Fisheries and Oceans Canada
ADDENDUM ONE
August 14th, 2019

F5211-190054
Cyber Protection Services

This Addendum shall be attached to and form an integral part of the Contract Documents.

Question 1

For **C.7 IT Security Design Specialist:**

R6. The Bidder should demonstrate the proposed resource's current professional qualifications from the following:

i. Registration/license to practice professional engineering in Canada;
ii. CISSP from (ISC)2;
iii. CISSP / ISSEP from (ISC)2;

Will the Crown accept CCNA Security Certified (Implementing Cisco IOS Network Security) 2012 as it is equivalent CISSP/ISSEP?

iv. CISSP / ISSAP from (ISC)2;

Will the Crown accept Qualiware Life Cycle Manager 2018 and DND Architecture Framework Certification 2018 as they are both equivalent to CISSP/ISSAP?

v. CISSP / ISSMP from (ISC)2;
vi. CISM from ISACA;
vii. CBCP from DRI;

Will the Crown accept Certificate of Cloud Security Knowledge (CCSK) version 4 2018 and ITIL Foundation Version 3 2011 as they are both equivalent to CBCP from DRI?

viii. CPP from ASIS;
ix. GIAC / Any Silver audit certification;
x. GIAC / Any Gold audit certification;
xi. C/CISO; or
xii. CRISC.

Answer 1

Yes to each.

Question 2

Table 3, Mandatory Criteria: Corporate Experience M1

Would the Crown accept three (3) project descriptions rather than four (4) project descriptions?

Answer 2

Yes.

Question 3

Table 3 – Mandatory Criteria: Corporate Experience – M1 i. states "*Include a minimum of three of the following resource categories: a TRA and C&A Analyst, an IT Security Design Specialist, an IT Security Methodology, Policy, and Procedures Analyst, an IT Security Vulnerability Assessment Specialist, **and** a Computer Forensics Specialist;*"

Can the Crown please change the wording to read "*Include a minimum of three of the following resource categories: a TRA and C&A Analyst, an IT Security Design Specialist, an IT Security Methodology, Policy, and Procedures Analyst, an IT Security Vulnerability Assessment Specialist, **and/or** a Computer Forensics Specialist;*"

Answer 3

Yes.

Question 4

Table 11 Point Rated Evaluation Criteria – R3 states "*The Bidder should demonstrate, using up to five project descriptions, that the corporation has experience in providing IT Security resources (with a minimum of three of the following resource categories on the team of resources provided by the Bidder: TRA and C&A Analyst, IT Security Design Specialist, IT Security Methodology, Policy, and Procedures Analyst, IT Security Vulnerability Assessment Specialist, **and** Computer Forensics Specialist) to complete the technical implementation of the following centrally managed, enterprise security solutions:*"

NOTE:
IT Security resources team = a minimum of three of the following resource categories on the team: TRA and C&A Analyst, IT Security Design Specialist, IT Security Methodology, Policy, and Procedures Analyst, IT Security Vulnerability Assessment Specialist, **and Computer Forensics Specialist.*

Can the Crown please change the wording to read "*The Bidder should demonstrate, using up to five project descriptions, that the corporation has experience in providing IT Security resources (with a minimum of three of the following resource categories on the team of resources provided by the Bidder: TRA and C&A Analyst, IT Security Design Specialist, IT Security Methodology, Policy, and Procedures Analyst, IT Security Vulnerability Assessment Specialist, **and/or** Computer Forensics Specialist) to complete the technical implementation of the following centrally managed, enterprise security solutions:*"

NOTE:
IT Security resources team = a minimum of three of the following resource categories on the team: TRA and C&A Analyst, IT Security Design Specialist, IT Security Methodology, Policy, and Procedures Analyst, IT Security Vulnerability Assessment Specialist, **and/or Computer Forensics Specialist*

Answer 4

Yes.

Question 5

Table 11 Point Rated Evaluation Criteria – R4 states "*NOTE: *IT Security resources team = a minimum of three of the following resource categories on the team: TRA and C&A Analyst, IT Security Design Specialist, IT Security Methodology, Policy, and Procedures Analyst, IT Security Vulnerability Assessment Specialist, **and** Computer Forensics Specialist*"

Can the Crown please change the wording to read *NOTE: *IT Security resources team = a minimum of three of the following resource categories on the team: TRA and C&A Analyst, IT Security Design Specialist, IT Security Methodology, Policy, and Procedures Analyst, IT Security Vulnerability Assessment Specialist, **and/or** Computer Forensics Specialist*"

Answer 5

Yes.

