REQUEST FOR PROPOSALS
MANAGED CYBER SECURITY SERVICES

BID NO: 19-19023

Addendum No. 2
April 5, 2019

This Addendum provides part two of two of the responses to questions regarding the referenced RFP.

Questions and Answers

1. **Question:** Currently, what security software is installed in the environment? How is it being utilized?

   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).*

2. **Question:** How is the current security infrastructure being utilized?

   Response: *SAWS uses defense in depth leveraging different technologies at different layers.*

3. **Question:** Can you provide us with a current network map? If not, can you provide us with detailed description of the IT infrastructure components? (e.g. servers, Scada systems etc..)

   Response: *Network map not relevant to engagement. More detail about network infrastructure can be found in other answers.*

4. **Question:** What are your critical business assets, functional groups / areas?

   Response: *This information is not relevant at this phase.*

5. **Question:** Where is your critical infrastructure located (city data center, colo-datacenter)? What about non critical assets?

   Response: *Our critical IT infrastructure is located in multiple data centers that will feed the SIEM. Non critical assets exist throughout San Antonio, but they are out of scope.*

6. **Question:** What SIEM and log aggregation and storage solution do you currently employ?

   Response: *Splunk Enterprise Security and Storage Area Network (SAN) storage.*

7. **Question:** Are there any compliance or legal obligations / regulations such as PCI and CCPA that are tied to these services?

   Response: *No, however we do have PCI and HIPAA requirements.*

8. **Question:** Is there a formal incident response plan? If so can you briefly describe or share it with us?

   Response: *Yes, however it cannot be shared at this stage.*

9. **Question:** Have there been any previous cyber security related incidents or breaches? If so, what occurred, how was it handled and who was overall in charge of the incident?

   Response: *There have been cyber security related incidents, however none that have resulted in a data breach. It was handled according to our Incident Response Plan and our Incident Response Manager was in charge.*

10. **Question:** How many computer users do you have?

    Response: *Approximately 1,800.*

11. **Question:** How many physical and virtual servers do you have?

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

12. **Question:** How many internet connections do you have and what is the bandwidth?

    Response: *We have redundant Internet connections.*

13. **Question:** Do you use Office365 or G-Suite?

    Response: *No.*

14. **Question:** How many Security Analyst do you have on staff?

    Response: *At least three.*

15. **Question:** What is your required SLA for MTTI (Mean Time To Identify)?

    Response: *Negotiable, but within industry standards.*

16. **Question:** What is the size of the Splunk license in gb's and how many gb's are being saved daily?

    Response: *Splunk is licensed for 50 Gb and we average 40 Gb currently.*

17. **Question:** Does this include the full scope of log sources and devices? If not please estimate the percentage of increase anticipated?

    Response: *No, we are going to be adding additional data sources and filtering some events that don't provide value.*

18. **Question:** How many indexers and search heads are deployed today?

    Response: *Two indexers and two search heads.*

19. **Question:** Are search heads deployed for different user groups?

    Response: *One instance is reserved for cyber security.*

20. **Question:** How many use cases / searches are implemented today?

    Response: *The shared search head is used for Network Troubleshooting and Analysis and Application Performance Monitoring.*

21. **Question:** How many notables are being generated today? How many of them are critical or high notables?

    Response: *Average of 1,460 per year. Critical or high average 73 per year.*

22. **Question:** What add on applications are deployed with Splunk today (e.g. Splunk UEBA, Security Essentials…)?

    Response: *Security Essentials and other applications from multiple vendors.*

23. **Question:** Does SAWS leverage Splunk for incident tracking or a third party case management system (e.g. Service Now)?

    Response: *At this time we are using Cherwell for incident tracking.*

24. **Question:** If SAWS leverages a third party case management system what solution is being used?

    Response: *We don't have a case management system at this point.*

25. **Question:** Is there an incumbent providing these services, or is this a new effort?

    Response: *This is a new effort.*

26. **Question:** Is there any cyber tooling (SIEM, firewall, sensors, etc.) in place already, and if yes, what and what vendor?

    Response: *Yes, however, vendors are not relevant to the engagement. We have 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).*

27. **Question:** Is there an existing SIEM? What SIEM is it?

    Response: *Yes, Splunk Enterprise Security*.

