



GUAM POWER AUTHORITY

ATURIDÁT ILEKTRESEDÁT GUAHAN
P.O.BOX 2977 • HAGÁTÑA, GUAM U.S.A. 96932-2977

May 28, 2021

AMENDMENT NO.: III
TO
REQUEST FOR PROPOSAL NO.: GPA-RFP-20-006
FOR
NETWORK VULNERABILITY ASSESSMENT

Interested Firms/Individuals are hereby notified of the following change and response to inquiries received from Offeror No.: 1 dated March 19, 2020, Offeror No.: 5 dated April 13, 2020:

CHANGE:

1. Closing date is changed **FROM** 4:00 P.M. Tuesday, April 28, 2020 (CHamoru Standard Time) **TO NOW READ** 2:00 P.M., Friday, June 18, 2021 (CHamoru Standard Time).

Offeror No.: 3 dated 03/19/2020:

QUESTIONS:

1. SEL LLC (Engineering Services – Infrastructure Defense - Secure Solution) desires to submit a proposal for GPA-RFP-20-006. Pertaining to Paragraph 7.1.3 on Independence we request if SEL LLC should bid based on:
 - Independent and not affiliated with any manufacturer or vendor of security equipment
 - Does not profit in any way from a client's selection of vendors or contractors
 - Does not sell security equipment
 - Does not have any form of affiliation with a product or service that could be construed as a possible conflict of interest

SEL Inc prides itself in including security in every product or system, but the majority of our devices are not "security equipment". Separate to SEL Inc, SEL LLC is not agnostic to only selling SEL equipment, Engineering Services and Secure Solutions focuses our expertise on selling right solution to meet our customer's needs. We are the experts in designing, assessing, and securing Energy Control Systems.

Please answer the following:

SEL LLC is a separate organization and legal entity from SEL Inc (R&D, Product, Manufacturing). Does this separate us enough from manufacturing or profiting from SEL Inc past, current, and future sales?

ANSWER:

Please provide such information on the RFP response so that the Review Committee can review the information.

2. SEL Inc design SEL-3620 Security Gateways and SEL OT-SDN and had security built into many products such as the SEL RTAC. Does this constitute the definition of “security equipment”?

ANSWER:

For this RFP, the meaning of Security Equipment is any equipment whose primary purpose is to provide network or application security. Security built into control devices whose primary function is not security is not considered Security Equipment. Please provide related information during the proposal for additional clarification.

Offeror No.: 5 dated 04/13/2020:

QUESTIONS:

1. Will GPA accept an electronic submission?

ANSWER:

Kindly refer to Page 4 of 44 under Section 1.4 Preparation and Submission of Proposals.

QUESTION:

2. Will a Notary Public from the United States be acceptable on the signed Affidavits?

ANSWER:

Yes.

QUESTIONS:

3. If the COVID-19 pandemic delays the project start beyond 60 days from the opening of the bids, will GPA allow the winning bidder to make necessary adjustments to their proposal?

ANSWER:

Yes

QUESTION:

4. There is no plan duration or scope defined; can GPA provide more information on expectations for the extent of the assessment and testing desired, including the expected budget, and what percentage is desired for IT vs. OT?

ANSWER:

Vendor is expected to provide project plan to include the scope of assessment, processes, duration, deliverables and project timeline.

QUESTION:

- 5. Please provide the number of buildings that will be included in the assessment, the types, and numbers of facilities, such as data centers, retail locations, power plants, etc. Will it be acceptable to evaluate the physical security of a sample of substations?

ANSWER:

Assessment of the physical security will be based on a sampling of related sites and locations as listed below:

Building Name	Location	Type of Facility	No of Locations
Fadian Data Center	Mangilao, Guam	Data Center	1
Substations	Various	Electrical Substation	31
Power Control Station	Mangilao, Guam	Data Center	1
Generation Plants	Various	Power Generation	16
Transmission & Distribution	Dededo, Guam	T&D Facility	1
Transportation	Tamuning, Guam	Transportation Bldg.	1
Julale Customer Service Site	Agana, Guam	Customer Service Site	1

QUESTION:

- 6. To assist in scoping, can GPA provide the approximate numbers for the following:
 - Routers, switches, firewalls, and modems that are to be assessed on the IT and OT networks?
 - Servers to be evaluated, and what percentage of the servers are virtual and cloud-based?
 - Desktops and laptops supported by GPA
 - IDS, Syslog servers, databases to be evaluated as part of the review
 - Individuals at GPA are engineers/operators/technicians that are relevant to be interviewed for cyber and physical security?

