Brazos River Authority

August 6, 2019

Addendum No. 1
SECURITY PROGRAM CONSULTING SERVICES
RFP No. 19-07-1121

It is the responsibility of the Respondent to assure and guarantee by acknowledging the receipt of this Addendum in the Proposal that the Respondent has received the Addendum in its entirety, and that the Respondent accepts all conditions contained herein.

Note to Potential Respondents: Based on some of the questions below, BRA is concerned that some Respondents are considering the submission of fee proposals as part of their responses to this RFP. This request is for a Statement of Qualifications, not a technical proposal including fee. Any response that includes a fee proposal, description of work effort (such as a FTE or hour tabulation), or any other cost related information related to the potential work *will not be reviewed and shall not be submitted.*

Question 1:
Under the Tab B requirement page, Is this a mandatory requirement to have the registered Project Engineer with the State of Texas? If yes, what is the scope of responsibilities for this Project Manager (Engineer)?
Answer 1:
As indicated in Tab B, Item 2, the project manager does not have to be a professional engineer, but a professional engineer is preferred. The contemplated work includes review and protection of critical, physical infrastructure including the assessment of asset risk. The intent is for this work to be conducted under the supervision of a professional engineer in the State of Texas (at the time the work is conducted). If the project manager is not a professional engineer, respondent must have professional engineers in responsible charge roles for the appropriate tasks.

Question 2:
What are the requirements Professional Liability Insurance coverages?
Answer 2:
Please refer to Section 12. Insurance Requirements of the solicitation.

Question 3:
Under Tab A, Item 4, it requires similar experience in the last 5 years. Since majority of the work was done back around 2002, it is difficult to meet this requirement, is it possible to waive this requirement or extend the timeline to cover the original work done back in 2002-2003.
Answer 3:
Recent experience and references are still requested, but relevant experience from 2000 to current may be submitted.

Question 4:
Does BRA have an existing security program plan documenting BRA's information security Program including the current program management and common security controls? If so, will This documentation be provided during due diligence?
Answer 4:
The BRA maintains a security program. Information related to the program will be provided to the selected consulting team upon execution of a contract and completion of appropriate security background checks.

Question 5:
What framework standards, guidelines, and/or practices (i.e., CIS CSC, COBIT 5, ISA 624432-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013, NIST SP 800-53 Rev. 4, etc.) Are currently being used and/or followed by BRA? Are any other common standards being utilized? If so, please identify.
Answer 5:
BRA is using the NIST Cyber Security Framework

Question 6:
The request reads security program development and alignment, while we didn't see any reference, does the scope include areas in the AWIA outside of cyber security and physical site security?
Answer 6:
No.

Question 7:
Does the scope of All-Hazards review include responses based on hazardous materials that could threaten water resources or is this strictly from the perspective of cybersecurity?
Answer 7:
Technically, yes, the hazards review will include a review of all hazards including hazards that could affect water quality as well as water supply availability. However, BRA maintains extensive information related to water quality and potential water quality impacts along the river. As such, most effort in the all-hazards review will be directed toward physical and cyber security.

Question 8:
Does BRA maintain administration over Operational Technology with in house staff or outsourced to 3rd party?
Answer 8:
In house staff.

Question 9:
Is there a time limit for management support under phase 3? Possibly an annual contract?
Answer 9:
A time limit for Phase 3 services has not been determined.

Question 10:
Is there a defined budget or price range for this project that the agency can share with respondents?
Answer 10:
Not available at this time.

Question 11:
If there is a distribution list for any notifications of this RFP, can you please add me to it?
Answer 11:
Not available at this time.

Question 12:
Is BRA is expecting a full assessment of the resiliency of these physical assets (including the source water itself) in case of various types of hazards such as cyber-attacks and natural disasters?
Answer 12:
The BRA currently has multiple initiatives underway that will address resiliency. This contract will focus on the resiliency of systems to anthropogenic physical and cyber threats. Natural disaster resiliency will be addressed under other initiatives with collaboration of this security effort.

Question 13:
Has BRA already conducted physical security assessments required for performance of phases 2 and 3?
Answer 13:
BRA maintains physical security assessments of its facilities. The selected consulting team will need to have the capabilities necessary to review these assessments and recommend improvements or adjustments to them. The BRA operates dam facilities, water treatment plants, wastewater treatment plants, pump stations, pipelines and associated offices.

Question 14:
Is BRA expecting this to be a table-top review or do we need to include site visits in Phase 1? If so, how many total sites are to be included?
Answer 14:
This is an item that will be developed during scope and fee negotiations and BRA is amenable to the proposed technical approach providing recommendations related to the value of desk-top vs. site based analyses. If site visits are required, BRA will provide access to facilities so that the selected firm can conduct their work.