28. **Question:** How much data is consumed daily within the SIEM (if one exists)? Or, how much is estimated if one does not exist today?

    Response: *An average of 40 Gb.*

29. **Question:** If no SIEM, is the MSSP expected to provide SIEM technology as part of its service?

    Response: *The managed security service provider (MSSP) is expected to manage the existing SIEM.*

30. **Question:** Is the MSSP expected to perform remediation, or just provide remediation steps to IT team of SAWS?

    Response: *The MSSP is not expected to perform remediation.*

31. **Question:** What are the # of endpoints across entire SAWS environment?

    Response: *2,600 clients.*

32. **Question:** What are the # of workstations used within the SAWS environment?

    Response: *2,600 clients.*

33. **Question:** Are any workstations BYOD? If yes, will MSSP be responsible for monitoring those devices as well?

    Response: *Bring your own device (BYOD) are on a separate network and are out of scope at this point.*

34. **Question:** What are the # of employees affiliated with the SAWS?

    Response: *1,800.*

35. **Question:** Which type of monitoring would SAWS like?
    a) Security Threat Analytics
    b) Device Health (up down)
    c) Device Management (managing the full device) (updates, patches, policies, etc.). If so we would take full control and they would not have access to manage it as it can only be us or them?
    d) Policy Management of devices
    e) Management of security policies on SaaS based technologies.
    f) All of the above

    Response: *A and B.*

36. **Question:** Would SAWS also like us to manage / monitor any other devices (security devices as well as non-security devices such as Servers, Active Directory, etc.?)

    Response: *We are going to be receiving logs from non-security devices like Active Directory and potentially others.*

37. **Question:** How many GB of raw log data do you ingest in a 24 hour period?

    Response: *We average 40 Gb per day.*

38. **Question:** Can you provide us with your average security log volume, measured in GB per day?
    a) Do you anticipate log volume growth over the next 18 months?

    Response: *We average 40 Gb per day and expect to grow based on additional log sources.*

39. **Question:** Do you currently have a requirement that the chosen vendor's SOC resides within the US?

    Response: *No.*

40. **Question:** Is Splunk Enterprise Security currently deployed or would are you looking to implement Splunk and requesting assistance?

    Response: *We are looking to receive guidance to make sure it is according to MSS vendor's specifications.*

41. **Question:** Service Level Agreement – Can you confirm your requirements for the Service Level Agreement?

    Response: *Per Section 1, B. Scope of Service, the vendor shall submit their service level agreement for SAWS to review.*

42. **Question:** Do you have security devices which do not report to your SIEM but require monitoring?

    Response: *No.*

43. **Question:** How many actionable incidents per month are triaged by your security team?

    Response: *We average 8 per month.*

44. **Question:** Can you provide us with a list of security devices you would like supported?

    Response: *Security devices will not supported by MSS with the exception the events they generate.*

45. **Question:** Can you define co-management of the SIEM?
    a) i.e: Division of **responsibilities** and access

    Response: *MSS vendor will provide their experience to help SAWS tune their SIEM by providing guidance and advocating for improvements that would produce better detection and visibility.*

46. **Question:** Do all of your security devices reside in the same physical location?
    a) If not, how many locations are there?

    Response: *Two physical locations and one from a logical point of view.*

47. **Question:** Section IV. C. 4. Safety refers to "SAWS PPE Guidelines for Industrial Facilities, Vendor/Contractors safety program". Can you please provide the guidelines for our review?

    Response: *For more information visit the following link:* http://www.saws.org/business_center/specs/safetyprodspecs/

48. **Question:** Are you looking for this to be a Co-Managed solution (i.e. both the customer and service provider have access to the SIEM platform 24/7)?

    Response: *Yes.*

49. **Question:** Are there any compliance requirements to be met with this Managed SIEM solution? If so, please describe.

    Response: *No, however we do have PCI and HIPAA requirements.*

50. **Question:** What size Splunk license is in use?

    Response: *50 Gb.*

51. **Question:** Please describe any recurring operational/security pain points.

    Response: *False positives.*

52. **Question:** Please list/identify any and all KPIs or success requirements for security monitoring.