ANSWER:

Because of security concerns this type of information can be provided upon request during the Price Proposal negotiations.

QUESTION:

- 7. Are Building Access Management systems to be evaluated as part of this assessment?

ANSWER:

No.

QUESTION:

- 8. Approximately how many pages of policy and procedure documents currently exist to be assessed as part of this effort?

ANSWER:

GPA has the following:

- GPA Cyber Security Policy
- Various SOP's in reference to GPA data, hardware, facility and security

QUESTION:

9. Are substation end devices (e.g., protective relays, RTUs, PLCs) to be evaluated? If so, is there a testbed environment that can be used for testing?

ANSWER:

RTU's, PLC's and other connected control devices can be considered but are not required to be part of scope.

QUESTION:

10. Is the Tier 2 Wireless Network to be evaluated for the AMI smart meters? Or are there additional wireless networks to be evaluated?

ANSWER:

Smart Meters will not be included. Only the Teir 2 Wireless network.

QUESTION:

11. Could additional details be provided on what devices are on the "IoT LAN" and what is desired to be evaluated?

ANSWER:

Currently GPA does not have any IoT Lan devices.

QUESTION:

12. How many Siemens Power 6 systems are present? Is it one per substation, or is it one master system in the primary Control Center?

ANSWER:

There is one Power 6 System in the primary Control Center.

QUESTION:

13. What is the make/model of the EMS to be evaluated?

ANSWER:

Because of security concerns this type of information can be provided upon request during the Price Proposal negotiations.

QUESTION:

14. Under 7.1.1 – Experience – is GPA really looking for copies of deliverables (i.e., other reports we've written for cybersecurity of utilities?) Or will descriptions of what we have done for other utilities suffice?

ANSWER:

Information from other related projects that will help in the review of prior experience related to the proposal is recommend.

QUESTION:

15. Will it be acceptable to update section XV of the draft contract to state: *“The CONTRACTOR shall indemnify and hold GPA harmless from any claim, liability or product liability, loss, damage, demand, cause of action or suit, expense or reasonable fee of legal counsel arising out of or in connection with the CONTRACTOR’S negligence in the performance of the goods or services the CONTRACTOR provides.”*

ANSWER:

This can be amended upon approval by GPA’s legal counsel.

QUESTION:

16. We would require the following under Supplemental contract provisions.

Network Access and Service Limitations

GPA understands that CONTRACTOR may use various methods, systems, equipment and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. The GPA authorizes CONTRACTOR to perform such Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services) on network resources with the internet protocol addresses (“IP Addresses”) identified by GPA. GPA represents that, if the GPA does not own such network resources, it will have obtained consent and authorization from the applicable third party to permit CONTRACTOR to provide the Security Services on such third party’s network resources. CONTRACTOR shall perform Security Services during a timeframe mutually agreed upon with GPA. The Security Services, such as penetration testing or vulnerability assessments, may also entail buffer overflows, fat pings, operating system specific exploits, and attacks specific to custom coded applications but will exclude intentional and deliberate DOS (“Denial of Service”) attacks. Furthermore, GPA acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding the GPA’s systems and accepts those risks and consequences. Upon execution of the Schedule/SOW for such Security Services, GPA consents and authorizes CONTRACTOR to provide any or all of the Security Services specified in the applicable Schedule/SOW with respect to the GPA’s systems. GPA further acknowledges that it is the GPA’s responsibility to restore network computer systems to a secure configuration after the completion of CONTRACTOR’s testing.

GPA understand that, although CONTRACTOR’s Services may discuss or relate to legal issues, (i) CONTRACTOR does not provide legal advice or services, (ii) none of such Compliance Services shall be deemed, construed as or constitute legal advice, and (iii) The GPA is ultimately

responsible for retaining their own legal counsel to provide legal advice. Furthermore, the Reports provided by CONTRACTOR in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to GPA's or GPA's legal or regulatory compliance.

ANSWER:

This can be amended upon approval by GPA's legal counsel.

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


for JOHN M. BENAVENTE, P.E.
 General Manager 