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 # 3

For RFP # WCB-2018-07

TO: **All Bidders**

FROM: **Procurement Services**

DATE: **November 2, 2018**

SUBJECT: **Questions and Answers**

Question #16 –

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - the RFP indicates that as part of the White Box IT Threat & Risk Assessment WCB is seeking a code review of the WCB Website and Online Services. Please clarify if it is a code review that is required or a web application security assessment, as a code review will impact pricing due to licensing requirements. If you are seeking a code review, will you be providing a SSTP site for code downloads to be able to perform the review?

Answer #16

Please refer to the response provided in Addendum #1, Answer #2.

Question #17 -

Regarding Section 4.1.1 (Black Box Network Penetration Test) - how many externally facing IPs are in scope? (#live IPs, not subnets)?

a. What types of devices ex: Firewalls

Answer #17

There are less than 5 external IPs.

a. Firewall.

Question #18 –

Regarding Section 4.1.1 (Black Box Network Penetration Test) - please confirm if the vendor will be required to discover the IP addresses in scope.

Answer #18

The WCB will provide the IP addresses in scope to the awarded vendor.

Question #19 –

Regarding Section 4.1.1 (Black Box Network Penetration Test) - will testing be during standard business hours? (9:00-5:00)

Answer #19

Please refer to the response provided in Addendum #2, Answer #15.

Question #20 –

Regarding Section 4.1.1 (Black Box Network Penetration Test) - Is testing required for compliance reasons such as PCI?

Answer #20

No.

Question #21 –

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - how many externally facing IPs are in scope? (#live IPs, not subnets)?

a. What types of devices ex: Firewalls

Answer #21

Please refer to the response provided in Addendum #2, Answer #7.

a. Firewall.

Question #22 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - please confirm that WCB will be providing the IP addresses in scope.

Answer #22

The WCB will provide the IP addresses in scope to the awarded vendor.

Question #23

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) – Will testing be during standard business hours? (9:00-5:00)

Answer #23

Please refer to the response provided in Addendum #2, Answer #15.

Question #24 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - Is testing required for compliance reasons such as PCI?

Answer #24

No.

Question #25 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) – How many web applications are in scope?

Answer #25

Please refer to the response provided in Addendum #2, Answer #10.

Question #26 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) – please answer the following per web application:

a. How many dynamic pages does the site contain (pages require user input)
b. What programming language is the app written in
c. What is the function of the site?
d. Does the site contain personally identifiable information (PII)
e. How many permission levels in scope? (User A, Admin, etc.)
f. Is the site internet facing or do clients remotely connect?
g. Approx how many lines of code is in the App?

Answer #26

a. Please refer to the response provided in Addendum #2, Answer #11.
b. Please refer to the response provided in Addendum #2, Answer #11.
c. WCB public website and WCB Online Services (see: http://www.wcb.pe.ca/Employers/EServices, http://www.wcb.pe.ca/Employers/LearnAboutOnlineServices, http://www.wcb.pe.ca/ServiceProviders/EServices for more information)
d. The WCB does not wish to disclose this information as part of the public RFP process.
e. Please refer to the response provided in Addendum #2, Answer #11.
f. Internet facing.
g. Please refer to the response provided in Addendum #1, Answer #2.

Question #27 -

Regarding Section 4.1.1 (Black Box Network Penetration Test) - the RFP states that "WCB will not be providing any resources to complete the black box network penetration testing". Will you be providing a technical point of contact with whom we can coordinate activities during testing?

Answer #27

Yes the WCB will provide a technical resource as a point of contact to coordinate activities with the vendor. The WCB will not be providing any resources to execute testing activities.

Question #28 -

The RFP states "It is incumbent on the vendor to insure that no disruption of production systems affecting the business of the WCB is allowed to occur." The nature of actual penetration testing, as opposed to vulnerability assessment, is that there can be no guarantee that the tests will not cause issues with systems. The actual risk depends on the vulnerability that is being exploited, and testing can be coordinated with WCB to minimize risk, however some risk will always be present. Are you able to back up production systems prior to active penetration testing, or are you able to deploy copies of production systems for testing?

Answer #28

Please refer to the response provided in Addendum #2, Answer #15.

Question #29 -

Regarding Section 4.1.1 (Black Box Network Penetration Test) - are there any times/dates that testing is not permitted?

Answer #29

Please refer to the response provided in Addendum #2, Answer #15.

Question #30 -

In section 4.3 (WCB Overview) the RFP lists services that are included. Are there other services?

Answer #30

Please refer to the response provided in Addendum #2, Answer #10.

Question #31 -

Regarding Section 4.1.1 (Black Box Network Penetration Test) - will we be provided with an IP address range to test, within which we will be required to discover services, or will you provide a complete list of target IPs/URLs to test?

Answer #31

Please refer to the response provided in Addendum #3, Answer #18.

Question #32 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - How many web applications do you want tested? Do you want them tested with credentials / accounts? If yes to the accounts questions how many different roles exist in each application?

Answer #32

Please refer to the response provided in Addendum #2, Answer #10.

No.

N/A

Question #33 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - does the WCB want application testing to happen in a production environment that may risk the unintended corruption of production data (or is there a current and updated acceptance testing environment that can be used for application testing?)

Answer #33

The WCB wishes to have testing occur in the production environment - however the vendor will need to communicate any risks with the WCB. If the risk is deemed too high to conduct the test in the production

environment, the test may be modified, abandoned, or an alternate means of testing may be explored at that time if feasible.

Question #34 -

Regarding Section 4.1.1 (Black Box Network Penetration Test) - Can you provide a rough estimate of how many IP addresses and URLs are in scope for the black box testing?

Answer #34

Please refer to the response provided in Addendum #3, Answer #17.

Question #35 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - how many external IP addresses and URLs are included in the security assessment portion of the TRA?

Answer #35

Please refer to the response provided in Addendum #2, Answer #9.

Question #36 -

Regarding Section 4.1.2 (White Box IT Threat & Risk Assessment) - How many internal IP addresses and URLs are included in the security assessment portion of the TRA?

Answer #36

Please refer to the response provided in Addendum #2, Answer #7.

Question #37 -

Regarding Section 4.1.2 - how many pages are on each application to be reviewed? How complex are the pages of the application?

Answer #37

Please refer to the response provided in Addendum #2, Answer #11.

End of Addendum.