Winnipeg

Corporate Finance Department
Materials Management Division

774-2023 ADDENDUM 2

WATER AND WASTE DEPARTMENT CYBERSECURITY REVIEW

ISSUED: Nov 07, 2023
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: Is it possible to perform the test remotely? (VPN or directly from the Internet or using our device establishing a connection between our and your infrastructure).

A1: While many aspects of cybersecurity testing and assessment can be conducted online, through the internet for public-facing sites or using VPNs, it's important to note that certain activities may necessitate in-person engagement to fully achieve the cybersecurity assessment's objectives. The choice between online and in-person engagement should be determined in consideration of the project objectives, as outlined in the RFP. Proponents can include their recommendations as part of their proposal response.

Q2: What is the Client expectation of high-level duration/timeline of the project?

A2: The City of Winnipeg is looking for a high-level duration/timeline of the project that aligns with industry standards for this type of cybersecurity assessment project. Proponents are encouraged to propose their project timelines based on their expertise and experience, ensuring that the proposed duration allows for a comprehensive and effective assessment while meeting the project's objectives and the City's expectations.

Q3: How many Corporate departments to be covered for vulnerability assessment (People, process, technology) other than IT and OT sections?

A3: The primary focus of the vulnerability assessment is on WWD IT and OT infrastructure, including people, processes, and technology. However, it's important to note that the vendor will need to collaborate closely with Corporate IT. While the assessment itself is solely on WWD IT and OT, Corporate IT plays a critical role in providing guidelines, processes, and best practices that guide and support the overall cybersecurity efforts. The alignment with Corporate IT ensures that the cybersecurity assessment adheres to the broader organizational standards and maintains consistency with corporate guidelines for security.

Q4: How many Site locations need to be covered? (Single premises or multiple locations)

A4: Multiple locations; specific location details can be provided following the NDA sign-off as per RFP document.

Q5: Technology involved - If it can be disclosed?

A5: This will be disclosed to the successful bidder during discovery phase of project.

Q6: Does the client have a test set-up that can be used for the purpose of SCADA Penetration testing by our tester?

A6: No. Proponents to propose approach for conducting SCADA Penetration testing in accordance with industry standards.

Q7: It 'seems NIST and Canadian guidelines requirements already mentioned in the RFP. Do we need to do an assessment using NERC-CIP also?

A7: No.

Q8: What would be the budget for this project? Are you looking for time and material cost or one lump sum quote?

A8: This project does not have a predefined budget. Proponents are invited to propose their budget for the assessment in a lump sum quote, aligning with the objectives and requirements outlined in the RFP.

Q9: IT infrastructure penetration test –

i) How many IPs (hosts / servers / computers / network devices) will be in the scope of the test? Please provide the number of IPs divided into internal (internal network) and external (Internet facing) addresses.
ii) Please provide the number of VLANs to be tested.
iii) What type of environment will be tested – production / test environment?

A9: See response below

i) Proponents are encouraged to propose a quantity that is sufficient to meet the objectives outlined in the RFP, leveraging their industry expertise and standards to determine the required scope and scale for these assessments. The scope will be agreed upon during the discovery phase of the initiative, and the City of Winnipeg relies on the Vendor's expertise to provide guidance on the necessary coverage for (hosts/servers/computers/network devices).
ii) Proponents are encouraged to propose a quantity that is sufficient to meet the objectives outlined in the RFP, leveraging their industry expertise and standards to determine the required scope and scale for these assessments. The scope will be agreed upon during the discovery phase of the initiative, and the City of Winnipeg relies on the Vendor's expertise to provide guidance on the necessary coverage for (hosts/servers/computers/network devices).
iii) Most applications will be tested in a TEST environment before transitioning to the PROD environment. However, there may be specific cases, such as critical updates or configurations, where testing directly in the PROD environment is necessary to ensure immediate effectiveness. It's essential to underline that any testing performed in the PROD environment will be executed with great care and vigilance to prevent any operational disruption. The decision regarding the choice of testing environment may be based on factors like urgency, criticality, and complexity of changes.

Q10: Web application penetration test – How many web applications will be tested?

A10: WWD has 12 key web applications (3 public facing and 9 internal).

Proponents are encouraged to propose a quantity that is sufficient to meet the objectives outlined in the RFP, leveraging their industry expertise and standards to determine the required scope and scale for these assessments. The final assessment details, encompassing factors such as the number of applications, platforms, forms, user roles, application specifics, technologies, audit environments, and the scope of testing categories, will be collaboratively defined with the selected vendor during the discovery phase to ensure they align with our specific cybersecurity requirements.

Q11: Mobile application penetration test – How many mobile applications will be tested?

A11: WWD has 3 key mobile applications.

Proponents are encouraged to propose a quantity that is sufficient to meet the objectives outlined in the RFP, leveraging their industry expertise and standards to determine the required scope and scale for these assessments. The final assessment details, encompassing factors such as the number of applications, platforms, forms, user roles, application specifics, technologies, audit environments, and the scope of testing categories, will be collaboratively defined with the selected vendor during the discovery phase to ensure they align with our specific cybersecurity requirements.

Q12: Native PC application ("thick client") penetration testing – How many native applications will be tested?

A12: WWD has 3 key thick client systems. Please note that SCADA systems are not included in this count.