Question 15:
Does BRA expect this team to perform additional security audits in phase 2?
Answer 15:
It is BRA's intent for the security audits in Phase 2 to be external to the security program team.

Question 16:
Please provide brief descriptions including size and capacities for the treatment facilities as well as length and size of pipeline systems.
Answer 16:
This information is not required for a statement of qualifications on capabilities and will be provided to the selected team as part of scope and fee negotiations.

Question 17:
Is an Emergency Response Plan for systems and facilities envisioned as part of the Comprehensive Security Program?
Answer 17:
Comprehensive emergency response planning is not anticipated as part of this work. However, detection, response and recovery planning related to physical and, in particular, cyber security incidents is a component of this work.

Question 18:
Does BRA have a preferred GRC documentation tool that should be used to document the framework and risk assessments?

Answer 18:
No. It is BRA's preference that the selected tool be a product that can be utilized and maintained by BRA following completion of this contract's services.

Question 19:
Under the description of Phase 1, it states that Consultant will assist BRA in development of a security program maturity assessment using industry standard materials. Can you clarify what is meant by Industry Standard Materials? Is this the CSF and RMF?
Answer 19:
Yes, the BRA is interested in use of materials built around the Cyber Security and Risk Management Frameworks, and not proprietary tools that do not map or will require a secondary translation of information to map to CSF/RMF.

Question 20:
Often control systems and networks are operated and controlled by different organizational units than those that support business applications and networks. To what extent are the functions separated, and possibly controlled though separate functional groups that have\ separate governance expectations? Asked a different way, are the control or SCADA systems operated and managed by the same organization that manages the business systems, or will there be a second set of similar controls performed by different people in the organization?

Answer 20:
One group has primary responsibility for the business network and supports multiple groups that utilize and maintain various components of the SCADA system. These groups currently collaborate on their needs and their respective roles to maintain a set of hard and soft controls for both systems. The consultant will be expected to coordinate soft and hard control improvements with each group to ensure a single set of final controls is developed that can be deployed across both systems. Where special features are required for the business or the SCADA network, those will be identified in the control set, but it is not the intent of the BRA at this time to have multiple control sets.

Question 21:
Does BRA have a software development function that will need to be evaluated for SDLC?

Answer 21:
No.

Question 22:
From a Cyber-security standpoint can you give an indication as the number of applications supported in house and if any data or applications are hosted by a cloud service provider? This would include independently operated treatment and pipeline control systems.

Answer 22:
This information is not required for submission of qualifications and will be provided to the selected consultant during scope and fee negotiations.

Question 23:
From both a cyber and physical assessment standpoint how many physical locations contain significant security concerns, computing resources such as control systems, security systems, application or database servers? From the description there are 18 separate facilities that BRA is responsible for, that would need to be evaluated.

a. 3 reservoir control facilities
b. 2 pipeline systems, are these operated out of the central office?
c. 9 wastewater treatment facilities
d. 2 water treatment facilities
e. 2 Office locations

Answer 23:
The listing of facilities provided in the question is accurate. Additional information on facility security will be provided to the selected consultant following notice to proceed and completion of appropriate security background checks.

Question 24:
Is it the expectation that all the facilities would be independently evaluated, or would a sampling approach be expected?

Answer 24:
This information is not required for submission of qualifications, and is anticipated to be a discussion point during scope and fee negotiations. In general, this is intended to be a holistic study, but redundant work is not the intent of the BRA. If certain vulnerabilities can be confirmed through a desk-top or facility plan review, BRA will be amenable to such a review.

Question 25:
Are subcontractors required to fill out the pre-qualification form?
Answer 25:
The pre-qualification form is not required.

Question 26:
How many cyber security specific assessments will be included in this *"comprehensive review of assets, security maturity, and vulnerability across all its <Brazos River Authority> assets and operations?"*
Answer 26:
This information is not required for submission of qualifications and will be provided to the selected consultant during scope and fee negotiations.

Question 27:
What is the desired scope of the cybersecurity specific assessments (e.g. specific applications, platforms, 3rd party, internally-developed code, etc.)?
Answer 27:
This information is not required for submission of qualifications and will be provided to the selected consultant during scope and fee negotiations.

Question 28:
How many security audits will the selected vendor complete each year?
Answer 28:
See answer to Question 15 above. Audits are anticipated to be external to the security program team. Further, this information is not required for submission of qualifications and will be provided to the selected consultant during scope and fee negotiations.

Question 29:
What is the nature of these audits (e.g. what governing body and associated certification, if applicable)?
Answer 29:
The nature of the audits will be developed as a component of Phase 1 services with input from the security program consultant.

Sincerely,

Clarissa Cabrera, CTPM, CTCM

Clarissa Cabrera, CTPM, CTCM
Purchasing Manager, Administrative Services