



**RETURN BIDS TO:  
RETOURNER LES SOUMISSIONS À:**

**Bid Receiving - PWGSC / Réception des  
soumissions - TPSGC**

**11 Laurier St., / 11, rue Laurier**

**Place du Portage, Phase III**

**Core 0B2 / Noyau 0B2**

**Gatineau**

**Québec**

**K1A 0S5**

**Bid Fax: (819) 997-9776**

**REQUEST FOR PROPOSAL  
DEMANDE DE PROPOSITION**

**Proposal To: Public Works and Government  
Services Canada**

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

**Proposition aux: Travaux Publics et Services  
Gouvernementaux Canada**

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

**Comments - Commentaires**

**Vendor/Firm Name and Address**

**Raison sociale et adresse du**

**fournisseur/de l'entrepreneur**

**Issuing Office - Bureau de distribution**

Informatics Professional Services - EL Division/Services  
professionnels en informatique - division EL

Terrasses de la Chaudière 4th Floor

10 Wellington Street

Gatineau

Québec

K1A 0S5

<b>Title - Sujet</b> Cyber Security program	
<b>Solicitation No. - N° de l'invitation</b> 24062-190077/B	<b>Date</b> 2019-05-21
<b>Client Reference No. - N° de référence du client</b> 24062-190077	
<b>GETS Reference No. - N° de référence de SEAG</b> PW-\$\$EL-638-35684	
<b>File No. - N° de dossier</b> 638el.24062-190077	<b>CCC No./N° CCC - FMS No./N° VME</b>
<b>Solicitation Closes - L'invitation prend fin</b> <b>at - à 02:00 PM</b> <b>on - le 2019-06-11</b>	<b>Time Zone</b> <b>Fuseau horaire</b> Eastern Daylight Saving Time EDT
<b>F.O.B. - F.A.B.</b> <b>Plant-Usine:</b> <input type="checkbox"/> <b>Destination:</b> <input checked="" type="checkbox"/> <b>Other-Autre:</b> <input type="checkbox"/>	
<b>Address Enquiries to: - Adresser toutes questions à:</b> Mao, Lan	<b>Buyer Id - Id de l'acheteur</b> 638el
<b>Telephone No. - N° de téléphone</b> (613) 858-9980 ( )	<b>FAX No. - N° de FAX</b> ( ) -
<b>Destination - of Goods, Services, and Construction:</b> <b>Destination - des biens, services et construction:</b>  Specified Herein Précisé dans les présentes	

**Instructions: See Herein**

**Instructions: Voir aux présentes**

<b>Delivery Required - Livraison exigée</b> See Herein	<b>Delivery Offered - Livraison proposée</b>
<b>Vendor/Firm Name and Address</b> <b>Raison sociale et adresse du fournisseur/de l'entrepreneur</b>	
<b>Telephone No. - N° de téléphone</b> <b>Facsimile No. - N° de télécopieur</b>	
<b>Name and title of person authorized to sign on behalf of Vendor/Firm</b> <b>(type or print)</b> <b>Nom et titre de la personne autorisée à signer au nom du fournisseur/</b> <b>de l'entrepreneur (taper ou écrire en caractères d'imprimerie)</b>	
<b>Signature</b>	<b>Date</b>

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

## **BID SOLICITATION**

### **FOR CONTRACTS AGAINST A SUPPLY ARRANGEMENT FOR TASK- BASED INFORMATICS PROFESSIONAL SERVICES (TBIPS)**

### **VARIOUS INFORMATICS PROFESSIONAL SERVICES CATEGORIES (SEE HEREIN)**

### **FOR TREASURY BOARD OF CANADA SECRETARIAT**

## Table of Contents

PART 1 - GENERAL INFORMATION.....	5
1.1 Introduction.....	5
1.2 Summary .....	5
1.3 Debriefings .....	7
PART 2 - BIDDER INSTRUCTIONS.....	8
2.1 Standard Instructions, Clauses and Conditions .....	8
2.2 Submission of Bids.....	10
2.3 Enquiries - Bid Solicitation .....	10
2.4 Former Public Servant.....	10
2.5 Applicable Laws.....	12
2.6 Basis for Canada's Ownership of Intellectual Property .....	12
2.7 Volumetric Data .....	12
PART 3 - BID PREPARATION INSTRUCTIONS.....	13
3.1 Bid Preparation Instructions.....	13
3.2 Section I: Technical Bid.....	15
3.3 Section II: Financial Bid.....	16
3.4 Section III: Certifications.....	17
PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION.....	18
4.1 Evaluation Procedures .....	18
4.2 Technical Evaluation.....	21
4.3 Financial Evaluation.....	22
4.4 Basis of Selection.....	28
PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION .....	30
5.1 Certifications Precedent to Contract Award and Additional Information.....	30
PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS.....	31
6.1 Security Requirement.....	31

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

6.2	Financial Capability .....	31
PART 7 - RESULTING CONTRACT CLAUSES .....		32
7.1	Requirement.....	32
7.2	Task Authorization .....	32
7.3	Minimum Work Guarantee .....	35
7.4	Standard Clauses and Conditions .....	36
7.5	Security Requirement .....	37
7.6	Contract Period.....	37
7.7	Authorities.....	37
7.8	Proactive Disclosure of Contracts with Former Public Servants.....	38
7.9	Payment.....	38
7.10	Invoicing Instructions .....	40
7.11	Certifications and Additional Information .....	41
7.12	Federal Contractors Program for Employment Equity - Default by Contractor .....	41
7.13	Applicable Laws.....	41
7.14	Priority of Documents .....	41
7.15	Foreign Nationals (Canadian Contractor).....	42
7.16	Foreign Nationals (Foreign Contractor) .....	42
7.17	Insurance Requirements .....	42
7.18	Limitation of Liability - Information Management/Information Technology .....	44
7.19	Joint Venture Contractor .....	45
7.20	Professional Services - General .....	46
7.21	Safeguarding Electronic Media .....	47
7.22	Representations and Warranties .....	47
7.23	Access to Canada's Property and Facilities.....	47
7.24	Identification Protocol Responsibilities.....	47

---

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

**List of Annexes to the Resulting Contract:**

Annex A Statement of Work

- Appendix A to Annex A - Tasking Assessment Procedure;
- Appendix B to Annex A - Task Authorization (TA) Form;
- Appendix C to Annex A - Resource Assessment Criteria and Response Table;
- Appendix D to Annex A - Certifications at the TA stage;

Annex B Basis of Payment

Annex C Security Requirements Check List

**List of Attachment to Part 3 (Bid Preparation Instructions):**

- Attachment 3.1: Bid Submission Form
- Attachment 3.2: Pricing Schedule

**List of Attachment to Part 4 (Evaluation Procedures and Basis of Selection):**

- Attachment 4.1: Mandatory Evaluation Criteria
- Attachment 4.2: Rated Evaluation Criteria
- Attachment 4.3: Bidder Response Templates

**List of Attachment to Part 5 (Certifications):**

- Attachment 5.1: FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY - CERTIFICATION

---

## **PART 1 - GENERAL INFORMATION**

### **1.1 Introduction**

This document states terms and conditions that apply to this bid solicitation. It is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, if applicable, and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The annexes include the Statement of Work and any other annexes.

### **1.2 Summary**

- (a) This bid solicitation cancels and supersedes previous bid solicitation number 24062-190077/A dated 2019/02/08 with a closing date of 2019/02/28 at 14:00 Eastern Standard Time (EST).
- (b) This bid solicitation is being issued to satisfy the requirement of Treasury Board of Canada Secretariat (the "Client") for Task-Based Informatics Professional Services (TBIPS) under the TBIPS Supply Arrangement (SA) method of supply.
- (c) It is intended to result in the award of up to two contracts in each of the two Workstreams, with each contract purchasing Work from only one Workstream. Each contract will be for three years plus two one-year irrevocable options allowing Canada to extend the term of the contract. Bidders do not have to submit a bid for each Workstream. In the event that a Bidder wants to bid on more than one Workstream, a separate technical bid should be submitted for each Workstream if the Bidder chooses to submit its bid in hard copies.
- (d) There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 – Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (<http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html>) website.
- (e) The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-Chile Free Trade Agreement (CCFTA), the Canada-Peru Free Trade Agreement (CPFTA), the Canada-Colombia Free Trade Agreement (CCoLFTA), the Canada-Panama Free Trade Agreement (CPanFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), and the Canadian Free Trade Agreement (CFTA).

- (f) The Federal Contractor's Program (FCP) for employment equity applies to this procurement; see Part 5 – Certifications and Additional Information, Part 7 – Resulting Contract Clauses and the attachment titled "Federal Contractors Program for Employment Equity – Certification."
- (g) This bid solicitation allows bidders to use the epost Connect service provided by Canada Post Corporation to transmit their bid electronically. Bidders must refer to Part 2 entitled "Bidder Instructions, and Part 3 entitled "Bid Preparation Instructions", of the bid solicitation, for further information
- (h) Only TBIPS SA Holders currently holding a TBIPS SA for Tier 2, in all resource categories of a given Workstream and in the National Capital Region under the EN578-170432 series of SAs are eligible to compete. The TBIPS SA EN578-170432 is incorporated by reference and forms part of this bid solicitation, as though expressly set out in it, subject to any express terms and conditions contained in this bid solicitation. The capitalized terms not defined in this bid solicitation have the meaning given to them in the TBIPS SA.
- (i) SA Holders that are invited to compete as a joint venture must submit a bid as that joint venture SA Holder, forming no other joint venture to bid. Any joint venture must be already qualified under the SA #EN578-170432 as that joint venture at the time of bid closing in order to submit a bid.
- (j) For each Workstream, the Resource Categories described below are required on an as and when requested basis in accordance with the TBIPS SA Annex "A":

**WORKSTREAM 1**

RESOURCE CATEGORY	LEVEL OF EXPERTISE	ESTIMATED NUMBER OF RESOURCES REQUIRED
C.2 IT Security Methodology, Policy and Procedures Analyst	LEVEL 3	1
C.3 IT Security TRA and C&A Analyst	LEVEL 3	1
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	2
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	LEVEL 3	3
P.12 Risk Management Specialist	LEVEL 3	1
B.1 Business Analyst	LEVEL 3	1
B.14 Technical Writer	LEVEL 3	1

---

**WORKSTREAM 2**

RESOURCE CATEGORY	LEVEL OF EXPERTISE	ESTIMATED NUMBER OF RESOURCES REQUIRED
C.3 IT Security TRA and C&A Analyst	LEVEL 3	1
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	1
C.11 IT Security VA Specialist	LEVEL 3	2
C.16 PIA Specialist	LEVEL 3	2
P.9 Project Manager	LEVEL 3	1
B.1 Business Analyst	LEVEL 3	1
A.7 Programmer/Analyst	LEVEL 3	1

**1.3 Debriefings**

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be provided in writing, by telephone or in person.

---

## PART 2 - BIDDER INSTRUCTIONS

### 2.1 Standard Instructions, Clauses and Conditions

- (a) All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the *Standard Acquisition Clauses and Conditions Manual* (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Works and Government Services Canada.
- (b) Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract(s).
- (c) The 2003 (2018-05-22) Standard Instructions - Goods or Services - Competitive Requirements are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003 and this document, this document prevails.
- (d) Subsection 3.a. of Section 01, Integrity provisions - bid of Standard Instructions 2003 incorporated by reference above is deleted in its entirety and replaced with the following:
  - a. at the time of submitting an arrangement under the Request for Supply Arrangement (RFSA), the Bidder has already provided a list of names, as requested under the *Ineligibility and Suspension Policy*. During this procurement process, the Bidder must immediately inform Canada in writing of any changes affecting the list of names.
- (e) Subsection 4 of Section 05, Submission of bids of Standard Instructions 2003 incorporated by reference above, is amended as follows:

Delete: 60 days

Insert: 180 days
- (f) Subsection 1 of Section 08, Transmission by facsimile or by epost Connect of Standard Instructions 2003 incorporated by reference above, is deleted and replaced by the following:
  - 1. Facsimile
  - Due to the nature of the bid solicitation, bids transmitted by facsimile or electronic mail to PWGSC will not be accepted.
- (g) Subsection 2 of Section 08, Transmission by facsimile or by epost Connect of Standard Instructions 2003 incorporated by reference above, is deleted and replaced by the following:
  - 2. epost Connect
    - a. Unless specified otherwise in the bid solicitation, bids may be submitted by using the [epost Connect service](#) provided by Canada Post Corporation.
      - i. PWGSC, National Capital Region: The only acceptable email address to use with epost Connect for responses to bid solicitations issued by PWGSC headquarters is:  
  
[tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca](mailto:tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca)  
  
or, if applicable, the email address identified in the bid solicitation.
      - ii. PWGSC regional offices: The only acceptable email address to use with epost Connect for responses to bid solicitations issued by PWGSC regional offices is identified in the bid solicitation.
    - b. To submit a bid using epost Connect service, the Bidder must either:

