Corporate Finance Department
Materials Management Division

577-2022 ADDENDUM 2

WATER AND WASTE DEPARTMENT CYBERSECURITY REVIEW

ISSUED: Oct 3, 2022
BY: Nand Kishore
TELEPHONE NO. 204 986-2089

URGENT

PLEASE FORWARD THIS DOCUMENT TO WHOEVER IS IN POSSESSION OF THE BID/PROPOSAL

THIS ADDENDUM SHALL BE INCORPORATED INTO THE BID/PROPOSAL AND SHALL FORM A PART OF THE CONTRACT DOCUMENTS

Template Version: Add 2021-03-05

Please note the following and attached changes, corrections, additions, deletions, information and/or instructions in connection with the Bid/Proposal, and be governed accordingly. Failure to acknowledge receipt of this Addendum in Paragraph 10 of Form A: Bid/Proposal may render your Bid/Proposal non-responsive.

QUESTIONS AND ANSWERS

Q1: Does the security clearance and Insurance need to be complete prior to submitting our bid, or can this be completed once we are selected as the final proponent.

A1: Security clearance and Insurance does not need to be completed prior to submitting a response. They are required only prior to signing a contract with the successful proponent.

Q2: Is there a budgetary range for this project?

A2: There no published budget for this project.

Q3: Will it be assigned to single vendor or can be assigned in parts as well? Suppose we will be able to fulfill requirements remotely, won't be able to do physical security assessment.

A3: This project will be awarded to a single Proponent response. Proponent s can include subcontractors in their responses and identify as per the instructions outlined in the RFP.

Q4: It’s hard to price this out as a lump sum. A project of this size and scope is best suited for prequalification of a vendor based on experience and hourly or daily rates. To prepare the best strategy for the organization there should be 1-2 whiteboard sessions to collectively build out the best plan. A lump-sum bid structure can be quite challenging for this type of project. Has there been any thought into a Prequalification bid structure instead?

A4: WWD has requested the responses to include a price breakdown, as well as the lump sum. If any assumptions are made while developing the price breakdown, please include them in your response.

Q5: Physical security assessment is mandatory?

A5: Yes.

Q6: Is it recommended to assess a representative sample less than 100% of assets to reduce engagement cost? If so, what rough level of coverage of IT and OT environments is desired?

A6: WWD expects a representative subset to be assessed. WWD would expect the Proponent to include in their response a recommendation for a subset that could be justified by an industry best-practice.

Q7: Any particular frameworks for gap analysis?

A7: WWD has no preference to a framework for the gap analysis.

Q8: How does the proponent demonstrate evidence of control if we are not allowed to retrieve or read data?

A8: This would be subject to the technology, process or people being assessed. Some examples to demonstrate evidence of control are:

- A screen shot
- Documentation of a repeatable process to gain control
- A picture
- Any other mechanism to show the issue

Q9: Do you have the numbers of internal assets (servers, SCADA systems, ...)?

A9: This information has been included in Addendum 1. Further information is available in the supplementary document; which will be provided after a signed NDA provided in the RFP is received.

Q10: Do all employees need to be email phished?

A10: WWD has no preference whether all employees or a subset of employees are email phished. We would be looking for the industry best practice when conducting phishing tests.

Q11: How many locations should be included in the physical assessment?

A11: The number of total locations is available in the supplementary document; which will be provided after a signed NDA provided in the RFP is received. It is expected that a subset of the locations would be assessed.

Q12: What safety measures will be given to covert testers as they try to access physical locations, particularly for diverse and minority individuals?

A12: In the RFP response, the Proponents can propose the safety measure they are looking for City to take care when they conduct covert testing.

Q13: Is there a date by which all enquiries must be received by?

A13: Enquiries must be received five (5) business days prior to the RFP response date. The response date at the time of publishing this addendum is October 12, 2022.

Q14: Will policies, procedures, and processes be provided to the proponent to review as part of the risk/vulnerability assessment?

A14: The first deliverable will be to develop a plan for the Covert and Overt phase. The Proponent and WWD will work together to determine the appropriate level of material to provide during the Covert exercise. More material will be provided during the Overt exercise.

Q15: Penetration testing and red teaming is intrusive by nature, is there a test lab/environment available for testing of OT infrastructure?

A15: Test environments are available for most of the applications and can be made available to Proponent during the testing. It is expected that Proponent will include their needs in the RFP response.

Q16: Will there be a whiteboarding session to learn what tools/techniques are used by WWD IT, WWD SCADA and Corporate teams in order to gauge preparedness and response times?

A16: A whiteboarding exercise can be in scope of the Overt exercise. It is expected that Proponent will include their needs in the RFP response.

Q17: Is WWD looking for a red team style approach for the covert testing?

A17: A red team style approach would be a valid approach for covert testing. Proponents can suggest any method that accomplishes the desired outcomes of the engagement.

Q18: Is WWD looking for a purple team style approach for the overt testing?

A18: A purple team style approach would be a valid approach for the Overt testing exercise.

Q19: In order to perform an effective penetration test and demonstrate evidence of control, we will need to retrieve and read information. Can you please amend section E2.4 as it currently states:

"All testing must be non-disruptive and non-destructive for both Phases. Despite gaining access, the Proponent cannot at any point in time retrieve, read, store, tamper, destroy or share data or information that has been compromised through the ethical hacking exercise during and after the engagement."

A19: It is expected that the minimum intrusion will be exercised to demonstrate control.

Q20: Please confirm that the proponents do not need to apply for the Global Sanctions & PEP Check and a Police Information Check until they have been selected as the winning proponent.

A20: That is correct.