ingest from these devices?

   Answer: Avg data is 2GHz/s with spikes around 6G. Current plan is minimum of 2 span ports.

7. **Question:** As threat intel ages out do you expect to have a framework that automatically manages that data or do you expect to manage that manually?

   Answer: Automatic

8. **Question:** Can you elaborate on the capabilities that the existing solution is providing?

   Answer: Currently we use ironport to inspect ssl traffic. Idea is this would either take feed from ironport or at a minimum not interfere.

9. **Question:** How many individuals are in the "prioritized group" and what level of access will be required for this group?

   Answer: That was part of the template. If this is how many will manage we are looking at a minimum of 3 and we would need full access to the system. If this is talking data then it needs to be able to monitor all the data we have as addressed above in question7.

10. **Question:** Does SAWS have any data sources that are currently ingested by Splunk that would also be ingested as a part of this solution? How much data is ingested and from what sources?

    Answer: Yes. Yes. Rest of the question is answered in 7 above. The intent here is for this to potentially push in to splunk as well. Would tune the input based on our splunk license.

11. **Question:** Where may Vendors acquire Exhibit G? Is SaaS in-scope for this procurement? Will SAWS consider a Cloud solution?

    Answer: We are not considering a SaaS solution at this time.

All other terms and conditions of the original bid remain unchanged.