Proponents are encouraged to propose a quantity that is sufficient to meet the objectives outlined in the RFP, leveraging their industry expertise and standards to determine the required scope and scale for these assessments. The final assessment details, encompassing factors such as the number of applications, platforms, forms, user roles, application specifics, technologies, audit environments, and the scope of testing categories, will be collaboratively defined with the selected vendor during the discovery phase to ensure they align with our specific cybersecurity requirements.

Q13: WiFi penetration test – How many buildings/locations will be audited?

A13: Approx. 12 locations, 60 Access Points, 3 Wifi Networks. All locations are in Winnipeg, Canada.

Proponents are encouraged to propose a quantity that is sufficient to meet the objectives outlined in the RFP, leveraging their industry expertise and standards to determine the required scope and scale for these assessments. The final assessment details, encompassing factors such as the number of applications, platforms, forms, user roles, application specifics, technologies, audit environments, and the scope of testing categories, will be collaboratively defined with the selected vendor during the discovery phase to ensure they align with our specific cybersecurity requirements.

Q14: Please specify the number and types of systems, network devices and database engines to be audited (along with their versions):

A14: Proponents are encouraged to propose a quantity that is sufficient to meet the objectives outlined in the RFP, leveraging their industry expertise and standards to determine the required scope and scale for these assessments. The final assessment details, encompassing factors such as the number of applications, platforms, forms, user roles, application specifics, technologies, audit environments, and the scope of testing categories, will be collaboratively defined with the selected vendor during the discovery phase to ensure they align with our specific cybersecurity requirements.

Q15: Social engineering / Red Teaming test –

a) What kind of tests/scenarios would you like to be performed among following?
   i) All possible
   ii) Phone attacks
   iii) Attacks through emails
   iv) Attacks through social media
b) How many people should be included in social engineering tests (for each scenario)?
c) Who in your opinion is a threat to your business? What kind of benefits can the hacker achieve?
d) Do you prefer non-intrusive social engineering tests (without taking control over the victim machines) or intrusive Red Teaming test (with taking control over the victim machines)?

A15: See response below

i) All tests and scenarios must be conducted to address the objectives specified in the RFP.

ii) The number of people to be included in social engineering tests for each scenario needs to be proposed by Proponents in their response, provided that the proposed number aligns with the objectives outlined in the RFP and adheres to industry standards.

iii) Threats can originate from both internal and external sources. Internally, any employees or contractors who interact with data, applications, or infrastructure, particularly those responsible for collecting personal or sensitive information, can pose a threat if their actions are malicious or

compromised. Externally, threat actors, including malicious hackers, cybercriminals, or state-sponsored entities, may target our business. These external threats seek various advantages, such as gaining unauthorized access to sensitive data, stealing intellectual property, committing financial fraud, causing operational disruption, or tarnishing our reputation.
Proponents are encouraged to propose in their response any additional factors that should be considered based on their experience and industry standards.

iv) The preference for social engineering tests or Red Teaming tests, whether non-intrusive or intrusive, will depend on the goals and objectives as mentioned in the RFP. We are open to considering both non-intrusive social engineering tests, which do not involve taking control over victim machines, and more intrusive Red Teaming tests that may include taking control over victim machines. The choice will be made in alignment with the project's aims, security needs, and any relevant agreements with the Vendor before the start of engagement, ensuring that the selected approach best serves the cybersecurity assessment objectives. Importantly, regardless of the testing approach chosen, all tests will be conducted with the utmost care to avoid any impact on operations or the compromise of sensitive information. Non-intrusive and intrusive tests will be executed without disrupting the business's ability to operate and without compromising the confidentiality or integrity of information.

Q16: Would the City be able to clarify what is meant by this question:

B11.1 Describe your approach to overall team formation and coordination of team members.

A16: The phrase "Describe your approach to overall team formation and coordination of team members" is a request for you to explain how you go about creating a team and managing its members in a professional or organizational context. When you are asked to elaborate on this, you are expected to provide a more detailed and comprehensive response. Here's a breakdown of what this request entails:

Approach to Team Formation: This part of the question asks you to explain how you typically assemble a team. Your answer should include information about the criteria you use to select team members, the skills and expertise you consider, and any other factors that play a role in team composition. You might also discuss how you decide on the size of the team and the roles within it.

Coordination of Team Members: This aspect of the question is about how you ensure that the team works together effectively. You should describe the strategies and techniques you employ to manage and coordinate team members. This could involve communication methods, task assignment, project management tools, and your approach to resolving conflicts or addressing challenges that arise within the team.

When elaborating on this topic, you can provide examples from your past experiences or specific strategies you've used to form and coordinate teams successfully. Your response should demonstrate your ability to build and manage teams to achieve common goals efficiently and effectively.

Q17: Would the City accept an excel spreadsheet for ongoing project updates?

A17: Yes, the City is flexible in terms of format for ongoing project updates. Proponents are permitted to use any format, including Excel spreadsheets, as long as they can effectively provide responses to the specific questions and information required by the City for project updates. Please ensure that your chosen format allows for clear and comprehensive reporting of the necessary project details and meets the City's information requirements.

Q18: The pricing spreadsheet asks for a lump sum, but also a breakdown of costs. Where should bidders provide the breakdown? i.e. can financial details be included with the technical proposal?

A18: The detailed price breakdown can be included as an attachment to the proposal.