- 
- i. send directly its bid only to the specified PWGSC Bid Receiving Unit, using its own licensing agreement for epost Connect provided by Canada Post Corporation; or
  - ii. send as early as possible, and in any case, at least six business days prior to the solicitation closing date and time, (in order to ensure a response), an email that includes the bid solicitation number to the specified PWGSC Bid Receiving Unit requesting to open an epost Connect conversation. Requests to open an epost Connect conversation received after that time may not be answered.
  - c. If the Bidder sends an email requesting epost Connect service to the specified Bid Receiving Unit in the bid solicitation, an officer of the Bid Receiving Unit will then initiate an epost Connect conversation. The epost Connect conversation will create an email notification from Canada Post Corporation prompting the Bidder to access and action the message within the conversation. The Bidder will then be able to transmit its bid afterward at any time prior to the solicitation closing date and time.
  - d. If the Bidder is using its own licensing agreement to send its bid, the Bidder must keep the epost Connect conversation open until at least 30 business days after the solicitation closing date and time.
  - e. The bid solicitation number should be identified in the epost Connect message field of all electronic transfers.
  - f. It should be noted that the use of epost Connect service requires a Canadian mailing address. Should a bidder not have a Canadian mailing address, they may use the Bid Receiving Unit address specified in the solicitation in order to register for the epost Connect service.
  - g. For bids transmitted by epost Connect service, Canada will not be responsible for any failure attributable to the transmission or receipt of the bid including, but not limited to, the following:
    - i. receipt of a garbled, corrupted or incomplete bid;
    - ii. availability or condition of the epost Connect service;
    - iii. incompatibility between the sending and receiving equipment;
    - iv. delay in transmission or receipt of the bid;
    - v. failure of the Bidder to properly identify the bid;
    - vi. illegibility of the bid;
    - vii. security of bid data; or,
    - viii. inability to create an electronic conversation through the epost Connect service.
  - h. The Bid Receiving Unit will send an acknowledgement of the receipt of bid document(s) via the epost Connect conversation, regardless of whether the conversation was initiated by the supplier using its own license or the Bid Receiving Unit. This acknowledgement will confirm only the receipt of bid document(s) and will not confirm if the attachments may be opened nor if the content is readable.
  - i. Bidders must ensure that they are using the correct email address for the Bid Receiving Unit when initiating a conversation in epost Connect or communicating with the Bid Receiving Unit and should not rely on the accuracy of copying and pasting the email address into the epost Connect system.
-

- 
- j. A bid transmitted by epost Connect service constitutes the formal bid of the Bidder and must be submitted in accordance with section 05.

## 2.2 Submission of Bids

- (a) Bids must be submitted only to the Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and at the PWGSC address indicated on page one of the bid solicitation.

**Note:** For bidders choosing to submit using epost Connect for bids closing at the Bid Receiving Unit in the National Capital Region (NCR) the email address is:

[tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca](mailto:tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca)

**Note:** Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

- (b) Due to the nature of the bid solicitation, bids transmitted by facsimile or electronic mail to PWGSC will not be accepted.

## 2.3 Enquiries - Bid Solicitation

- (a) All enquiries must be submitted in writing to the Contracting Authority no later than 5 calendar days before the bid closing date. Enquiries received after that time may not be answered.
- (b) Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered with copies to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

## 2.4 Former Public Servant

- (a) Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, Bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

(b) **Definitions**

For the purposes of this clause, "*former public servant*" is any former member of a department as defined in the [Financial Administration Act](#), R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

- (i) an individual;

- 
- (ii) an individual who has incorporated;
  - (iii) a partnership made of former public servants; or
  - (iv) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"*lump sum payment period*" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"*pension*" means a pension or annual allowance paid under the [Public Service Superannuation Act](#) (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the [Supplementary Retirement Benefits Act](#), R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the [Canadian Forces Superannuation Act](#), R.S., 1985, c. C-17, the [Defence Services Pension Continuation Act](#), 1970, c. D-3, the [Royal Canadian Mounted Police Pension Continuation Act](#), 1970, c. R-10, and the [Royal Canadian Mounted Police Superannuation Act](#), R.S., 1985, c. R-11, the [Members of Parliament Retiring Allowances Act](#), R.S. 1985, c. M-5, and that portion of pension payable to the [Canada Pension Plan Act](#), R.S., 1985, c. C-8.

(c) **Former Public Servant in Receipt of a Pension**

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes ( ) No ( )**

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

- (i) name of former public servant;
- (ii) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with [Contracting Policy Notice: 2012-2](#) and the [Guidelines on the Proactive Disclosure of Contracts](#).

(d) **Work Force Adjustment Directive**

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes ( ) No ( )**

If so, the Bidder must provide the following information:

- (i) name of former public servant;
- (ii) conditions of the lump sum payment incentive;
- (iii) date of termination of employment;
- (iv) amount of lump sum payment;
- (v) rate of pay on which lump sum payment is based;

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

- 
- (vi) period of lump sum payment including start date, end date and number of weeks;
- (vii) number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is \$5,000, including Applicable Taxes.

## 2.5 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

**Note to Bidders:** Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of its bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of its choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidder. Bidders are requested to indicate the Canadian province or territory they wish to apply to any resulting contract in their Bid Submission Form.

## 2.6 Basis for Canada's Ownership of Intellectual Property

The Treasury Board of Canada Secretariat has determined that any intellectual property rights arising from the performance of the Work under any resulting contract will belong to Canada, on the following grounds:

- national security

## 2.7 Volumetric Data

The estimated number of resources required per resource category has been provided to Bidders to assist them in preparing their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of the service identified in this bid solicitation will be consistent with this data. It is provided purely for information purposes.

---

## PART 3 - BID PREPARATION INSTRUCTIONS

### 3.1 Bid Preparation Instructions

#### (a) Epost Connect Bid Submission

- (i) If the Bidder chooses to submit its bid electronically, Canada requests that the Bidder submits its bid in accordance with section 08 of the 2003 Standard Instructions. The epost Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation.
- (ii) The bid must be gathered per section and separated as follows:
  - (A) Section I: Technical Bid
  - (B) Section II: Financial Bid
  - (C) Section III: Certifications
- (iii) For further information please refer to article 08 - Transmission by facsimile or by epost Connect at <https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual/1/2003/23#transmission-by-facsimile>.

#### (b) Soft Copy Bid Submission (USB key)

- (i) If the Bidder chooses to submit its bid in soft copy via the PWGSC Bid Receiving Unit, Canada requests that the Bidder submits its bid in separate sections as follows:
  - (A) Section I: Technical Bid – One soft copy on a USB key
  - (B) Section II: Financial Bid – One soft copy on a USB key
  - (C) Section III: Certifications – One soft copy on a USB key
- (c) If the Bidder is simultaneously providing an epost Connect copy and soft copy of the bid and if there is a discrepancy between the wording of the epost Connect copy and soft copy, the wording of the epost Connect copy will have priority over the wording of the soft copy.
- (d) Canada is not requesting a hard copy of the bid. However, if the Bidder submits a hard copy of its bid, and if there is a discrepancy between the wording of the soft or epost Connect copy and the hard copy, the wording of the soft or epost Connect copy will have priority over the wording of the hard copy.
- (e) Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.
- (f) **Format for Bid:** Canada requests that Bidders follow the format instructions described below in the preparation of their bid:
  - (i) use 8.5 x 11 inch (216 mm x 279 mm) page size;
  - (ii) use a numbering system that corresponds to the bid solicitation;
  - (iii) include a title page at the front of each volume of the bid that includes the title, date, bid solicitation number, bidder's name and address and contact information of its representative; and
  - (iv) include a table of contents.
- (g) **Canada's Policy on Green Procurement:** In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process. See the Policy on Green Procurement

---

(<http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html>). To assist Canada in reaching its objectives, Bidders should:

- (i) use paper containing fibre certified as originating from a sustainably-managed forest and/or containing a minimum of 30% recycled content; and
- (ii) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, and using staples or clips instead of cerlox, duotangs or binders.

(h) **Submission of Only One Bid:**

- (i) A Bidder, including related entities, will be permitted to submit only one bid in response to this bid solicitation. If a Bidder or any related entities participate in more than one bid (participating means being part of the Bidder, not being a subcontractor), Canada will provide those Bidders with 2 working days to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all the affected bids being disqualified. A single bid may contain bids to be awarded a contract in one or more Workstreams. However, a bid may not contain a bid from the Bidder, including related entities to be awarded more than one contract in any given Workstream.
- (ii) For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity is a natural person, corporation, partnership, etc), an entity will be considered to be "**related**" to a Bidder if:
  - (A) they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);
  - (B) they are "related persons" or "affiliated persons" according to the Canada Income Tax Act;
  - (C) the entities have now or in the two years before bid closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or
  - (D) the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.
- (iii) Individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture. .

(i) **Joint Venture Experience:**

- (i) Where the Bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and O. A bid solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and O), the bidder has previously done the work. This bidder can use this experience to meet the requirement. If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding.

- (ii) A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this bid solicitation.

Example: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder have 3 years of experience providing maintenance service,

---

and (b) that the bidder have 2 years of experience integrating hardware with complex networks, then each of these two requirements can be met by a different member of the joint venture. However, for a single criterion, such as the requirement for 3 years of experience providing maintenance services, the bidder cannot indicate that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive.

- (iii) Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this bid solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a criterion is required, the Bidder is requested to indicate which joint venture member satisfies the requirement. If the Bidder has not identified which joint venture member satisfies the requirement, the Contracting Authority will provide an opportunity to the Bidder to submit this information during the evaluation period. If the Bidder does not submit this information within the period set by the Contracting Authority, its bid will be declared non-responsive.

Example: A bidder is a joint venture consisting of members A and B. If a bid solicitation requires that the bidder demonstrate experience providing resources for a minimum number of 100 billable days, the bidder may demonstrate that experience by submitting either:

- Contracts all signed by A;
- Contracts all signed by B; or
- Contracts all signed by A and B in joint venture, or
- Contracts signed by A and contracts signed by A and B in joint venture, or
- Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days.

- (iv) Any Bidder with questions regarding the way in which a joint venture bid will be evaluated should raise such questions through the Enquiries process as early as possible during the bid solicitation period.

### 3.2 Section I: Technical Bid

- (a) The technical bid consists of the following:

- (i) **Bid Submission Form:** Bidders are requested to include the Bid Submission Form - Attachment 3.1 with their bids. It provides a common form in which bidders can provide information required for evaluation and contract award, such as a contact name and the Bidder's Procurement Business Number, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.
- (ii) **Substantiation of Technical Compliance:**
- (A) **Mandatory Technical Criteria:** The technical bid must substantiate the compliance with the specific articles of Attachment 4.1, which is the requested format for providing the substantiation. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder or its proposed solution or resources comply is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be considered non-responsive and disqualified. The substantiation may refer to

---

additional documentation submitted with the bid - this information can be referenced in the "Bidder's Response" column of Attachment 4.1, where Bidders are requested to indicate where in the bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

- (B) **Point-Rated Technical Criteria:** The technical bid must substantiate the compliance with the specific articles of Attachment 4.2, which is the requested format for providing the substantiation. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder or its proposed solution or resources comply is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be rated accordingly. The substantiation may refer to additional documentation submitted with the bid - this information can be referenced in the "Bidder's Response" column of Attachment 4.2, where Bidders are requested to indicate where in the bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

(iii) **Customer Reference Contact Information:**

- (A) The Bidder must provide customer references. The customer reference must each confirm, if requested by PWGSC, the facts identified in the Bidder's bid, as required by Attachment 4.1 and Attachment 4.2.
- (B) The form of question to be used to request confirmation from customer references is as follows:

[Sample Question to Customer Reference: "Has [the Bidder] provided your organization with [describe the services and, if applicable, describe any required time frame within which those services must have been provided]?"

☐ Yes, the Bidder has provided my organization with the services described above.

☐ No, the Bidder has not provided my organization with the services described above.

☐ I am unwilling or unable to provide any information about the services described above.

- (C) For each customer reference, the Bidder must, at a minimum, provide the name and either the telephone number or e-mail address for a contact person. If only the telephone number is provided, it will be used to call to request the e-mail address and the reference check will be done by e-mail.

Bidders are also requested to include the title of the contact person. It is the sole responsibility of the Bidder to ensure that it provides a contact who is knowledgeable about the services the Bidder has provided to its customer and who is willing to act as a customer reference. Crown references will be accepted.

### 3.3 Section II: Financial Bid

- (a) **Pricing:** Bidders must submit their financial bid in accordance with the Pricing Schedule provided in Attachment 3.2. The total amount of Applicable Taxes must be shown separately, if applicable.

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

Unless otherwise indicated, bidders must include a single, firm, all-inclusive per diem rate quoted in Canadian dollars in each cell requiring an entry in the pricing tables.

- (b) **All Costs to be Included:** The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option periods. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.
- (c) **Blank Prices:** Bidders are requested to insert "\$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "\$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, \$0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is \$0.00 will be declared non-responsive.

### 3.4 Section III: Certifications

It is a requirement that bidders submit the certifications and additional information identified under Part 5.