    Response: *Meeting the actionable requirement and the Service Level Agreement.*

53. **Question:** What Splunk Licenses (type & volume) does SAWs own?
    a) Example: 100GB/day Splunk Enterprise
    b) Example: 100GB/day Splunk Enterprise Security

    Response: *50 Gb/day Splunk Enterprise and Splunk Enterprise Security.*

54. **Question:** Are there any apps or vendor plug-ins installed?

    Response: *Yes.*

55. **Question:** Is the environment on premise (SAWs Data Center) or in a cloud environment? If so what vendor (Splunk Cloud, Bring your Own Licenses to MS Azure, Google, etc.).

    Response: *The environment is on premise.*

56. **Question:** With regards to training what is expected? Are you looking for custom classes or unlimited Splunk education credits?

    Response: *An explanation of key configuration and tuning would be expected. Delivery of Splunk training or custom classes are not required from MSS vendor.*

57. **Question:** If custom training, please define the number of students, frequency of classes, agenda / subject matter, and if remote or on-site learning is desired.

    Response: *Delivery of Splunk training or custom classes are not required from MSS vendor.*

58. **Question:** Is SAWS software under active Splunk subscription & support (maintenance)?

    Response: *Yes.*

59. **Question:** Can we respond using a DIR (Department of Information Resources) contract vehicle?

    Response: *This is an open market solicitation. While DIR is not a requirement if a vendor should choose to submit in accordance to DIR the proposal will be reviewed. However, all of the SAWS solicitation required documents need to be submitted as stated in the RFP to include, but not limited to the Compensation Proposal.*

60. **Question:** Has SAWS had a 3rd party perform a maturity analysis and compare the results with the industry baseline for current, target, and future state in the last 12 months?

    Response: *Yes.*

61. **Question:** How many FTE's are currently supporting the SAWS Threat Program? What functions?

    Response: *Three full-time equivalents (FTE) with security analyst/engineering and architecting functions.*

62. **Question:** Are you working with additional partners or other 3rd parties around this project? If so, which ones and/or what is their anticipated involvement today and in the future?

    Response: *No.*

63. **Question:** Is there a case management or ticketing solution dedicated to the threat detection and response program?
    a) Is there any automation with a ticketing/workflow tool?

    Response: *There is currently no case management system and Cherwell is used for ticketing. Some tickets are created automatically.*

64. **Question:** What is the geographic scope of the SOC? Multi or single location?

    Response: *One single location.*

65. **Question:** What devices/data is feeding into their SIEM? Please provide a detailed list/approx. count.
    a) File/Gen Servers
    b) Workstations
    c) Firewalls (models)
    d) Switches/Routers
    e) AD Servers
    f) SQL Servers

    Response: *A, B, C, D, E and F.*

66. **Question:** What are the Splunk EPS/EPD counts?

    Response: *11,000 EPS and 950,400,000 EPD.*

67. **Question:** Do you have an Operating Manual?

    Response: *We have an Incident Response Plan and Playbooks used by our Computer Security Incident Response Team (CSIRT).*

68. **Question:** Do you have defined Runbooks? RACIs?

    Response: *Yes, we have runbooks. We have not developed a responsibility assignment matrix (RACI), but one would need to be developed.*

69. **Question:** Can you share any other processes currently being leveraged in your SOC?

    Response: *No, it is not used for any other process.*

70. **Question:** Is the current SOC responsible only for threat monitoring and response or is it also responsible for Technology tuning and use case development?

    Response: *Yes, it is also used for technology tuning and use case development.*

71. **Question:** Can you provide any sample reports that are used in the SOC to help provide an indicator of how we can propose maturing them in a proposal?

    Response: *No.*

72. **Question:** What is your desired finding/alert triage process?

    Response: *Follow our Security Incident Risk Categorization Guidelines to assign an initial category to a potential incident and follow agreed Escalation Procedures.*

73. **Question:** Do you have any custom Use Cases or Reports?

    Response: *No.*

End of Questions and Answers

ACKNOWLEDGEMENT BY RESPONDENT

Each Respondent shall acknowledge receipt of this Addendum No. 2 by noting such and signing below.

This undersigned acknowledges receipt of this Addendum No. 2 and the bid proposal submitted herewith is in accordance with the information and stipulations set forth.

_____ _____

Date Signature of Respondent

End of Addendum