DEPARTMENT OF FINANCE
PROCUREMENT SERVICES
95 Rochford Street, 2nd Floor South, Shaw Building, Room 27
Charlottetown, PEI, C1A 7N8
Telephone: (902) 368-4040 or Facsimile (902) 368-5171

ADDENDUM # 5

For RFP # WCB-2018-07

TO: **All Bidders**

FROM: **Procurement Services**

DATE: **November 9, 2018**

SUBJECT: **Questions and Answers**

Question #38 –

Regarding Black Box Penetration Test;

a) Please specify the type (Server, Database...etc.) and number of hosts/applications in scope for penetration testing?
b) How many hosts are accessible over the internet and how many intranet?
c) Is the penetration testing will be completely onsite or anything in scope from offshore?
d) Is there any wireless devices are in scope? Please describe?

Answer #38

a) Windows Server / SQL Server. Please refer to the response to Question 17 in Addendum 3.
b) Internet: Please refer to the response to Question 17 in Addendum 3. Intranet: None.
c) It is acceptable if the work is done remotely.
d) No.

Question #39 -

Regarding White Box IT Threat & Risk Assessment;

a) Web Applications: How many input fields are there in each application?
b) Web Applications: How many user roles to be assessed in each application?

c) Threat Risk Assessment: How many and what type of policies will be provided for review, and what is the size of each policy?
d) Online Services: Please provide more details about the online services in terms of quantity, size, business purpose, user roles…etc.?
e) Corporate network: Please specify the type and number of hosts/applications in scope for penetration testing?
f) Corporate network: How many hosts are accessible over the internet and how many intranet?
g) Corporate network: Is the penetration testing will be completely onsite or anything in scope from offshore
h) Corporate network: Is there any wireless devices are in scope? Please describe,
i) Remote access, and any other internet facing applications : Could you please provide more details like number of components, purpose, type of service, access details, authentication, end users...etc?
j) Code review: How many code bases will be provided for review?
k) Code review: What is the size of each code base in terms of "Number of Lines of Code"
l) Code review: What are the programming languages used in each code base?

Answer #39

a) Not available.
b) Please refer to the response to Question 32 in Addendum 3.
c) Policies and procedures related to IT security and administration will be provided. There are an estimated eight (8) policies and procedures.
d) Please refer to the response to Question 26(c) in Addendum 3.
e) Please refer to the response to Question 7 in Addendum 2.
f) Internet: Please refer to the response to Question 17 in Addendum 3. Intranet: None
g) Preference will be given to proposals that will conduct the work onsite.
h) No.
i) Please refer to the response to Question 17 in Addendum 3.
j) Please refer to the response to Question 10 in Addendum 2.
k) Please refer to the response to Question 2 in Addendum 1.
l) Please refer to the response to Question 11 in Addendum 2.

Question #40 –

In order to effectively scope the project, can WCB PEI please confirm the following;

Will there be an expectation for web applications to be in scope during the external penetration testing? The applications are a large portion of the external attack surface and would certainly not be ignored by a malicious actor. Without inclusion of the web applications, we do not believe that your organization will obtain an accurate picture of the risk. We recommend an unauthenticated assessment at minimum.

Answer #40

Proposals should consider the website and online services noted in section 4.3 (WCB Overview) of the RFP for the external penetration testing.

Question #41 –

In order to effectively prepare our response, can WCB PEI please confirm the following;

RFP, First Page of WCBRFP form, Section 1. Check for changes to this request, indicates that changes may be posted up until the tender closing time and that it is the responsibility of bidders to take into account ALL Addenda.

Question 2: With all due respect to the RFP's clear intentions to obtain hard copy submissions for responses, we ask that the WCB of PEI to reconsider this stance. With consideration to the fact that Addenda and changes may be posted up until the tender closing time and that it is the responsibility of the bidders to take each into account, hard copy physical deliveries impose undue costs on industry to respond and may limit the amount of responses received by the client. There are printing, packaging, and shipping costs associated with hard copy physical deliveries. Further, as bidders will need to monitor the solicitation posting site to adapt responses to any changes until the tender closing time, respondents will be stuck with last minute surge pricing shipping costs in order to mitigate the risk associated with submitting "early" and potentially missing changes that we are responsible to incorporate. In order for respondents to be agile to potential changes and prepare thorough and compliant responses to the WCB of PEI for this requirement, we recommend that email submissions be considered for responses to the subject solicitation.

Answer #41

The WCB will not be changing the submission procedures as indicated in section 2.5 (Submission Procedures) of the RFP. As indicated in this RFP section – Fax or email responses will not be accepted.

Question #42 –

a) For the black box penetration testing, what would be the scope of the required work? Internal penetration testing? External penetration testing?
b) For the White box and IT& Risk assessment point, what would be the scope of the required work? Web application penetration testing? If yes, how many applications? For the code review phase; How many applications would be in scope? Approximately how many lines of code does each of the applications have?
c) For the assessment, would you like to include the governance and information security management aspect as well as the security technology?
d) How many firewalls do you have?
e) Do you have documentation on your company policies? If yes, how many pages of documentation?
f) Do you have any technical documentation of your environment (network architecture, Visio design)?
g) Is the organization complex to get information from (lots of teams to get information from)?

Answer #42

a) External penetration testing.
b) Please refer to the response to Question 2 in Addendum 1. Proposals should consider the website and online services noted in section 4.3 (WCB Overview) of the RFP as in scope for this work. The WCB is looking for Vendors to propose the approach and methods that will be used to carry out this objective.
c) Governance and information security management will be considered out of scope for this piece of work.
d) One (1).

e) Yes. Please refer to the response to Question 39 (c) in Addendum 5. Estimated pages are less than 100.
f) Some high level network diagrams / documentation will be made available to the awarded vendor.
g) Not complex.

END OF ADDENDUM.

Please return this sheet with your formal bid proposal.