---

## PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

### 4.1 Evaluation Procedures

- (a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria. There are several steps in the evaluation process, which are described below. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.
- (b) An evaluation team composed of representatives of the Client and PWGSC will evaluate the bids on behalf of Canada. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.
- (c) In addition to any other time periods established in the bid solicitation:
  - (i) **Requests for Clarifications:** If Canada seeks clarification or verification from the Bidder about its bid, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.
  - (ii) **Requests for Further Information:** If Canada requires additional information in order to do any of the following pursuant to the Section entitled "Conduct of Evaluation" in 2003, Standard Instructions - Goods or Services - Competitive Requirements:
    - (A) verify any or all information provided by the Bidder in its bid; or
    - (B) contact any or all references supplied by the Bidder (e.g., references named in the résumés of individual resources) to verify and validate any information submitted by the Bidder,the Bidder must provide the information requested by Canada within 2 working days of a request by the Contracting Authority.
  - (iii) **Extension of Time:** If additional time is required by the Bidder, the Contracting Authority may grant an extension in his or her sole discretion.

#### 4.1.1 Phased Bid Compliance Process

##### 4.1.1.1 General

- (a) For each Workstream, Canada will conduct the Phased Bid Compliance Process (PBCP) described below for this requirement ONLY if Canada receives 4 or fewer Bids by the bid solicitation closing date.
- (b) Notwithstanding any review by Canada at Phase I or II of the PBCP, Bidders are and will remain solely responsible for the accuracy, consistency and completeness of their Bids and Canada does not undertake, by reason of this review, any obligations or responsibility for identifying any or all errors or omissions in Bids or in responses by a Bidder to any communication from Canada.

THE BIDDER ACKNOWLEDGES THAT THE REVIEWS IN PHASE I AND II OF THIS PBCP ARE PRELIMINARY AND DO NOT PRECLUDE A FINDING IN PHASE III THAT THE BID IS NON-RESPONSIVE, EVEN FOR MANDATORY REQUIREMENTS WHICH WERE SUBJECT TO REVIEW IN PHASE I OR II AND NOTWITHSTANDING THAT THE BID HAD BEEN FOUND RESPONSIVE IN SUCH EARLIER PHASE. CANADA MAY DEEM A BID TO BE NON-RESPONSIVE TO A MANDATORY REQUIREMENT AT ANY PHASE. THE BIDDER ALSO

---

ACKNOWLEDGES THAT ITS RESPONSE TO A NOTICE OR A COMPLIANCE ASSESSMENT REPORT (CAR) (EACH DEFINED BELOW) IN PHASE I OR II MAY NOT BE SUCCESSFUL IN RENDERING ITS BID RESPONSIVE TO THE MANDATORY REQUIREMENTS THAT ARE THE SUBJECT OF THE NOTICE OR CAR, AND MAY RENDER ITS BID NON-RESPONSIVE TO OTHER MANDATORY REQUIREMENTS.

- (c) Canada may, in its discretion, request and accept at any time from a Bidder and consider as part of the Bid, any information to correct errors or deficiencies in the Bid that are clerical or administrative, such as, without limitation, failure to sign the Bid or any part or to checkmark a box in a form, or other failure of format or form or failure to acknowledge; failure to provide a procurement business number or contact information such as names, addresses and telephone numbers; inadvertent errors in numbers or calculations that do not change the amount the Bidder has specified as the price or of any component thereof that is subject to evaluation. This shall not limit Canada's right to request or accept any information after the bid solicitation closing in circumstances where the bid solicitation expressly provides for this right. The Bidder will have the time period specified in writing by Canada to provide the necessary documentation. Failure to meet this deadline will result in the Bid being declared non-responsive.
- (d) The PBCP does not limit Canada's rights under Standard Acquisition Clauses and Conditions (SACC) 2003 (2018-05-22) Standard Instructions – Goods or Services – Competitive Requirements nor Canada's right to request or accept any information during the solicitation period or after bid solicitation closing in circumstances where the bid solicitation expressly provides for this right, or in the circumstances described in subsection (c).
- (e) Canada will send any Notice or CAR by any method Canada chooses, in its absolute discretion. The Bidder must submit its response by the method stipulated in the Notice or CAR. Responses are deemed to be received by Canada at the date and time they are delivered to Canada by the method and at the address specified in the Notice or CAR. An email response permitted by the Notice or CAR is deemed received by Canada on the date and time it is received in Canada's email inbox at Canada's email address specified in the Notice or CAR. A Notice or CAR sent by Canada to the Bidder at any address provided by the Bidder in or pursuant to the Bid is deemed received by the Bidder on the date it is sent by Canada. Canada is not responsible for late receipt by Canada of a response, however caused.

#### **4.1.1.2 Phase I: Financial Bid**

- (a) After the closing date and time of this bid solicitation, Canada will examine the Bid to determine whether it includes a Financial Bid and whether any Financial Bid includes all information required by the solicitation. Canada's review in Phase I will be limited to identifying whether any information that is required under the bid solicitation to be included in the Financial Bid is missing from the Financial Bid. This review will not assess whether the Financial Bid meets any standard or is responsive to all solicitation requirements
- (b) Canada's review in Phase I will be performed by officials of the Department of Public Works and Government Services.
- (c) If Canada determines, in its absolute discretion that there is no Financial Bid or that the Financial Bid is missing all of the information required by the bid solicitation to be included in the Financial Bid, then the Bid will be considered non-responsive and will be given no further consideration.
- (d) For Bids other than those described in c), Canada will send a written notice to the Bidder ("Notice") identifying where the Financial Bid is missing information. A Bidder, whose Financial Bid has been found responsive to the requirements that are reviewed at Phase I, will not receive a Notice. Such Bidders shall not be entitled to submit any additional information in respect of their Financial Bid.

- 
- (e) The Bidders who have been sent a Notice shall have the time period specified in the Notice (the "Remedy Period") to remedy the matters identified in the Notice by providing to Canada, in writing, additional information or clarification in response to the Notice. Responses received after the end of the Remedy Period will not be considered by Canada, except in circumstances and on terms expressly provided for in the Notice.
- (f) In its response to the Notice, the Bidder will be entitled to remedy only that part of its Financial Bid which is identified in the Notice. For instance, where the Notice states that a required line item has been left blank, only the missing information may be added to the Financial Bid, except that, in those instances where the addition of such information will necessarily result in a change to other calculations previously submitted in its Financial Bid, (for example, the calculation to determine a total price), such necessary adjustments shall be identified by the Bidder and only these adjustments shall be made. All submitted information must comply with the requirements of this solicitation.
- (g) Any other changes to the Financial Bid submitted by the Bidder will be considered to be new information and will be disregarded. There will be no change permitted to any other Section of the Bidder's Bid. Information submitted in accordance with the requirements of this solicitation in response to the Notice will replace, in full, **only** that part of the original Financial Bid as is permitted above, and will be used for the remainder of the bid evaluation process.
- (h) Canada will determine whether the Financial Bid is responsive to the requirements reviewed at Phase I, considering such additional information or clarification as may have been provided by the Bidder in accordance with this Section. If the Financial Bid is not found responsive for the requirements reviewed at Phase I to the satisfaction of Canada, then the Bid shall be considered non-responsive and will receive no further consideration.
- (i) Only Bids found responsive to the requirements reviewed in Phase I to the satisfaction of Canada, will receive a Phase II review.

#### **4.1.1.3 Phase II: Technical Bid**

- (a) Canada's review at Phase II will be limited to a review of the Technical Bid to identify any instances where the Bidder has failed to meet any Eligible Mandatory Criterion. This review will not assess whether the Technical Bid meets any standard or is responsive to all solicitation requirements. Eligible Mandatory Criteria are all mandatory technical criteria that are identified in this solicitation as being subject to the PBCP. Mandatory technical criteria that are not identified in the solicitation as being subject to the PBCP, will not be evaluated until Phase III.
- (b) Canada will send a written notice to the Bidder (Compliance Assessment Report or "CAR") identifying any Eligible Mandatory Criteria that the Bid has failed to meet. A Bidder whose Bid has been found responsive to the requirements that are reviewed at Phase II will receive a CAR that states that its Bid has been found responsive to the requirements reviewed at Phase II. Such Bidder shall not be entitled to submit any response to the CAR.
- (c) A Bidder shall have the period specified in the CAR (the "Remedy Period") to remedy the failure to meet any Eligible Mandatory Criterion identified in the CAR by providing to Canada in writing additional or different information or clarification in response to the CAR. Responses received after the end of the Remedy Period will not be considered by Canada, except in circumstances and on terms expressly provided for in the CAR.
- (d) The Bidder's response must address only the Eligible Mandatory Criteria listed in the CAR as not having been achieved, and must include only such information as is necessary to achieve such compliance. Any additional information provided by the Bidder which is not necessary to achieve such compliance will not be considered by Canada, except that, in those instances where such a response to the Eligible Mandatory Criteria specified in the

---

CAR will necessarily result in a consequential change to other parts of the Bid, the Bidder shall identify such additional changes, provided that its response must not include any change to the Financial Bid.

- (e) The Bidder's response to the CAR should identify in each case the Eligible Mandatory Criterion in the CAR to which it is responding, including identifying in the corresponding section of the original Bid, the wording of the proposed change to that section, and the wording and location in the Bid of any other consequential changes that necessarily result from such change. In respect of any such consequential change, the Bidder must include a rationale explaining why such consequential change is a necessary result of the change proposed to meet the Eligible Mandatory Criterion. It is not up to Canada to revise the Bidder's Bid, and failure of the Bidder to do so in accordance with this subparagraph is at the Bidder's own risk. All submitted information must comply with the requirements of this solicitation.
- (f) Any changes to the Bid submitted by the Bidder other than as permitted in this solicitation, will be considered to be new information and will be disregarded. Information submitted in accordance with the requirements of this solicitation in response to the CAR will replace, in full, **only** that part of the original Bid as is permitted in this Section.
- (g) Additional or different information submitted during Phase II permitted by this section will be considered as included in the Bid, but will be considered by Canada in the evaluation of the Bid at Phase II only for the purpose of determining whether the Bid meets the Eligible Mandatory Criteria. It will not be used at any Phase of the evaluation to increase or decrease any score that the original Bid would achieve without the benefit of such additional or different information. For instance, an Eligible Mandatory Criterion that requires a mandatory minimum number of points to achieve compliance will be assessed at Phase II to determine whether such mandatory minimum score would be achieved with such additional or different information submitted by the Bidder in response to the CAR. If so, the Bid will be considered responsive in respect of such Eligible Mandatory Criterion, and the additional or different information submitted by the Bidder shall bind the Bidder as part of its Bid, but the Bidder's original score, which was less than the mandatory minimum for such Eligible Mandatory Criterion, will not change, and it will be that original score that is used to calculate any score for the Bid.
- (h) Canada will determine whether the Bid is responsive for the requirements reviewed at Phase II, considering such additional or different information or clarification as may have been provided by the Bidder in accordance with this Section. If the Bid is not found responsive for the requirements reviewed at Phase II to the satisfaction of Canada, then the Bid shall be considered non-responsive and will receive no further consideration.
- (i) Only Bids found responsive to the requirements reviewed in Phase II to the satisfaction of Canada, will receive a Phase III evaluation.

#### **4.1.1.4 Phase III: Final Evaluation of the Bid**

- (a) In Phase III, Canada will complete the evaluation of all Bids found responsive to the requirements reviewed at Phase II. Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria.
- (b) A Bid is non-responsive and will receive no further consideration if it does not meet all mandatory evaluation criteria of the solicitation.

## **4.2 Technical Evaluation**

A separate technical evaluation will be conducted for each Workstream.

---

(a) **Mandatory Technical Criteria:**

- (i) Each bid will be reviewed for compliance with the mandatory requirements of the bid solicitation. Any element of the bid solicitation that is identified specifically with the words "must" or "mandatory" is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.
- (ii) The mandatory technical criteria are described in Attachment 4.1.
- (iii) If the Phased Bid Compliance Process applies, it will apply to all mandatory technical criteria.

(b) **Point-Rated Technical Criteria:**

- (i) Each bid will be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word "rated" or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly.
- (ii) The rated requirements are described in Attachment 4.2.

(c) **Reference Checks:**

- (i) Whether or not to conduct reference checks is discretionary. However, if PWGSC chooses to conduct reference checks for any given rated or mandatory requirement, it will check the references for that requirement for all bidders who have not, at that point, been found non-responsive.
- (ii) For reference checks, Canada will conduct the reference check in writing by email. Canada will send all email reference check requests to contacts supplied by all the Bidders within a 48-hour period using the email address provided in the bid. Canada will not award any points and/or a bidder will not meet the mandatory experience requirement (as applicable) unless the response is received within 5 working days of the date that Canada's email was sent.
- (iii) If Canada does not receive a response from the contact person within the 5 working days, Canada will not contact the Bidder and will not permit the substitution of an alternate contact person.
- (iv) Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated.
- (v) Points will not be allocated and/or a bidder will not meet the mandatory experience requirement (as applicable) if (1) the reference customer states he or she is unable or unwilling to provide the information requested, or (2) the customer reference is not a customer of the Bidder itself (for example, the customer cannot be the customer of an affiliate of the Bidder instead of being a customer of the Bidder itself). Nor will points be allocated or a mandatory met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder.

