GUAM POWER AUTHORITY
ATURIDÅT ILEKTRESEDÅT GUAHAN
P.O.BOX 2977 • AGANA, GUAM U.S.A. 96932-2977

May 22, 2017

AMENDMENT NO.: I

TO

INVITATION FOR BID NO.: GPA-062-17

FOR

SPLUNK ENTERPRISE LICENSE UPGRADE & SUPPORT

Prospective Bidders are hereby notified of the following response to inquiries received from Data Management Resources dated May 17, 2017:

QUESTION:

1. Bid Item 1.0 specifies "Splunk Enterprise License Upgrade & Support."
   a. What is the current Splunk implementation in terms of daily data indexing, data sources, number of users, dashboards and charts?
   b. How is the current Splunk installation being managed?
   c. Who is managing the current Splunk system?
   d. What is their role in the upgrade?
   e. How many total users are expected to use the tool?
   f. How many concurrent users are expected to use the tool?

ANSWER:

   a. Daily Volume is at 500Mb; around 10 data sources; 5 current users accessing; built-in dashboard and charts.
   b. This is managed by GPAIT.
   c. This is managed by GPAIT.
   d. GPAIT shall configure all endpoints for machine data export (Bidder/Vendor shall not configure any endpoint).
   e. 10 users are expected to use the tool.
   f. 5-7 concurrent users.

QUESTION:

2. Bid item 1.0 specifies "On-premise Perpetual License/10GB Daily Index Volume." Please provide more details behind the 10GB sizing estimation. What are the daily expected data volume estimations per server, firewall, switches intrusion prevention devices, chassis, blades and AD controller?

ANSWER:

GPA has required '10GB Daily Index Volume'. Daily volume estimations are not of concern as long as 10GB is not exceeded. Fine tuning of data export and/or reduction of endpoints will be done as needed to fit in the 10GB daily requirement.

QUESTION:

3. Bid item 1.0 specifies "Maintenance and Support." Is there any expectation of onsite support?

ANSWER:

No onsite support has been specified, therefore is not required.

QUESTION:

4. Section 1.3.1, letter b of the bid specifies "Server/Compute, Storage, and/or Virtual Machines."
   a. Please clarify what type of storage is available; e.g. SAN DAS, NAS etc.?
   b. Where is the geographical location where the VMs will be setup?
   c. Will there be any multiple VM geographical locations?

ANSWER:

a. SAN storage will be used.
b. Fadian HQ is the location of the setup.
c. No multiple geographical locations.

QUESTION:

5. Section 2.2 of the bid specifies "Log Sources-Machine data shall be required to be collected." What are the different types of log file formats that need to be integrated? e.g. .cvs, .txt, .log, etc.

ANSWER:

There are only two (2) types of logs specified from 2.2.1 to 2.2.7 which is syslog and SNMP. However, for some devices, 'eStreamer' shall be a required format.

QUESTION:

6. Section 2.2.1 of the bid specifies "GPA's Blade Server Infrastructure."
   a. What is the output log file format of the Blade servers?
   b. What is the expected daily average log volume per server?

ANSWER:

Log file format is Syslog, SNMP, or eStreamer. There shall be no need to know what are the variants of devices because GPAIT shall handle the export of the machine data.

QUESTION:

7. Section 2.2.4 of the bid specifies "Intrusion Prevention Systems."
   a. How many variants of intrusion prevention systems need to be integrated?
   b. What is the file format for the logs generated?

ANSWER:

Kindly refer to the response of Question No.: 6.

QUESTION:

8. Section 2.2.5 of the bid specifies "Network Firewalls."
   a. How many variants of firewalls need to be integrated?
   b. What format of logs do they generate?

ANSWER:

Kindly refer to the response of Question No.: 6.

QUESTION:

9. Section 2.2.6 of the bid specifies "Layer-3 (L3) Switches."
   a. How many variants of switches need to be integrated?
   b. What format of logs do they generate?

ANSWER:

Kindly refer to the response of Question No.: 6.

QUESTION:

10. Section 2.3 of the bid specifies "Dashboards and Charts."
    a. Who is the target audience for the dashboards and charts from Splunk?
    b. Does GPA have any wireframes/prototypes for dashboards/charts?
    c. If yes, Can we obtain a copy of all wireframes/prototypes?

ANSWER:

a. This is specified from 2.3.1 to 2.3.3, which is 'Executive' for Executive or Management Team, 'Security' for Security Team, 'Network Infrastructure Operations' for Network Infrastructure Operations Team.
b. GPA does not have wireframe or prototypes for dashboards/charts. Bidder shall propose design which they believe is industry standard and shall be approved by GPA.

QUESTION

11. Section 3.1.1 of the bid specifies "Operating System setup and configuration." Does GPA have a preferred operating system? e.g. Windows, Linux, Unix

ANSWER:

Refer to 2.1, Bidder shall provide the design and architecture of the solution, however, the Splunk solution normally calls for Linux based OSes for proper operation. GPA recommends Red Hat, Bidder shall propose which and best version to use.

QUESTION:

12. Section 3.1.2 of the bid specifies "Bug-fixes and Prerequisite patches: Bidder shall be responsible for the installation of required bug-fixes, program/s and/or patches to ensure the normal and reliable operation of the installed Operating systems; security updates/patches shall be installed as requirement for GPA's cyber security policy.
    a. What are the specific security policies/standards that are required to be met?
    b. What type of threat subscriptions may be available for correlation?

ANSWER:

a. NIST 800 series.
b. None at the moment

GPA requires that all systems be updated with current security patches respective of OS and patched for any known bugs of the solution, OS, and/or both.

QUESTION:

13. Does GPA require any alerts to be setup? If yes, please specify what alerts and the frequency of these alerts that are required to be setup.

ANSWER:

It is not specified and is not required at the moment. However, Bidder may configure alerts if they wish as an alternative or 'free of charge' but must still meet delivery timelines.

QUESTION:

14. Is database monitoring required? If yes, how many databases and which variants will need to be monitored?

ANSWER:

Database monitoring has not been specified and is not required at the moment.

QUESTION:

15. What are the data retention requirements? i.e. Retain data in Splunk for 1 year, 6 months or 3 months.

ANSWER:

Data retention shall be 1-YR and not exceeding 5TB of storage space.

QUESTION:

16. Is there any requirement to archive data? If yes, what is the archiving requirement?

ANSWER:

No. There is no requirement at the moment. This shall be the responsibility of GPAIT.

QUESTION:

17. In consideration of backing up Splunk configuration files/data regularly, what are the available data backup policies in a VM?

ANSWER:

This shall be the responsibility of GPAIT.

QUESTION:

18. Is there any versioning control system already in place? e.g. Github

ANSWER:

No, there is no versioning control in place.

QUESTION:

19. Will there be any TEST/DEV environments for Splunk?

ANSWER:

There is no TEST/DEV environments in place. GPA shall provide resources, but Bidder shall prescribe environments and specifications.

QUESTION:

20. We respectfully request a two (2) week extension in the bid submission deadline to allow for adequate bid preparation time upon receipt of GPA responses to the above.

ANSWER:

Bid Opening date is changed from 2:00 P.M., Wednesday, May 24, 2017 to now read 2:30 P.M., Wednesday, May 31, 2017.

All other Terms and Conditions in the bid package shall remain unchanged and in full force.

JOHN M. BENAVENTE, P.E.
General Manager