REQUEST FOR PROPOSAL

SECURITY AWARENESS SOLUTION SLICITATION FILE NO. RFx000110

QUESTIONS & ANSWERS – OCT. 1, 2019

QUESTION 1

Whether companies from Outside Canada can apply for this (like, from India or USA)?

CMHC RESPONSE

The company must meet the mandatory requirements of the RFP, which includes the ability to provide training in English and Canadian French

QUESTION 2

Whether we need to come over there for meetings?

CMHC RESPONSE

Proposals that meet the mandatory requirements of the RFP will be assessed based on their response to the rated requirements. A short list may be created and asked to present their solution to CMHC preferably in person, however, online would be acceptable.

QUESTION 3

Can we perform the tasks (related to RFP) outside Canada (like, from India or USA)?

CMHC RESPONSE

Yes

QUESTION 4

Can we submit the proposals via email?

CMHC RESPONSE

Yes. Please follow instructions in RFP for submitting propsals.

QUESTION 5

Could you confirm if there has been or is a company who is doing or has done this or similar work in the last 24 month?

CMHC RESPONSE

No, CMHC has been developing their own internal security awareness program.

QUESTION 6

Due to the complex nature of this RFP, would you consider extending the end date to October 21st?

CMHC RESPONSE

No, CMHC has an internal requirement to have this contract in place at our earliest timeframe.

QUESTION 7

I have a question regarding the RFP for the Security Awareness Solution posted by CMHC. Section 1.2 'Introduction and Scope' describes the solution modules to be bilingual. Is that bilingualism also a requirement for the security testing phishing campaigns?

CMHC RESPONSE

Yes, any available module MUST be bilingual English and Canadian French.

QUESTION 8

4.1 Overview of Section – Section 4.6 Project Management Plan is absent from the list of Response Items provided. Is CMHC expecting proponents to respond to the Project Management Plan section in addition to the items listed?

CMHC RESPONSE

Yes, a Project Mgmt. Plan should be included with Proponent's proposals.. It was left off inadvertently from Response List.

QUESTION 9

Appendix A SOW – Under the Scope section CMHC states "The Proponent must provide managed services and support to the CMHC security awareness team", can CMHC explain the scope of 'managed services' they are expecting?

CMHC RESPONSE

The managed services would be hours available from the vendor for professional services support to CMHC at CMHC's physical site and executing their program.

QUESTION 10

Will CMHC accept that emails addresses, first and last name are hosted outside of Canada via Data Center located in USA or Ireland?

CMHC RESPONSE

Yes.

QUESTION 11

Even though you have an LMS, if the proposed console we are suggesting has better reporting and tracking capabilities outside of LMS integration, would you be willing to consider using our proposed solution directly in place of your LMS system? (Keeping in mind, manual set up of the program with your LMS system increases the amount of PS effort required, rather than using the proposed console directly).

CMHC RESPONSE

CMHC requires a vendor with an LMS.

QUESTION 12

Who is your LMS vendor? (We need to understand this for formatting compatibility).

CMHC RESPONSE

CMHC requires a vendor with an LMS.

QUESTION 13

What actions do you envision the Managed Service Desk taking when receiving phishing reported emails from a phishing report button? Please select one of the following options:

a) No service desk action required – You just want your employees to get into the habit of reviewing and taking precautions with all their emails. They will be rewarded and notified if their reported email was a fake phishing email created by us. If it is not a fake, it is simply removed from their inbox, away from harms way, whether it was a real phishing email or just regular spam email.

b) Partial Managed Service Desk Action Required – Service Provider will review all incoming reported phishing emails and advise a CMHC IT Security Desk employee to perform the follow up incident response required on the determined malicious phishing emails.

c) Full Managed Service Desk Action Required – Service Provider will review all incoming reporting phishing emails and provide the necessary incident response on behalf of CMHC on the determined malicious phishing emails defined by the service provider to CHMC.

CMHC RESPONSE

This would depend on the overall viability and structure of the proposed solution. c) would not be an option.