#### **4.3 Financial Evaluation**

- (a) The financial evaluation will be conducted using the firm per diem rates provided by the responsive bid(s). A separate financial evaluation will be conducted for each Workstream.
- (b) There are two possible financial evaluation methods for this requirement. The first method will be used if three or more bids are determined responsive (see (c) Financial Evaluation - Method A below). The second method will be used if fewer than three bids are determined responsive (see (d) Financial Evaluation - Method B below).

(c) **Financial Evaluation - Method A:** The following financial evaluation method will be used if three or more bids are determined responsive:

- (i) **STEP 1 - ESTABLISHING THE LOWER AND UPPER MEDIAN BAND LIMITS FOR EACH PERIOD AND EACH RESOURCE CATEGORY:** The Contracting Authority will establish, for each period and each Resource Category of each Workstream, the median band limits based on the firm per diem rates provided by the technically responsive bids. For each such Resource Category the median will be calculated using the median function in Microsoft Excel and will represent a range that encompasses any rate to a value of minus (-) 10% of the median, and an upper median rate to a value of plus (+) 30% of the median. When an even number of technically responsive bids have been determined, an average of the middle two rates will be used to calculate the median band limits and for an odd number of technically responsive bids, the middle rate will be used.
- (ii) **STEP 2 - POINTS ALLOCATION:** For each period and each Resource Category of each Workstream, points will be allocated as follows:
- (A) A Bidder's proposed firm per diem rate that is either lower than the established lower median band limit or higher than the established upper median band limit for that period and Resource Category will be allocated 0 points.
- (B) A Bidder's proposed firm per diem rate falling within the upper and lower median band limits, for that period and Resource Category, will be allocated points using the following calculation, which will be rounded to two decimal places:
- $$\frac{\text{Lowest proposed firm per diem rate within the median band limits}}{\text{Bidder's proposed firm per diem rate within the median band limits}} \times \text{Maximum Points Assigned at Table 1 below}$$
- (C) A Bidder's proposed firm per diem rate falling within the established median band limits which is the lowest proposed firm per diem rate will be allocated the applicable maximum points assigned at Table 1 below.

#### Workstream 1

TABLE 1 - MAXIMUM POINTS ASSIGNED				
RESOURCE CATEGORIES	INITIAL (3 YEARS) CONTRACT PERIOD	OPTION PERIOD 1	OPTION PERIOD 2	TOTAL POINTS
C.2 IT Security Methodology, Policy and Procedures Analyst – Level 3	225	75	75	375
C.3 IT Security TRA and C&A Analyst – Level 3	225	75	75	375
C.7 IT Security Design Specialist (General Stream) – Level 3	225	75	75	375
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream) – Level 3	225	75	75	375
P.12 Risk Management Specialist – Level 3	225	75	75	375
B.1 Business Analyst – Level 3	150	50	50	250
B.14 Technical Writer – Level 3	150	50	50	250
<b>TOTAL</b>	<b>1425</b>	<b>475</b>	<b>475</b>	<b>2375</b>

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

## Workstream 2

TABLE 1 - MAXIMUM POINTS ASSIGNED				
RESOURCE CATEGORIES	INITIAL (3 YEARS) CONTRACT PERIOD	OPTION PERIOD 1	OPTION PERIOD 2	TOTAL POINTS
C.3 IT Security TRA and C&A Analyst – Level 3	225	75	75	375
C.7 IT Security Design Specialist (General Stream) – Level 3	225	75	75	375
C.11 IT Security VA Specialist – Level 3	225	75	75	375
C.16 PIA Specialist – Level 3	225	75	75	375
P.9 Project Manager – Level 3	150	50	50	250
B.1 Business Analyst – Level 3	150	50	50	250
A.7 Programmer/Analyst – Level 3	180	60	60	300
<b>TOTAL</b>	<b>1380</b>	<b>460</b>	<b>460</b>	<b>2300</b>

- (iii) **STEP 3 - FINANCIAL SCORE:** Points allocated under STEP 2 for each period and Resource Category of each Workstream will be added together and rounded to two decimal places to produce the Financial Score. Bidders will find below an example of a financial evaluation using Method A.

- (iv) **EXAMPLE OF A FINANCIAL EVALUATION USING METHOD A**

TABLE 2 - EXAMPLE OF A FINANCIAL EVALUATION USING METHOD A:							
Resource Category	Max. Points	Bidder 1		Bidder 2		Bidder 3	
		Year 1	Year 2	Year 1	Year 2	Year 1	Year 2
<b>Programmer</b>	150 (75 pts. per year)	\$400.00	\$400.00	\$420.00	\$450.00	\$450.00	\$450.00
<b>Business Analyst</b>	100 (50 pts. per year)	\$600.00	\$600.00	\$600.00	\$620.00	\$650.00	\$820.00
<b>Project Manager</b>	50 (25 pts. per year)	\$555.00	\$900.00	\$750.00	\$800.00	\$700.00	\$800.00
<b>TOTAL</b>	<b>300</b>						
<b>STEP 1 - Establishing the lower and upper median band limits for each year and each resource category</b>							
(Median 1)	For the Programmer Resource Category, the year 1 median would be \$420.00. The lower median band limit would be \$336.00 and higher median band limit would be \$546.00.						
(Median 2)	For the Programmer Resource Category, the year 2 median would be \$450.00. The lower median band limit would be \$360.00 and higher median band limit would be \$585.00.						
(Median 3)	For the Business Analyst Resource Category, the year 1 median would be \$600.00. The lower median band limit would be \$480.00 and higher median band limit would be \$780.00.						
(Median 4)	For the Business Analyst Resource Category, the year 2 median would be \$620.00. The lower median band limit would be \$496.00 and higher median band limit would be \$806.00.						
(Median 5)	For the Project Manager Resource Category, the year 1 median would be \$700.00. The lower median band limit would be \$560.00 and higher median band limit would be \$910.00.						

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

(Median 6) For the Project Manager Resource Category, the year 2 median would be \$800.00. The lower median band limit would be \$640.00 and higher median band limit would be \$1,040.00.

**STEP 2 - Points Allocation:**

**Bidder 1:**

Programmer Year 1 = 75 points (lowest rate within the lower and upper median band limits)  
Programmer Year 2 = 75 points (lowest rate within the lower and upper median band limits)

Business Analyst Year 1 = 50 points (lowest rate within the lower and upper median band limits)  
Business Analyst Year 2 = 50 points (lowest rate within the lower and upper median band limits)

Project Manager Year 1 = 0 points (outside the lower and higher median band limits)  
Project Manager Year 2 = 22.22 points (based on the following calculation = (Lowest rate of \$800.00 / Bidder's proposed rate of \$900.00) Multiplied by 25 pts)

**Bidder 2:**

Programmer Year 1 = 71.43 points (based on the following calculation = (Lowest rate of \$400.00 / Bidder's proposed rate of \$420.00) Multiplied by 75 pts)  
Programmer Year 2 = 66.67 points (based on the following calculation = (Lowest rate of \$400.00 / Bidder's proposed rate of \$450.00) Multiplied by 75 pts)

Business Analyst Year 1 = 50 points (lowest price within the lower and upper median band limits)  
Business Analyst Year 2 = 48.39 points (based on the following calculation = (Lowest rate of \$600.00 / Bidder's proposed rate of \$620.00) Multiplied by 50 pts)

Project Manager Year 1 = 23.33 points (based on the following calculation = (Lowest rate of \$700.00 / Bidder's proposed rate of \$750.00) Multiplied by 25 pts)  
Project Manager Year 2 = 25 points (lowest price within the lower and upper median band limits)

**Bidder 3:**

Programmer Year 1 = 66.67 points (based on the following calculation = (Lowest rate of \$400.00 / Bidder's proposed rate of \$450.00) Multiplied by 75 pts)  
Programmer Year 2 = 66.67 points (based on the following calculation = (Lowest rate of \$400.00 / Bidder's proposed rate of \$450.00) Multiplied by 75 pts)

Business Analyst Year 1 = 46.15 points (based on the following calculation = (Lowest rate of \$600.00 / Bidder's proposed rate of \$650.00) Multiplied by 75 pts)  
Business Analyst Year 2 = 0 points (outside the lower and higher median band limits)

Project Manager Year 1 = 25 points (lowest price within the lower and upper median band limits)  
Project Manager Year 2 = 25 points (lowest price within the lower and upper median band limits)

**STEP 3 - Financial Score:**

**Bidder 1:** 75 + 75 + 50 + 50 + 0 + 22.22 = Total Financial Score of 272.22 points out of a possible 300 points

**Bidder 2:** 71.43 + 67.67 + 50 + 48.39 + 23.33 + 25 = Total Financial Score of 284.82 points out of a possible 300 points

**Bidder 3:** 66.67 + 66.67 + 46.15 + 0 + 25 + 25 = Total Financial Score of 229.49 points out of a possible 300 points

(d) **Financial Evaluation - Method B:** The following financial evaluation method will be used if less than three bids are determined responsive:

(i) **STEP 1 - POINTS ALLOCATION:** For each period and each Resource Category of each Workstream, points will be allocated as follows:

- (A) Points will be established based on the following calculation, with points rounded to two decimal places:

$$\frac{\text{Lowest proposed firm per diem rate}}{\text{Bidder's proposed firm per diem rate}} \times \text{Maximum Points Assigned at Table 3 below}$$

The Bidder with the lowest proposed firm per diem rate will be allocated the applicable maximum points assigned at Table 3 below.

### Workstream 1

TABLE 3 - MAXIMUM POINTS ASSIGNED				
RESOURCE CATEGORIES	INITIAL (3 YEARS) CONTRACT PERIOD	OPTION PERIOD 1	OPTION PERIOD 2	TOTAL POINTS
C.2 IT Security Methodology, Policy and Procedures Analyst – Level 3	225	75	75	375
C.3 IT Security TRA and C&A Analyst – Level 3	225	75	75	375
C.7 IT Security Design Specialist (General Stream) – Level 3	225	75	75	375
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream) – Level 3	225	75	75	375
P.12 Risk Management Specialist – Level 3	225	75	75	375
B.1 Business Analyst – Level 3	150	50	50	250
B.14 Technical Writer – Level 3	150	50	50	250
<b>TOTAL</b>	<b>1425</b>	<b>475</b>	<b>475</b>	<b>2375</b>

### Workstream 2

TABLE 3 - MAXIMUM POINTS ASSIGNED				
RESOURCE CATEGORIES	INITIAL (3 YEARS) CONTRACT PERIOD	OPTION PERIOD 1	OPTION PERIOD 2	TOTAL POINTS
C.3 IT Security TRA and C&A Analyst – Level 3	225	75	75	375
C.7 IT Security Design Specialist (General Stream) – Level 3	225	75	75	375
C.11 IT Security VA Specialist – Level 3	225	75	75	375
C.16 PIA Specialist – Level 3	225	75	75	375
P.9 Project Manager – Level 3	150	50	50	250
B.1 Business Analyst – Level 3	150	50	50	250
A.7 Programmer/Analyst – Level 3	180	60	60	300
<b>TOTAL</b>	<b>1380</b>	<b>460</b>	<b>460</b>	<b>2300</b>

- 
- (ii) **STEP 2 - FINANCIAL SCORE:** Points allocated under STEP 1, for each period and each Resource Category, will be added together and rounded to two decimal places to produce the Financial Score.

(e) **Substantiation of Professional Services Rates**

In Canada's experience, bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates bid for professional services, Canada may, but will have no obligation to, require price support in accordance with this Article. If Canada requests price support, it will be requested from all otherwise responsive bidders who have proposed a rate that is at least 20% lower than the median rate bid by all responsive bidders for the relevant resource category or categories. If Canada requests price support, the Bidder must provide the following information:

- (i) an invoice (referencing a contract serial number or other unique contract identifier) that shows that the Bidder has provided and invoiced a customer (with whom the Bidder deals at arm's length) for services performed for that customer similar to the services that would be provided in the relevant resource category, where those services were provided for at least three months within the eighteen months before the bid solicitation closing date, and the fees charged were equal to or less than the rate offered to Canada;
- (ii) in relation to the invoice in (i), evidence from the Bidder's customer that the services identified in the invoice include at least 50% of the tasks listed in the Statement of Work for the category of resource being assessed for an unreasonably low rate. This evidence must consist of either a copy of the contract (which must describe the services to be provided and demonstrate that at least 50% of the tasks to be performed are the same as those to be performed under the Statement of Work in this bid solicitation) or the customer's signed certification that the services subject to the charges in the invoice included at least 50% of the same tasks to be performed under the Statement of Work in this bid solicitation; and
- (iii) the name, telephone number and, if available, e-mail address of a contact person at the customer who received each invoice submitted under (i), so that Canada may verify any information provided by the Bidder.

Once Canada requests substantiation of the rates bid for any resource category, it is the sole responsibility of the Bidder to submit information (as described above and as otherwise may be requested by Canada, including information that would allow Canada to verify information with the resource proposed) that will allow Canada to determine whether it can rely, with confidence, on the Bidder's ability to provide the required services at the rates bid. If Canada determines that the information provided by the Bidder does not adequately substantiate the unreasonably low rates, the bid will be declared non-responsive.

(f) **Formulae in Pricing Tables**

If the pricing tables provided to bidders include any formulae, Canada may re-input the prices provided by bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a bidder.

