TRANSBAY JOINT POWERS AUTHORITY

REQUEST FOR PROPOSALS No. 17-11
INFORMATION SECURITY/CYBERSECURITY SERVICES

QUESTIONS & ANSWERS

The following questions were received by the original deadline. An additional Q&A set is pending.

1. ***Is there an existing InfoSec/Cybersecurity Plan?***

   A: No.

2. ***How many servers and what operating systems?***

   A: Refer to Specification Section 27 21 00, Data Communications Network Equipment, for hardware information.

3. ***What applications/functions are the above servers supporting?***

   A: Refer to the Network Topology Diagrams in Attachment 6 – Reference Documents.

4. ***How many endpoints and what operating systems?***

   A: Refer to the port matrices in the IT drawings (Attachment 6 – Reference Documents) for preliminary endpoint quantities. The workstation operating system is Microsoft Windows.

5. ***What is the internal and external IP address count for vulnerability scanning purposes?***

   A: The external IP address count has not been finalized. Refer to the port matrices in the IT drawings for preliminary internal IP address quantities (excluding guest internet access).

6. ***Is penetration testing required?***

   A: Yes.

7. ***Is multi factor authentication deployed, and if so, which solution is in place?***

   A: Multi-factor authentication is provided only for external remote access with limited session numbers. Cisco ISE is the currently specified project solution.

8. ***Is there any existing server/desktop patch management and monitoring solution deployed?***

   A: No.

9. ***Section 10 appears to indicate that the resulting agreement would be based on the form agreement provided within the RFP; however, due to the sensitive and unique nature of the security services to be provided, we request that we be permitted to submit our response to the RFP using our IT services agreement as the base document for any subsequent negotiations. We would then, in good faith and collaboration with the Authority, redline this IT services agreement to include any Authority required terms. Is this something that may be considered in lieu of the suggested form agreement at this stage of the RFP?***

   A: Yes, although a service agreement that closely resembles one provided in the RFP is preferred. Exceptions to terms in the Model Agreement attached to the RFP must be noted.

10. ***Are there additional security tools or applications (other than those listed in Attachment 6) that TJPA intends to deploy (e.g. Endpoint Detection and Response, Vulnerability Management tools, etc.). If so, will the selected vendor have full access to those tools? If TJPA does not intend to deploy other security tools, what is the minimum toolset TJPA would look to the vendor to provide.***

    A: No. Additional security monitoring and management tools and/or applications may be recommended by the Respondent/Consultant. Should additional security monitoring and management tools and/or applications be needed per the Respondent/Consultant's recommendations, they are to be provided by the Consultant as part of the Services.

11. ***Would TJPA be open to having device management services provided from the U.S., but security event monitoring services provided by onshore/offshore Security Operations Center analysts (all monitoring of infrastructure would be U.S.-based and no client data would be sent offshore), in order to allow for more advantageous cost in delivering the services?***

    A: No.

12. ***Does TJPA want to include targeting of TJPA, their brand, employees, etc., in the trend/threat reporting?***

    A: Yes.

13. ***Does TJPA prefer to use existing security tools with centrally managed consoles or with established vendor relationships?***

    A: Yes. Any additional security monitoring and management tools are to be provided by the Consultant as part of the Services.

14. ***TJPA communicated that the interviews will be held on January 16. In the event our proposal becomes shortlisted, is there flexibility to attend the interview the week of January 8 due to a military reserve commitment of one of our key personnel?***

    A: Specific arrangements may be possible when interviews are scheduled.

15. ***In section 2.4.f it is mentioned that 2x1 Gigabit Internet connections provided by AT&T are, or will be, in place at the facility. Are there, or will there be, any additional "WAN" type connections, regardless of provider, that are to be supported and managed at this facility?***

    A: The current Internet access contract is for two (2) 1 GB circuits with the capability to expand the circuit to two (2) 10 GB circuits. No additional WAN-type connections are planned at this time.

16. ***Which devices specifically are included in the building IP systems inventory?***

    A: Refer to the port matrices in the IT drawings for preliminary endpoint quantities and end device details.

17. ***Many of the response times listed in the Incident Severity Level Table (section 4.5) require a restoration time of 24 hours or less. However, it appears that the maintenance associated with the devices listed in Attachment 6 specifies an 8 hour per day by 5 days a week with next business day response (8x5xNBD). Can you please clarify the variance between the two? Example: a device fails at 6pm on a Friday, the selected maintenance program only requires the service provider to respond on Monday.***

    A: The Consultant's Services will be subject to the requirements in Table 1 - Cyber Incident Service Response (Single Incident) in Section 4.5. The Facility IT Operations Group will be responsible for servicing IT equipment.

18. ***In reference to the SLAs outlined in Section 4.5, are there associated penalties for non-compliance?***

    A: Yes, refer to Attachment 2, Model Professional Services Agreement, Article 19.

19. ***Will Internet access be enabled for the security solution? Can the solution take advantage of real-time threat awareness and analysis from outside sources?***

    A: Yes.

20. ***Will the selected vendor be responsible for managing all equipment, software, maintenance, and licenses as detailed in the "Attach 6a Equipment-Software List"? Or, is the intent that the selected vendor will manage only the security equipment and related services?***

    A: The Consultant will be responsible for security equipment and related services. The Facility IT Operations Group will be responsible for servicing IT equipment.

21. Will the selected vendor be responsible for procuring all equipment and software as detailed in the "Attach 6a Equipment-Software List"? Or, will the equipment be procured separately by TJPA?

A: Equipment identified in the attachment has already been procured. Any additional security monitoring and management tools are to be provided by the Consultant as part of the Services.

22. Will the selected vendor be responsible for installation and configuration of all equipment in "Attach 6a Equipment-Software List"? Or, will the selected vendor be responsible for installation, configuration for a subset of the equipment, such as the security devices and services?

A: Equipment identified in attachment has already been procured and will be configured by a separate IT contractor, NetXperts, Inc. Any additional security monitoring and management tools are to be provided by the Consultant as part of the Services.

23. Given the Attachment 6a network equipment list, please provide estimates of the other asset types. What is the estimated total number of assets in scope? What is the estimated number of workstations?

A: Refer to the port matrices in the IT drawings for preliminary endpoint quantities and types.

24. Although there is no goal established for the SBE or DBE participation, do you still expect firms to perform a good faith effort? While we value the work of SBEs and DBEs, we would not be seeking any of their services for this project. Above all, we seek to submit a compliant, competitive bid to the Transbay Joint Powers Authority. Please advise how best to comply with the requirements of RFP 7-11 without the use of SBEs or DBEs.

A: As noted in the RFP, there is no SBE goal for this contract. The Good Faith Efforts Form states that it must be submitted "if the…SBE goal has not been met." As there is no SBE goal, no form is required. However, as also noted in the RFP, Respondents are encouraged to obtain DBE and/or SBE participation. SBE and DBE reporting is required for the proposal and for the duration of the awarded contract irrespective of established participation and goals.