Question 6

Table 16 Point Rated Evaluation Criteria – R1 states "*The bidder should demonstrate, using project descriptions for five projects, the proposed resource has experience preparing Departmental IT Security Methodology, Policy and Procedures including:*
i. IT Security Policies, Directives, Standards, or Guidelines
ii. IT Security frameworks
iii. IT Security Standard Operating Procedures
iv. IT Security Configuration Standards
v. IT Security Risk Management Procedures
vi. IT Security Risk Management related Templates"

Can the Crown please change the wording to read "T*he bidder should demonstrate, using project descriptions for five projects, the proposed resource has experience preparing Departmental IT Security Methodology, Policy and Procedures including:*
i. IT Security Policies, Directives, Standards, or Guidelines
ii. IT Security frameworks
iii. IT Security Standard Operating Procedures
iv. IT Security Configuration Standards
*v. IT Security Risk Management Procedures **or***
vi. IT Security Risk Management related Templates"

Answer 6

Yes.

Question 7

Table 17 Point Rated Evaluation Criteria R3 – reads: "*The Bidder should demonstrate, using project descriptions for four projects, thatthe proposed resource has experience performing on-site assessments of threats, penetrations and technical vulnerabilities to networks as follows:*
i. The assessment was of threats to networks
ii. The assessment was of penetrations to networks
iii. The assessment was of technical vulnerabilities to networks
iv. The assessment was for a Large Organization*"

Can the Crown please change the wording to read "*The Bidder should demonstrate, using project descriptions for four projects, that the proposed resource has experience performing on-site assessments of threats, penetrations and technical vulnerabilities to networks as follows:*
i. The assessment was of threats to networks
ii. The assessment was of penetrations to networks
iii. The assessment was of technical vulnerabilities to networks __or__
iv. The assessment was for a Large Organization*"

Answer 7

Yes.

Question 8

Table 18 Point Rated Evaluation Criteria R2 reads "*The Bidder should demonstrate, using project descriptions for five projects, that the proposed resource has experience conducting forensic analyses of digital evidence for:*
i. Digital evidence obtained from Windows environments
ii. Digital Evidence obtained from Linux or Unix or Macintosh environments

Can the Crown please change the wording to read "*The Bidder should demonstrate, using project descriptions for five projects, that the proposed resource has experience conducting forensic analyses of digital evidence for:*
i. Digital evidence obtained from Windows environments __or__
ii. Digital Evidence obtained from Linux or Unix or Macintosh environments"

Answer 8

Yes.

Question 9

Table 18 Point Rated Evaluation Criteria R3 reads "*The Bidder should demonstrate, using project descriptions for four projects, that the proposed resource has experience in the development of:*
i. Security Standard Operating Procedures (SOPs)
ii. IT Security Guidelines

Can the Crown please change the wording to read "*The Bidder should demonstrate, using project descriptions for four projects, that the proposed resource has experience in the development of:*
i. Security Standard Operating Procedures (SOPs) *or*
ii. IT Security Guidelines

Answer 9

Yes.

Question 10

Can the Crown please confirm that the same client on the same project can be used **multiple times** to demonstrate a requirement as different tasks were performed during the contract?

Answer 10

Yes.

Question 11

Rated criterion R9 for the IT Security Design Specialist requires the bidder's resource to demonstrate 3 qualifications for full points. Would DFO consider adding the following certifications as they are also relevant to the category?

1. Certified Information Systems Auditor (CISA)
2. Common Criteria EAL4 evaluator from the Communications Security Establishment

Answer 11

Yes.

Question 12

With respect to Attachment 1 to Part 4 – Bid Evaluation Criteria, DFO has indicated that bidders are required to provide complete contact information for each project used to demonstrate experience. DFO has also indicated that bidders are required to provide two client references using Table 2 for all resources in M2. Most client references beyond five (5) years will likely not be in the same role, department or retired which makes it very challenging. Can DFO please confirm our understanding that

bidders simply need to provide two client references in M2 for all resources and do not to provide client references for every cited project as this can prove to be an onerous exercise?

Answer 12

Yes.

Question 13

Reference R6 for both TRA and C&A Analyst Level 3- pg 71 and Bilingual TRA and C&A Analyst Level 3 (pg 76).

Since DFO maintains various online payments systems such as the National Online Licensing System or the system to purchase a Salmon Conservation Catch card online, would the Crown consider including PCI-QSA certification to the list of professional qualifications required in R6 for both TRA and C&A Analyst Level 3- pg 71 and Bilingual TRA and C&A Analyst Level 3 (pg 76)?