---

#### 4.4 Basis of Selection

**Note to Bidders:** *if a bidder is selected for award of more than one Workstream, Canada reserves the right to award one contract for all the Workstreams awarded to that bidder.*

##### (a) Evaluation of Bid – Multiple Contracts Awarded for Multiple Workstreams

**Selection Process:** The following selection process will be conducted for each Workstream:

- (i) A bid must comply with the requirements of the bid solicitation, meet all mandatory evaluation criteria and obtain the required pass marks for the point rated criteria identified in this bid solicitation to be declared responsive.
- (ii) The responsive bid that obtains the highest Total Bidder Score will be recommended for award of a contract. For any given Bidder, the greatest possible Total Technical Score is 70 while the greatest possible Total Financial Score is 30.

- (A) Calculation of Total Technical Score: For each Workstream, the Total Technical Score will be computed for each responsive bid by converting the Technical Score obtained for the point-rated technical criteria using the following formula, rounded to two decimal places:

$$\frac{\text{Technical Score}}{\text{Maximum Technical Points (Bidders, please refer to the maximum technical points for each Workstream at Attachment 4.2)}} \times 70 = \text{Total Technical Score}$$

- (B) Calculation of Total Financial Score: For each Workstream, the Total Financial Score will be computed for each responsive bid by converting the Financial Score obtained for the financial evaluation using the following formula rounded to two decimal places:

$$\frac{\text{Financial Score}}{\text{Total Maximum Points Assigned (Bidders, please refer to the total maximum points assigned for each Workstream)}} \times 30 = \text{Total Financial Score}$$

- (C) Calculation of the Total Bidder Score: For each Workstream, the Total Bidder Score will be computed for each responsive bid in accordance with the following formula:

$$\text{Total Technical Score} + \text{Total Financial Score} = \text{Total Bidder Score}$$

- (iii) In the event of identical Total Bidder Scores occurring within a given Workstream, then the bid with the highest Total Financial Score will become the top-ranked bidder.

- (b) **Contract Funding Allocation:** Where for a Workstream more than one contract is awarded, each contract issued for that particular Workstream will be issued with an amount of funding specified in the article titled "Limitation of Expenditure" calculated based on the following:

- (i) when one contract is awarded, the amount of the Limitation of Expenditure will be determined at Canada's discretion;
- (ii) where two contracts are awarded, the amount of the Limitation of Expenditure of each contract will be determined in accordance with the following:

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Bidder	Total Bidder Score	Fund Allocation Formula (%)	Total Funds Allocated
1 <sup>st</sup> ranked	98	$98/187 \times 100 = 52.41$	\$5,241,000.00
2 <sup>nd</sup> ranked	89	$89/187 \times 100 = 47.59$	\$4,759,000.00
Total	187		\$10,000,000.00
Total funds available: \$10,000,000.00			

**NOTE: This is an example only. Actual numbers will be determined after bid evaluation.**

- (c) Bidders should note that all contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

---

## **PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION**

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

### **5.1 Certifications Precedent to Contract Award and Additional Information**

The certifications and additional information listed below should be submitted with the bid, but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame provided will render the bid non-responsive.

#### **(a) Federal Contractors Program for Employment Equity - Bid Certification**

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "[FCP Limited Eligibility to Bid](https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html)" list available at the bottom of the page of the Employment and Social Development Canada (ESDC) - Labour's website. (<https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html> ).

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "[FCP Limited Eligibility to Bid](https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html)" list at the time of contract award.

Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "[FCP Limited Eligibility to Bid](https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html)" list during the period of the Contract.

The Bidder must provide the Contracting Authority with a completed Attachment 5.1, Federal Contractors Program for Employment Equity - Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed Attachment Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

#### **(b) Certification of Language - English Essential**

By submitting a bid, the Bidder certifies that, should it be awarded a contract as result of the bid solicitation, every individual proposed in its bid will be fluent in English. The individual(s) proposed must be able to communicate orally and in writing in English without any assistance and with minimal errors.

#### **(c) Submission of Only One Bid**

By submitting a bid, the Bidder is certifying that it does not consider itself to be related to any other bidder.

---

## PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

### 6.1 Security Requirement

- (a) Before award of a contract, the following conditions must be met:
  - (i) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;
- (b) Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.
- (c) For additional information on security requirements, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (<http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html>) website.
- (d) In the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

### 6.2 Financial Capability

- (a) SACC Manual clause A9033T (2012-07-16) Financial Capability applies, except that subsection 3 is deleted and replaced with the following: "If the Bidder is a subsidiary of another company, then any financial information required by the Contracting Authority in 1(a) to (f) must be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the Bidder; however, if the Bidder is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary, the financial information of the parent company must be provided. If Canada determines that the Bidder is not financially capable but the parent company is, or if Canada is unable to perform a separate assessment of the Bidder's financial capability because its financial information has been combined with its parent's, Canada may, in its sole discretion, award the contract to the Bidder on the condition that the parent company grant a performance guarantee to Canada."
- (b) In the case of a joint venture bidder, each member of the joint venture must meet the financial capability requirements.

---

## PART 7 - RESULTING CONTRACT CLAUSES

**Note to Bidders:** Any resulting contract would only list the applicable Workstream(s) above that are awarded to the successful bidder(s) in accordance with the evaluation methodology set out in this bid solicitation. If a bidder is selected for award of more than one Workstream, Canada reserves the right to award one contract for all the Workstreams awarded to that bidder.

The following clauses apply to and form part of any contract resulting from the bid solicitation.

### 7.1 Requirement

- (a) \_\_\_\_\_ (the "**Contractor**") agrees to supply to the Client the services described in the Contract, including the Statement of Work, in accordance with, and at the prices set out in, the Contract. This includes providing professional services as and when requested by Canada, to one or more locations to be designated by Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.
- (b) **Client:** Under the Contract, the "**Client**" is Treasury Board of Canada Secretariat.
- (c) **Reorganization of Client:** The Contractor's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Client. The reorganization, reconfiguration and restructuring of the Client includes the privatization of the Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the Contracting Authority or Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.
- (d) **Defined Terms:** Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions or Supplemental General Conditions. Any reference to an Identified User in the Supply Arrangement is a reference to the Client. Also, any reference to a "deliverable" or "deliverables" includes all documentation outlined in this Contract. A reference to a "local office" of the Contractor means an office having at least one full time employee that is not a shared resource working at that location.

### 7.2 Task Authorization

- (a) **As-and-when-requested Task Authorizations:** The Work or a portion of the Work to be performed under the Contract will be on an "as-and-when-requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract. The Contractor must not commence work until a validly issued TA has been issued by Canada and received by the Contractor. The Contractor acknowledges that any work performed before such issuance and receipt will be done at the Contractor's own risk.
- (b) **Allocation of Task Authorizations:**
  - (i) More than one Contract has been awarded for this requirement. As a result, the Task Authorizations issued under this series of contracts will be allocated in accordance with the following.
  - (ii) Canada will make a reasonable effort to ensure that the dollar value of the TAs issued to the Contractors are proportionally balanced throughout the Contract Period based on the percentage values described in the Contract Funding Allocation in the bid solicitation. A review of TAs issued to the Contractors will be conducted at six-month intervals and at

---

the beginning of each fiscal year to confirm proportional utilization and distribution of the TAs.

- (iii) In the event that Canada determines the proposed resource(s) does not meet the minimum experience or other requirements of the categories identified in the draft TA, Canada may, at its entire discretion request that the contractor propose another resource and the contractor will have the time set out in the subparagraph "Contractor's Response to Draft Task Authorization" to respond. If the contractor fails to respond on time or Canada determines that the proposed resource(s) does not meet the minimum experience or other requirements of the categories identified in the draft TA, the draft TA will be forwarded to the next contractor, under the same allocation process. The dollar value of the refused TA may be subtracted from the dollar value of the Contractor's Contract and may be re-allocated, at the Contracting Authority's sole discretion, in whole or in part, to one or more of the other contractors. Should all Contractors refuse a TA under the Contract, Canada reserves the right to use other methods of supply.
- (c) **Assessment of Resources Proposed at TA Stage:** Processes for issuing, responding to and assessing Task Authorizations are further detailed in Appendices A, B, C and D of Annex A.
- (d) **Form and Content of draft Task Authorization:**
  - (i) The Technical Authority will provide the Contractor with a description of the task in a draft Task Authorization using the form specified in Annex B.
  - (ii) The draft Task Authorization will contain the details of the activities to be performed, and must also contain the following information:
    - (A) the task number;
    - (B) The date by which the Contractor's response must be received (which will appear in the draft Task Authorization, but not the issued Task Authorization);
    - (C) the categories of resources and the number required;
    - (D) a description of the work for the task outlining the activities to be performed and identifying any deliverables (such as reports);
    - (E) the start and completion dates;
    - (F) any option(s) to extend initial end date (if applicable);
    - (G) milestone dates for deliverables and payments (if applicable);
    - (H) the number of person-days of effort required;
    - (I) whether the work requires on-site activities and the location;
    - (J) the language profile of the resources required;
    - (K) the level of security clearance required of resources;
    - (L) the price payable to the Contractor for performing the task, with an indication of whether it is a firm price or a maximum TA price (and, for maximum price task authorizations, the TA must indicate how the final amount payable will be determined; where the TA does not indicate how the final amount payable will be determined, the amount payable is the amount, up to the maximum, that the Contractor demonstrates was actually worked on the project, by submitting time sheets filled in at the time of the work by the individual resources to support the charges); and
    - (M) any other constraints that might affect the completion of the task.

(e) **Contractor's Response to Draft Task Authorization:** The Contractor must provide to the Technical Authority, within 2 working days of receiving the draft Task Authorization (or within any longer time period specified in the draft TA), a quotation with the proposed total price for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract, as well as its corresponding proposed resource(s) in accordance with Appendix A to Annex A of the Contract. The Contractor's quotation must be based on the rates set out in the Contract. The Contractor will not be paid for preparing or providing its response or for providing other information required to prepare and validly issue the TA.

(f) **Task Authorization Limit and Authorities for Validly Issuing Task Authorizations:**

(i) To be validly issued, a TA must include the following signatures:

(A) for any TA, inclusive of revisions, with a value less than or equal to \$300,000.00 (excluding Applicable Taxes), the TA must be signed by:

(1) the Technical Authority; and

(2) a representative from TBS;

(B) for any TA, inclusive of revisions, with a value greater than this amount, a TA must include the following signatures:

(1) the Technical Authority; and

(2) the Contracting Authority.

Any TA that does not bear the appropriate signatures is not validly issued by Canada. Any work performed by the Contractor without receiving a validly issued TA is done at the Contractor's own risk. If the Contractor receives a TA that is not appropriately signed, the Contractor must notify the Contracting Authority. By providing written notice to the Contractor, the Contracting Authority may suspend the Client's ability to issue TA's at any time, or reduce the dollar value threshold described in subarticle (A) above; any suspension or reduction notice is effective upon receipt.

(g) **Periodic Usage Reports:**

(i) The Contractor must compile and maintain records on its provision of services to the federal government under Task Authorizations validly issued under the Contract. The Contractor must provide this data to Canada in accordance with the reporting requirements detailed below. If some data is not available, the reason must be indicated. If services are not provided during a given period, the Contractor must still provide a "NIL" report. The data must be submitted on a quarterly basis to the Contracting Authority. From time to time, the Contracting Authority may also require an interim report during a reporting period.

(ii) The quarterly periods are defined as follows:

(A) 1<sup>st</sup> quarter: April 1 to June 30;

(B) 2<sup>nd</sup> quarter: July 1 to September 30;

(C) 3<sup>rd</sup> quarter: October 1 to December 31; and

(D) 4<sup>th</sup> quarter: January 1 to March 31.

The data must be submitted to the Contracting Authority no later than 10 calendar days after the end of the reporting period.

(iii) Each report must contain the following information for each validly issued TA (as amended):

- 
- (A) the Task Authorization number and the Task Authorization Revision number(s), if applicable;
  - (B) a title or a brief description of each authorized task;
  - (C) the name, Resource category and level of each resource involved in performing the TA, as applicable;
  - (D) the total estimated cost specified in the validly issued TA of each task, exclusive of Applicable Taxes;
  - (E) the total amount, exclusive of Applicable Taxes, expended to date against each authorized task;
  - (F) the start and completion date for each authorized task; and
  - (G) the active status of each authorized task, as applicable (e.g., indicate whether work is in progress or if Canada has cancelled or suspended the TA, etc.).
- (iv) Each report must also contain the following cumulative information for all the validly issued TA's (as amended):
- (A) the amount, exclusive of Applicable Taxes, specified in the Contract (as last amended, as applicable) as Canada's total liability to the Contractor for all validly issued TA's; and
  - (B) the total amount, exclusive of Applicable Taxes, expended to date against all validly issued TA's.
- (h) **Refusal of Task Authorizations or Submission of a Response which is not Valid:** The Contractor is not required to submit a response to every draft TA sent to it by Canada. However, in addition to Canada's other rights to terminate the Contract, Canada may immediately, and without further notice, terminate the Contract for default in accordance with the General Conditions if the Contractor in at least three instances has either not responded or has not submitted a valid response when sent a draft TA. For greater clarity, each draft TA, which is identifiable by its task number, will only count as one instance. A valid response is one that is submitted within the required time period and meets all requirements of the draft TA issued, including proposing the required number of resources who each meet the minimum experience and other requirements of the categories identified in the draft TA at pricing not exceeding the rates set out in Annex B.
- (i) **Consolidation of TA's for Administrative Purposes:** The Contract may be amended from time to time to reflect all validly issued Task Authorizations to date, to document the Work performed under those TA's for administrative purposes.

### 7.3 Minimum Work Guarantee

- (a) In this clause,
- (i) **"Maximum Contract Value"** means the amount specified in the **"Limitation of Expenditure"** clause set out in the Contract; and
  - (ii) **"Minimum Contract Value"** means \$20,000 (excluding Applicable Taxes).
- (b) Canada's obligation under the Contract is to request Work in the amount of the Minimum Contract Value or, at Canada's option, to pay the Contractor at the end of the Contract in accordance with sub-article (c), subject to sub-article (d). In consideration of such obligation, the Contractor agrees to stand in readiness throughout the Contract Period to perform the Work described in the Contract. Canada's maximum liability for work performed under the Contract must not exceed the Maximum Contract Value, unless an increase is authorized in writing by the Contracting Authority.

- 
- (c) In the event that Canada does not request work in the amount of the Minimum Contract Value during the Contract Period, Canada must pay the Contractor the difference between the Minimum Contract Value and the total cost of the Work requested.
- (d) Canada will have no obligation to the Contractor under this article if Canada terminates the entire Contract
- (i) for default;
  - (ii) for convenience as a result of any decision or recommendation of a tribunal or court that the contract be cancelled, re-tendered or awarded to another supplier; or
  - (iii) for convenience within ten business days of Contract award.

#### 7.4 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Works and Government Services Canada.

(a) **General Conditions:**

- (i) 2035 (2018-06-21), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

With respect to Section 30 - Termination for Convenience, of General Conditions 2035, Subsection 04 is deleted and replaced with the following Subsections 04, 05 and 06:

- 4. The total of the amounts, to which the Contractor is entitled to be paid under this section, together with any amounts paid, due or becoming due to the Contractor must not exceed the Contract Price.
- 5. Where the Contracting Authority terminates the entire Contract and the Articles of Agreement include a Minimum Work Guarantee, the total amount to be paid to the Contractor under the Contract will not exceed the greater of:
  - (a) the total amount the Contractor may be paid under this section, together with any amounts paid, becoming due other than payable under the Minimum Work Guarantee, or due to the Contractor as of the date of termination, or
  - (b) the amount payable under the Minimum Work Guarantee, less any amounts paid, due or otherwise becoming due to the Contractor as of the date of termination.
- 6. The Contractor will have no claim for damages, compensation, loss of profit, allowance arising out of any termination notice given by Canada under this section except to the extent that this section expressly provides. The Contractor agrees to repay immediately to Canada the portion of any advance payment that is unliquidated at the date of the termination.

(b) **Supplemental General Conditions:**

The following Supplemental General Conditions:

- (i) 4002 (2010-08-16), Supplemental General Conditions - Software Development or Modification Services;
- (ii) 4007 (2010-08-16), Supplemental General Conditions - Canada to Own Intellectual Property Rights in Foreground Information;

apply to and form part of the Contract.

---

## 7.5 Security Requirement

The following security requirements (SRCL #34 and related clauses provided by the Contract Security Program) as set out under Annex "B" to the Supply Arrangement, applies to and forms part of the Contract.

Security Requirement for Canadian Supplier: Public Services and Procurement Canada File #Common-Professional Services Security Requirement Check List #34

1. The Contractor must, at all times during the performance of the Contract, hold a valid Facility Security Clearance at the level of **secret**, issued by the Canadian Industrial Security Directorate (CISD), Public Services and Procurement Canada (PSPC)
2. The Contractor personnel requiring access to protected/classified information, assets or sensitive work site(s) must EACH hold a valid personnel security screening at the level of **secret** as required, granted or approved by CISD/PSPC
3. The Contractor must not remove any protected/classified information from the identified work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restriction
4. Subcontracts which contain security requirements are not to be awarded without the prior written permission of CISD/PSPC
5. The Contractor must comply with the provisions of the:
  - a. Security Requirements Check List and security guide (if applicable), attached at Annex C
  - b. Industrial Security Manual (Latest Edition)

## 7.6 Contract Period

- (a) **Contract Period:** The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:
- (i) The "**Initial Contract Period**", which begins on the date the Contract is awarded and ends three year(s) later; and
  - (ii) The period during which the Contract is extended, if Canada chooses to exercise any options set out in the Contract.
- (b) **Option to Extend the Contract:**
- (i) The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to two additional one-year period(s) under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.
  - (ii) Canada may exercise this option at any time by sending a written notice to the Contractor before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced, for administrative purposes only, through a contract amendment.

## 7.7 Authorities

(a) **Contracting Authority**

The Contracting Authority for the Contract is:

Name:	Lan Mao
Title:	Supply Team Leader Public Works and Government Services Canada, Acquisitions Branch
Directorate:	Informatics and Telecommunications Systems Procurement Directorate
Address:	10 Wellington, Gatineau, Québec

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Telephone: (613) 858-9980  
E-mail address: [lan.mao@tpsgc-pwgsc.gc.ca](mailto:lan.mao@tpsgc-pwgsc.gc.ca)

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

(b) **Technical Authority**

The Technical Authority for the Contract is: ***(To be completed at contract award)***

Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Organization: \_\_\_\_\_  
Address: \_\_\_\_\_  
Telephone: \_\_\_\_\_  
Facsimile: \_\_\_\_\_  
E-mail address: \_\_\_\_\_

The Technical Authority [is the representative of the department or agency for whom the Work is being carried out under the Contract and] is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

(c) **Contractor's Representative *(To be completed at contract award)***

**7.8 Proactive Disclosure of Contracts with Former Public Servants**

By providing information on its status, with respect to being a former public servant in receipt of a Public Service Superannuation Act (PSSA) pension, the Contractor has agreed that this information will be reported on departmental web sites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

**7.9 Payment**

(a) **Basis of Payment**

- (i) **Professional Services provided under a Task Authorization with a Maximum Price:** For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked and any resulting deliverables in accordance with the firm all-inclusive per diem rates set out in Annex B, Basis of Payment, Applicable Taxes extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.
- (ii) **Professional Services provided under a Task Authorization with a Firm Price:** For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor the firm price set out in the Task Authorization (based on the firm, all-inclusive per diem rates set out in Annex B), Applicable Taxes extra.
- (iii) **Travel and Living Expenses – National Joint Council Travel Directive:** The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal and private vehicle

---

expenses provided in Appendices B, C and D of the *National Joint Council Travel Directive* and with the other provisions of the directive referring to “travellers”, rather than those referring to “employees”. All travel must have the prior authorization of the Technical Authority. Travel requests will only be considered for a work location which is located more than 100 kilometers from 90 Elgin Street, Ottawa, ON. The Contractor will be paid for actual time spent travelling in accordance with the firm per diem rate set out in Annex B which per diem is based on a 7.5-hour workday.

(iv) **Competitive Award:** The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.

(v) **Contractor's Firm Per Diem Rates:** The Contractor agrees that the rates set out in Annex B remain firm throughout the Contract Period, except as may be provided for in the express terms of the contract. In reference to Article 18(1) of SACC General Conditions 2035, the Contractor acknowledges that its obligation to provide services in accordance with the firm rates set out in Annex B is unaffected by the application of any existing law or any new law which may come into effect during the Contract Period.

(vi) **Professional Services Rates:** In Canada's experience, bidders from time to time propose rates at the time of bidding for one or more Resource Categories that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. This denies Canada of the benefit of the awarded contract. If the Contractor does not respond or refuses to provide an individual with the qualifications described in the Contract within the time described in the Contract (or proposes instead to provide someone from an alternate category at a different rate), whether or not Canada terminates the Contract as a whole or in part or chooses to exercise any of the rights provided to it under the general conditions, Canada may impose sanctions or take other measures in accordance with the PWGSC Vendor Performance Corrective Measure Policy (or equivalent) then in effect, which measures may include an assessment that results in conditions applied against the Contractor to be fulfilled before doing further business with Canada, or full debarment of the Contractor from bidding on future requirements.

(b) **Limitation of Expenditure – Cumulative Total of all Task Authorizations**

(i) Canada's total liability to the Contractor under the Contract for all validly issued Task Authorizations (TAs), inclusive of any revisions, must not exceed the amount set out on page 1 of the Contract, less any Applicable taxes. With respect to the amount set out on page 1 of the Contract, Customs duties are excluded and Applicable Taxes are included

(ii) No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

(iii) The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

(A) when it is 75 percent committed, or

(B) 4 months before the contract expiry date, or

(C) As soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized TAs, inclusive of any revisions,

whichever comes first.

- 
- (i) If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Providing this information does not increase Canada's liability.
- (c) **Method of Payment for Task Authorizations with a Maximum Price:** For each Task Authorization validly issued under the Contract that contains a maximum price:
- (i) Canada will pay the Contractor no more frequently than once a month in accordance with the Basis of Payment. The Contractor must submit time sheets for each resource showing the days and hours worked to support the charges claimed in the invoice.
- (ii) Once Canada has paid the maximum TA price, Canada will not be required to make any further payment, but the Contractor must complete all the work described in the TA, all of which is required to be performed for the maximum TA price. If the work described in the TA is completed in less time than anticipated, and the actual time worked (as supported by the time sheets) at the rates set out in the Contract is less than the maximum TA price, Canada is only required to pay for the time spent performing the work related to that TA.
- (d) **Method of Payment for Task Authorizations with a Firm Price - Lump Sum Payment on Completion:** Canada will pay the Contractor upon completion and delivery of all the Work associated with the validly issued Task Authorization in accordance with the payment provisions of the Contract if:
- (i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- (ii) all such documents have been verified by Canada; and
- (iii) the Work delivered has been accepted by Canada.
- (e) **Time Verification**
- Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contractor must repay any overpayment, at Canada's request.
- (f) **No Responsibility to Pay for Work not performed due to Closure of Government Offices**
- (i) Where the Contractor, its employees, subcontractors, or agents are providing services on government premises under the Contract and those premises are inaccessible because of the evacuation or closure of government offices, and as a result no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if there had been no evacuation or closure.
- (ii) If, as a result of any strike or lock-out, the Contractor or its employees, subcontractors or agents cannot obtain access to government premises and, as a result, no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if the Contractor had been able to gain access to the premises

#### 7.10 Invoicing Instructions

- (a) The Contractor must submit invoices in accordance with the information required in the General Conditions.
- (b) The Contractor's invoice must include a separate line item for each subparagraph in the Basis of Payment provision, and must show all applicable Task Authorization numbers.

- 
- (c) By submitting invoices, the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.
  - (d) The Contractor must provide the original and two copies of each invoice to the Technical Authority, and a copy to the Contracting Authority.

#### **7.11 Certifications and Additional Information**

- (a) Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, any TA quotation and the ongoing cooperation in providing additional information are conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire Contract Period.

#### **7.12 Federal Contractors Program for Employment Equity - Default by Contractor**

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the "[FCP Limited Eligibility to Bid](#)" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

#### **7.13 Applicable Laws**

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in \_\_\_\_\_.

#### **7.14 Priority of Documents**

If there is a discrepancy between the wording of any documents that appear on the following list, the wording of the document that first appears on the list has priority over the wording of any document that appears later on the list:

- (a) these Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement;
- (b) Supplemental General Conditions, in the following order:
  - (i) 4002 (2010-08-16), Supplemental General Conditions - Software Development or Modification Services;
  - (ii) 4007 (2010-08-16), Supplemental General Conditions - Canada to Own Intellectual Property Rights in Foreground Information;
- (c) General Conditions 2035 (2018-06-21), Higher Complexity - Services;
- (d) Annex A, Statement of Work, including its Appendices as follows:
  - (i) Appendix A to Annex A - Tasking Assessment Procedure;
  - (ii) Appendix B to Annex A - Task Authorization (TA) Form;
  - (iii) Appendix C to Annex A - Resource Assessment Criteria and Response Table;
  - (iv) Appendix D to Annex A - Certifications at the TA stage;
- (e) Annex B, Basis of Payment;
- (f) Annex C, Security Requirements Check List;

- (g) the validly issued Task Authorizations and any required certifications (including all of their annexes, if any); and
- (h) the Contractor's bid dated \_\_\_\_\_, as clarified on \_\_\_\_\_ "or" as amended \_\_\_\_\_.