Answer 13

Yes.

Question 14

Reference R6 for both TRA and C&A Analyst Level 3- pg 71 and Bilingual TRA and C&A Analyst Level 3 (pg 76).

Since ISO 27001 covers all types of organizations including government departments and specifies the requirements for both establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organizations overall business risks as well as the implementation of security controls customized to the needs of individuals organizations of parts thereof, would the Crown include ISO27001 Lead implementer to the list of professional qualification for the Bilingual TRA resource?

Answer 14

Yes.

Question 15

Reference R9 for IT Security Design Specialist, Level 3, resource 1 and 2- (pgs 81 and 86).

Since the Certified Information Systems Auditor (CISA) certification is a globally recognized certification for Information Security audit control, assurance and security professionals, would the Crown consider including the Certified Information Systems Auditor (CISA) to the list of certifications for required in R6 for both IT Security Design Specialists, Level 3, resource 1 and 2- (pgs 81 and 86).?

Answer 15

Yes.

Question 16

Reference R9 for IT Security Design Specialist, Level 3, resource 1 and 2- (pgs 81 and 86).

Would the Crown consider including a University level Master's Degree in Information Security to the current list of professional qualifications for IT Security Design Specialist, Level 3, resource 1 and 2- (pgs 81 and 86). ?

Answer 16

Yes.

Question 17

Reference R1 for Corporate Rated Criteria.

Can the crown clarify the relevancy of the paragraph relating to TRA? ("conducting TRA specific tasks for a minimum of one (1) month, also acceptable if the project take 20 days level of effort; therefore a 12 month project could be equivalent to 12 projects.") We do not believe TRA length of experience is specifically related to Corporate Rated R1 and was inadvertently included. Please confirm.

Answer 17

We don't do TRA's anymore so yes, the length of experience should not have been included.

Question 18

Page 12 point iv. For Previous Similar Projects: Where the bid must include a description of previous similar projects: (i) a project must have been completed by the Bidder itself (and cannot include the experience of any proposed subcontractor or any affiliate of the Bidder); (ii) a project must have been completed by the bid closing date;
Typically companies that focus on remediation and security assessments outsource digital forensics audit. Will Canada accept a subcontractor/resource reference and project experience for Digital Forensics.

Answer 18

Yes.

Question 19

Will Canada accept a bid for role in C.3-C.11 only?

Answer 19

Yes.

Question 20

Table 2: Proposed Resource Client Reference Template
1) Based from our experience, our clients in Digital Forensics do not want to be referenced for privacy reasons. Will Canada accept a detailed project description that provide insights into the engagements instead of client contact information?

Answer 20

Yes.

Question 21

Reference Table 3, Mandatory Corporate Criteria M1 (page 55) and Table 11, R3 and R4 (pages 65-67) of the RFP: These criteria require 4 or 5 projects where 3 of the RFP listed resource categories worked on each project. We have noticed that many projects where a team was provided include only 2 of the resource categories listed and not 3 of the list. Clients usually request resources based on what categories are available under the vendor contracts that they have access to at any given time. Given this, can you please amend M1, R3 and R4 to require that each project include 2 instead of 3 of the RFP listed categories?

Answer 21

No, it needs to be 3.

Question 22

Reference Table 3, Mandatory Corporate Criteria M1 (page 55) and Table 11, R3 and R4 (pages 65-67) of the RFP: Can you please confirm that bidders can present projects with similar categories as the RFP categories, as long as 50% of the task performed by the resource is the same or similar to the RFP category tasks?

Answer 21

No, 50% is not enough.

Question 22

For all Corporate Mandatory and Rated Criteria: Please note that many CPSA long-term contracts are still ongoing today or have been ongoing within the past 5 years. The CPSA categories were simply transferred to TBIPS and include the original CPSA tasks and responsibilities. Can you please confirm that projects conducted under CPSA contracts that included the same categories of resource are compliant and can be presented in response to all mandatory and rated corporate criteria?

Answer 22

Yes.

Question 23

Can you please confirm that bidders can present the same projects under different Corporate Criteria as applicable?

Answer 23

Yes.

Question 24

Corporate Rated Criteria R1, requests 5 projects where a team was provided. There is no definition of the team so we assume that a team is 2 or more IT Security resources regardless of categories. Can you please confirm?

Answer 24

Yes.

Question 25

Can the crown confirm what percentage and/or amount of days, each of the 7 resources requires to be onsite? Will this remain consistent over the course of the option periods?

Answer 25

Yes.