#### **7.15 Foreign Nationals (Canadian Contractor)**

- (a) SACC Manual clause A2000C (2006-06-16) Foreign Nationals (Canadian Contractor)

**Note to Bidders:** *Either this clause or the one that follows, whichever applies (based on whether the successful Bidder is a Canadian Contractor or Foreign Contractor), will be included in any resulting contract.*

#### **7.16 Foreign Nationals (Foreign Contractor)**

- (a) SACC Manual clause A2001C (2006-06-16) Foreign Nationals (Foreign Contractor)

#### **7.17 Insurance Requirements**

##### **(a) Compliance with Insurance Requirements**

- (i) The Contractor must comply with the insurance requirements specified in this Article. The Contractor must maintain the required insurance coverage for the duration of the Contract. Compliance with the insurance requirements does not release the Contractor from or reduce its liability under the Contract.
- (ii) The Contractor is responsible for deciding if additional insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any additional insurance coverage is at the Contractor's expense, and for its own benefit and protection.
- (iii) The Contractor should forward to the Contracting Authority within ten (10) days after the date of award of the Contract a Certificate of Insurance evidencing the insurance coverage. Coverage must be placed with an Insurer licensed to carry out business in Canada and the Certificate of Insurance must confirm that the insurance policy complying with the requirements is in force. If the Certificate of Insurance has not been completed and submitted as requested, the Contracting Authority will so inform the Contractor and provide the Contractor with a time frame within which to meet the requirement. Failure to comply with the request of the Contracting Authority and meet the requirement within the time period will constitute a default under the General Conditions. The Contractor must, if requested by the Contracting Authority, forward to Canada a certified true copy of all applicable insurance policies.

##### **(b) Commercial General Liability Insurance**

- (i) The Contractor must obtain Commercial General Liability Insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature, but for not less than \$2,000,000 per accident or occurrence and in the annual aggregate.
- (ii) The Commercial General Liability policy must include the following:
  - (A) Additional Insured: Canada is added as an additional insured, but only with respect to liability arising out of the Contractor's performance of the Contract. The interest of Canada should read as follows: Canada, as represented by Public Works and Government Services Canada.
  - (B) Bodily Injury and Property Damage to third parties arising out of the operations of the Contractor.

- 
- (C) Products and Completed Operations: Coverage for bodily injury or property damage arising out of goods or products manufactured, sold, handled, or distributed by the Contractor and/or arising out of operations that have been completed by the Contractor.
- (D) Personal Injury: While not limited to, the coverage must include Violation of Privacy, Libel and Slander, False Arrest, Detention or Imprisonment and Defamation of Character.
- (E) Cross Liability/Separation of Insureds: Without increasing the limit of liability, the policy must protect all insured parties to the full extent of coverage provided. Further, the policy must apply to each Insured in the same manner and to the same extent as if a separate policy had been issued to each.
- (F) Blanket Contractual Liability: The policy must, on a blanket basis or by specific reference to the Contract, extend to assumed liabilities with respect to contractual provisions.
- (G) Employees and, if applicable, Volunteers must be included as Additional Insured.
- (H) Employers' Liability (or confirmation that all employees are covered by Worker's compensation (WSIB) or similar program)
- (I) Broad Form Property Damage including Completed Operations: Expands the Property Damage coverage to include certain losses that would otherwise be excluded by the standard care, custody or control exclusion found in a standard policy.
- (J) Notice of Cancellation: The Insurer will endeavour to provide the Contracting Authority thirty (30) days written notice of policy cancellation.
- (K) If the policy is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.
- (L) Owners' or Contractors' Protective Liability: Covers the damages that the Contractor becomes legally obligated to pay arising out of the operations of a subcontractor.
- (M) Advertising Injury: While not limited to, the endorsement must include coverage for piracy or misappropriation of ideas, or infringement of copyright, trademark, title or slogan.
- (c) **Errors and Omissions Liability Insurance**
- (i) The Contractor must obtain Errors and Omissions Liability (a.k.a. Professional Liability) insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature but for not less than \$1,000,000 per loss and in the annual aggregate, inclusive of defence costs.
- (ii) If the Professional Liability insurance is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.
- (iii) The following endorsement must be included:
- Notice of Cancellation: The Insurer will endeavour to provide the Contracting Authority thirty (30) days written notice of cancellation.
-

---

**7.18 Limitation of Liability - Information Management/Information Technology**

---

- (a) This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this Article, even if it has been made aware of the potential for those damages.
- (b) **First Party Liability:**
- (i) The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:
    - (A) any infringement of intellectual property rights to the extent the Contractor breaches the section of the General Conditions entitled "Intellectual Property Infringement and Royalties";
    - (B) physical injury, including death.
  - (ii) The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.
  - (iii) Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.
  - (iv) The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (i)(A) above.
  - (v) The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:
    - (A) any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and
    - (B) Any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of .75 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the cell titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or \$1,000,000.00.

In any case, the total liability of the Contractor under subparagraph (v) will not exceed the total estimated cost (as defined above) for the Contract or \$1,000,000.00, whichever is more.

- 
- (vi) If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

(c) **Third Party Claims:**

- (i) Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.
- (ii) If Canada is required, as a result of joint and several liability or joint and solidarily liable, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite Sub-article (i), with respect to special, indirect, and consequential damages of third parties covered by this Section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.
- (iii) The Parties are only liable to one another for damages to third parties to the extent described in this Sub-article (c).

**7.19 Joint Venture Contractor**

- (a) The Contractor confirms that the name of the joint venture is \_\_\_\_\_ and that it is comprised of the following members:
- (b) With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:
- (i) \_\_\_\_\_ has been appointed as the "representative member" of the joint venture Contractor and has fully authority to act as agent for each member regarding all matters relating to the Contract;
- (ii) by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and
- (iii) all payments made by Canada to the representative member will act as a release by all the members.
- (c) All the members agree that Canada may terminate the Contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.
- (d) All the members are jointly and severally or solidarily liable for the performance of the entire Contract.
- (e) The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing

member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.

- (f) The Contractor acknowledges that all security and controlled goods requirements in the Contract, if any, apply to each member of the joint venture Contractor.

**Note to Bidders:** *This Article will be deleted if the Bidder awarded the contract is not a joint venture. If the contractor is a joint venture, this clause will be completed with information provided in its bid.*

## 7.20 Professional Services - General

- (a) The Contractor must provide professional services on request as specified in this Contract. All resources provided by the Contractor must meet the qualifications described in the Contract (including those relating to previous experience, professional designation, education, language proficiency and security clearance) and must be competent to provide the required services by any delivery dates described in the Contract.
- (b) If the Contractor fails to deliver any deliverable (excluding delivery of a specific individual) or complete any task described in the Contract on time, in addition to any other rights or remedies available to Canada under the Contract or the law, Canada may notify the Contractor of the deficiency, in which case the Contractor must submit a written plan to the Technical Authority within ten working days detailing the actions that the Contractor will undertake to remedy the deficiency. The Contractor must prepare and implement the plan at its own expense.
- (c) In General Conditions 2035, the Article titled "Replacement of Specific Individuals" is deleted and the following applies instead:

### Replacement of Specific Individuals

- (i) If the Contractor is unable to provide the services of any specific individual identified in the Contract to perform the services, the Contractor must within five working days of having this knowledge, the individual's departure or failure to commence Work (or, if Canada has requested the replacement, within ten working days of Canada's notice of the requirement for a replacement) provide to the Contracting Authority:
- (A) the name, qualifications and experience of a proposed replacement immediately available for Work; and
- (B) security information on the proposed replacement as specified by Canada, if applicable.

The replacement must have qualifications and experience that meet or exceed those obtained for the original resource.

- (ii) Subject to an Excusable Delay, where Canada becomes aware that a specific individual identified under the Contract to provide services has not been provided or is not performing, the Contracting Authority may elect to:
- (A) exercise Canada's rights or remedies under the Contract or at law, including terminating the Contract in whole or in part for default under the Article titled "Default of the Contractor", or
- (B) assess the information provided under (c) (i) above or, if it has not yet been provided, require the Contractor to propose a replacement to be rated by the Technical Authority. The replacement must have qualifications and experience that are similar or exceed those obtained for the original resource and be acceptable to Canada. Upon assessment of the replacement, Canada may accept the replacement, exercise the rights in (ii) (A) above, or require another replacement in accordance with this sub-article (c).

---

Where an Excusable Delay applies, Canada may require (c) (ii) (B) above instead of terminating under the "Excusable Delay" Article. An Excusable Delay does not include resource unavailability due to allocation of the resource to another Contract or project (including those for the Crown) being performed by the Contractor or any of its affiliates.

- (iii) The Contractor must not, in any event, allow performance of the Work by unauthorized replacement persons. The Contracting Authority may order that an original or replacement resource stop performing the Work. In such a case, the Contractor must immediately comply with the order. The fact that the Contracting Authority does not order a resource to stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.
- (iv) The obligations in this article apply despite any changes that Canada may have made to the Client's operating environment.

#### **7.21 Safeguarding Electronic Media**

- (a) Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.
- (b) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

#### **7.22 Representations and Warranties**

The Contractor made statements regarding its own and its proposed resources' experience and expertise in its bid that resulted in the award of the Contract and the issuance of TA's. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the Contract and adding work to it through TA's. The Contractor also represents and warrants that it has, and all its resources and subcontractors that perform the Work have, and at all times during the Contract Period they will have and maintain, the skills, qualifications, expertise and experience necessary to perform and manage the Work in accordance with the Contract, and that the Contractor (and any resources or subcontractors it uses) has previously performed similar services for other customers.

#### **7.23 Access to Canada's Property and Facilities**

Canada's property, facilities, equipment, documentation, and personnel are not automatically available to the Contractor. If the Contractor would like access to any of these, it is responsible for making a request to the Technical Authority. Unless expressly stated in the Contract, Canada has no obligation to provide any of these to the Contractor. If Canada chooses, in its discretion, to make its property, facilities, equipment, documentation or personnel available to the Contractor to perform the Work, Canada may require an adjustment to the Basis of Payment and additional security requirements may apply.

#### **7.24 Identification Protocol Responsibilities**

The Contractor will be responsible for ensuring that each of its agents, representatives or subcontractors (hereinafter referred to as Contractor Representatives) complies with the following self-identification requirements:

- (a) Contractor Representatives who attend a Government of Canada meeting (whether internal or external to Canada's offices) must identify themselves as Contractor Representatives prior to the

- 
- commencement of the meeting, to ensure that each meeting participant is aware of the fact that the individual is not an employee of the Government of Canada;
- (b) During the performance of any Work at a Government of Canada site, each Contractor Representative must be clearly identified at all times as being a Contractor Representative; and
  - (c) If a Contractor Representative requires the use of the Government of Canada's e-mail system in the performance of the Work, then the individual must clearly identify him or herself as an agent or subcontractor of the Contractor in all electronic mail in the signature block as well as under "Properties." This identification protocol must also be used in all other correspondence, communication, and documentation.
  - (d) If Canada determines that the Contractor is in breach of any obligation stated in this Article, upon written notice from Canada the Contractor must submit a written action plan describing corrective measures it will implement to eliminate the recurrence of the problem. The Contractor will have five working days to deliver the action plan to the Client and the Contracting Authority, and twenty working days to rectify the underlying problem.
  - (e) In addition to any other rights it has under the Contract, Canada may terminate the Contract for default if the corrective measures required of the Contractor described above are not met.

---

## ANNEX A

### Statement of Work

#### 1. Objectives

The Treasury Board of Canada Secretariat (TBS) Chief Information Officer Branch (CIOB) has a requirement for professional services on an “as and when required basis” for the services provided by IT Professionals in IT Security domain, to support the Government of Canada (GC)’s digital transformation program and to support the establishment of a consistent enterprise-wide security posture that enables the secure delivery of GC programs and services to Canadians and the public.

#### 2. Background

The Government of Canada (GC) is made up of more than 100 organizations that deliver a broad range of programs and services to individuals and businesses in Canada and abroad. Information Management (IM) and Information Technology (IT) support the government in providing these programs and services. Digital capabilities continue to transform the way individuals and businesses work and the GC is increasingly reliant on technology to deliver services to Canadians, individuals and businesses and to consume services from other sectors and partners. For Canadians, it is important to ensure a consistent end-user experience government-wide, regardless of geographical location. Issues of latency (delays in transmission), bandwidth, security, infrastructure, service levels and other considerations need to be taken into account in designing programs and services. The GC must adapt to meet demands and expectations from clients, stakeholders, partners and employees.

The GC has an ambitious agenda to become a digital government that is founded on the vision of services that are simple, seamless and digitally-enabled. Enabling a digital transformation requires the GC to adopt new approaches for the delivery of digital services. Disruptive technologies such as cloud computing can support this need for agility and flexibility, but this alternate service delivery model also introduces risks that must be appropriately mitigated to ensure the continued protection of GC information and IT assets.

The [GC Digital Operations Strategic Plan \(DOSP\)](#) outlines the following digital government vision:

*“The Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device.”*

Enabling this vision requires a strong foundation including modern technology, information stewardship and practices. The government must embrace the innovative and responsible use of new and emerging technologies while keeping in mind users, accessibility, security, privacy, and good data stewardship and information management requirements. The “Secure and trusted” pillar focuses on safeguarding sensitive government data, ensuring that the systems underpinning digital services are properly designed and secured, and that Canadians accessing online services can trust the government with their personal information. The DOSP also identifies detailed key strategic actions for the GC that help to enable and transform the GC. These initiatives will help the GC manage risks related to cyber security and aging IT through the implementation of proactive measures to reduce the threat surface of Internet-connected networks and improved controls over access to government-held information. This plan also highlights an enterprise approach which means that the size and complexity of IT-enabled projects are increasing as we move toward a more horizontal delivery model. In support of the enterprise approach, a new GC Enterprise Architecture Review Board (EARB) has been established to further the “whole of government as one enterprise” vision. It is integrated into the larger GC governance structure and looks at alignment

of initiatives, system and solution gaps and overlaps, development of new digital capabilities and innovation opportunities, setting technology standards and providing IM/IT investment direction.

Within this context, TBS is seeking professional services resources to meet the increasing demands for Cyber Security support, not only to address the actions outlined within the existing strategic plan, but also to support strategy development as the GC prepares to develop a larger digital policy.

### **3. Scope of Work**

The Contractor is required to provide informatics professional services to TBS for the following programs to provide cyber security and digital services support on an “as and when requested” basis through Task Authorizations (TAs).

#### **Workstream 1 – Strategy & Design**

##### **GC Cyber Security Strategy and Design**

- Scope:
  - Develop strategies, roadmaps, architectures, and designs that align with GC business objectives.
  - Issue direction and guidance to enable whole-of-government approach.
  - Provide expertise and strategic oversight for the implementation of effective and efficient GC cyber security practices.
  - Engage with partners (across jurisdictions) to ensure execution of strategic vision.
- Functions include but are not limited to:
  - Develop IT security strategies to improve GC IT security posture (e.g. Digital Operations Strategic Plan – SECURE and TRUSTED pillar);
  - Develop enterprise cyber and IT security reference architectures, design patterns (e.g. blueprints), and requirements to integrate security into enterprise GC IT systems;
  - Develop reusable artifacts, tools and templates for departments to standardize IT security practices GC-wide;
  - Develop IT security standards that support Treasury Board policy instruments and future digital policy;
  - Review project artifacts (architectures, risk registers, etc.) to confirm appropriate level of security is embedded into enterprise projects before they are put into production;
  - Ensure that enterprise IT services achieve an appropriate level of security before they enter operations (in support of GC CIO role as security “authorizer” of enterprise applications);
  - Support for various enterprise security architecture focus areas including data security, endpoint security, application security, compute and storage services security, and security operations.

##### **GC Digital Identity**

- Scope:
  - Lead the GC Digital Identity Strategy with a vision of an open identity-proofing context
  - Lead GC contributions to the Pan-Canadian Trust Framework
  - Develop GC strategy, roadmap, architecture, and designs for digital identity
- Functions include but are not limited to:
  - Design & lead procurement of Sign In Canada

- 
- Business owner and program lead for implementation of GCpass (centralized authentication service for GC employees)
  - Develop IT security strategies to enabling GC Digital Identity program as outlined in the Digital Operations Strategic Plan
  - Lead transformation of GC file/email encryption and digital (electronic) signature capabilities to increase security, modernize processes and reduce costs
  - Develop application integration strategies that will enable seamless adoption of GC Digital Identity components within GC enterprise and departmental applications

## **Workstream 2 – Security Assurance**

### **IT Security Risk Management**

- Scope:
  - Perform IT security risk management including support for security assessment and authorization of information systems solutions
  - Provide security and privacy advice and guidance for projects
  - Support continuous monitoring activities of authorized systems.
- Functions include but are not limited to:
  - Perform analysis and develop business requirements in support of information system development and integration of security and privacy
  - Review project artifacts (architectures, risk registers, etc.) to confirm appropriate level of security is embedded into projects before they are put into production;
  - Ensure that enterprise departmental IT services achieve an appropriate level of security before they enter operations
  - Verify that security safeguards have been implemented correctly and that assurance requirements have been met. This includes confirming that the system has been properly configured, and establishing that the safeguards meet applicable standards.
  - Conduct security testing and evaluation (ST&E) to determine if the technical safeguards are functioning correctly.
  - Conduct privacy analysis to provide evidence of compliance with privacy principles and to identify privacy risks

## **4. Personnel Requirements**

### **Workstream 1 – Strategy & Design**

<b>RESOURCE CATEGORY</b>	<b>Level</b>
C.2 IT Security Methodology, Policy and Procedures Analyst	3
C.3 IT Security TRA and C&A Analyst	3
C.7 IT Security Design Specialist (General Stream)	3
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	3
P.12 Risk Management Specialist	3
B.1 Business Analyst	3
B.14 Technical Writer	3

## **Workstream 2 – Security Assurance**

<b>RESOURCE CATEGORY</b>	<b>Levels</b>
C.3 IT Security TRA and C&A Analyst	3
C.7 IT Security Design Specialist (General Stream)	3
C.11 IT Security VA Specialist	3
C.16 PIA Specialist	3
P.9 Project Manager	3
B.1 Business Analyst	3
A.7 Programmer/Analyst	3

### **5. Tasks**

Each Task Authorization will identify the specific tasks to be conducted. The tasks apply to both Workstream 1 and Workstream 2.

The Contractor's resources may be required, but are not limited to, to perform the following:

#### **5.1 C.2 IT Security Methodology, Policy and Procedures Analyst (Level 3)**

- Review, analyze, and/or apply Federal, Provincial or Territorial Government IT Security methodologies, programs, policies, procedures, standards, guidelines, and IT Security Risk Management methodologies.
- Develop IT Security standards, procedures and guidelines pursuant to the requirements of The National Security Policy, Policy on Government Security, supporting operational standards (e.g., MITS), departmental/agency security policy, and other relevant standards, procedures and guidelines.
- Develop IT Security policy in the areas of IT security and assurance, standard Security Assessment and Authorization frameworks for IT systems, information infrastructure protection, product evaluation, privacy, Business Continuity Planning, contingency planning and Disaster Response Planning, Research & Development.
- Develop IT Security risk assessment methodologies for application to Government of Canada institutions.
- Develop and deliver training or presentation material relevant to the resource category.
- Analyze and develop documents such as a security requirements definition, a threat and risk assessment, and a privacy impact assessment.
- Prepare a concept of operations document that includes processes and methodologies that will support the architecture, development, implementation, of a transparent GC Enterprise Risk Management approach.

#### **5.2 C.3 IT Security TRA and C&A Analyst (Level 3)**

- Review, analyze, and/or apply Federal, Provincial or Territorial IT Security policies, System IT Security Assessment and Authorization processes, IT Security products, safeguards and best practices, and the IT Security risk mitigation strategies.
- Identify threats to, and vulnerabilities of operating systems (such as MS, Unix, Linux, and Novell), and wireless architectures.

- 
- Identify personnel, technical, physical, and procedural threats to and vulnerabilities of Federal, Provincial or Territorial IT systems.
  - Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings.
  - Conduct security assessment activities such as: Develop Security Assessment Plans, Verify that security safeguards meet the applicable policies and standards, Validate the security requirements by mapping the system-specific security policy to the functional security requirements, and mapping the security requirements through the various stages of design documents, Verify that security safeguards have been implemented correctly and that assurance requirement have been met. This includes confirming that the system has been properly configured, and establishing that the safeguards meet applicable standards, Conduct security testing and evaluation (ST&E) to determine if the technical safeguards are functioning correctly, Assess the residual risk provided by the risk assessment to determine if it meets an acceptable level of risk.
  - Conduct Authorization activities such as: Review of the security assessment results in the design review documentation by the Authorization Authority to ensure that the system will operate with an acceptable level of risk and that it will comply with the departmental and system security policies and standards and identify the conditions under which a system is to operate (for approval purposes). This may include the following types of approvals:
    - Developmental approval by both the Operational and the Authorization Authorities to proceed to the next stage in an IT system's life cycle development if sensitive information is to be handled by the system during development
    - Operational written approval for the implemented IT system to operate and process sensitive information if the risk of operating the system is deemed acceptable, and if the system is in compliance with applicable security policies and standards
    - Interim approval - a temporary written approval to process sensitive information under a set of extenuating circumstances where the risk is not yet acceptable, but there is an operational necessity for the system under development.
  - Support continuous monitoring activities of authorized systems.
  - Support development and evolution of GC Security Assessment and Authorization (SA&A) and its related governance.
  - Develop and deliver training material relevant to the resource category.
  - Develop and deliver presentation materials to support engagement with IT security practitioners, senior level executives, etc.
  - Development of Security Plans and process improvements.
  - Verify that security safeguards meet the applicable policies and standards
  - Validate security requirements by mapping the system-specific security policy to the functional security requirements, and mapping the security requirements through the various stages of design documents.
  - Verify that security safeguards have been implemented correctly and that assurance requirements have been met. This includes confirming that the system has been properly configured, and establishing that the safeguards meet applicable standards.
  - Conduct security testing and evaluation (ST&E) to determine if the technical safeguards are functioning correctly.
  - Develop and deliver SA&A training.
  - Contribute to improvement of GC SA&A framework.
-

---

### **5.3 C.7 IT Security Design Specialist (both General and ICAM Streams) (Level 3)**

- Review, analyze, and/or apply: Architectural methods, frameworks, and models such as TOGAF, US government FEAP, the Government of Canada Enterprise Security Architecture Program, Zachman, UMM.
- Review, analyze, and/or apply a broad range of security technologies including multiple types of systems and applications architectures, and multiple hardware and software platforms, including:
  - Directory Standards such as X.400, X.500, and SMTP
  - Operating Systems such as MS, Unix, Linux, and Novell
  - Networking Protocols (e.g., HTTP, FTP, Telnet)
  - Network routers, multiplexers and switches
  - Domain Name Services (DNS) and Network Time Protocols (NTP)
  - Cloud Infrastructure such as MS Azure, AWS
- Review, analyze, and/or apply Secure IT architectures, standards, communications, and security protocols such as IPSec, SSL, SSH, S-MIME, HTTPS.
- Review, analyze, and/or apply IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) stacks.
- Review, analyze, and/or apply the significance and implications of market and technology trends in order to apply them within architecture roadmaps and solution designs. (Examples: web services security, incident management, identity management).
- Review, analyze, and/or apply best practices and standards related to the concept of network zoning and defence in-depth principles.
- Review, analyze, and/or apply Identity, Credential, and Access Management practices, technologies and architectures.
- Analyze IT Security statistics, tools and techniques.
- Analyze security data and provide advisories and reports.
- Prepare technical reports such as requirement analysis, options analysis, technical architecture documents, mathematical risk modeling.
- Brief senior managers.
- Security architecture design and engineering support.
- Conduct data security designation/classification studies.
- Prepare tailored IT Security alerts and advisories from open and closed sources.
- Develop and deliver training material relevant to the resource category.
- Develop and deliver presentation materials to support engagement with IT security practitioners, senior level executives, etc.

### **5.4 C.11 IT Security VA Specialist (Level 3)**

- Review, analyze, and/or apply:
  - Threat agents analysis tools and other emerging technologies including privacy enhancement, predictive analysis, VoIP, data visualization and fusion, wireless security devices, PBX and telephony firewall
  - War dialers, password crackers
  - Public Domain IT vulnerability advisory services
  - Network scanners and vulnerability analysis tools such as SATAN, ISS, Portscan & NMap
  - Networking Protocols (HTTP, FTP, Telnet)
  - Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP
  - Wireless Security

- 
- Intrusion detection systems, firewalls and content checkers
    - Host and network intrusion detection and prevention systems - Anti-virus management
  - Identify threats to, and technical vulnerabilities of, networks.
  - Conduct on-site reviews and analysis of system security logs.
  - Collect, collate, analyze and disseminate public domain information related to networked computer threats and vulnerabilities, security incidents and incident responses.
  - Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings.
  - Develop and deliver training material relevant to the resource category.

#### **5.5 C.16. PIA Specialist (Level 3)**

- Review, analyze, and/or apply:
  - Treasury Board Privacy Impact Assessment Policy and Guidelines
  - Federal Privacy Act and Regulations
  - Treasury Board Privacy and Data Protection Policy
  - Personal Information Protection and Electronic Documents Act (PIPEDA)
  - GC IT/IM policies and guidelines
  - Government On-Line (GOL) initiatives
  - Secure Channel Network including its technical and business processes and service offerings
  - IT Security practices and principles
  - IT Security technological solutions
- Conduct privacy impact assessments (PIAs) and preliminary privacy impact assessments (PPIAs) of projects and concepts, in accordance with the requirements of:
  - Treasury Board Privacy Impact Assessment Policy
  - Treasury Board Privacy Impact Assessment Policy Guidelines
  - Other relevant standards, procedures and guidelines
- Analyze the flow of information using the PIA model provided by the client
- Conduct privacy analysis to provide evidence of compliance with privacy principles and to identify privacy risks
- Develop Privacy Risk Management Plans
- Develop recommendations as to possible privacy risk mitigation strategies
- Complete tasks directly supporting the departmental IT Security and Cyber Protection Program
- Develop and deliver training material relevant to the resource category

#### **5.6 P.9 Project Manager (Level 3)**

- Manage and coordinate the work and provide quality control oversight on all deliverables.
- Develop and maintain project work plans as directed by the Technical Authority (TA).
- Provide regular status reports, format and frequency to be defined in consultation with the TA.
- Request agenda items from the TA, prepare a consolidated agenda for regular progress meetings and prepare a record of discussion/decisions resulting from the progress meetings.
- Immediately notify the TA of any issue/problem that may impede, delay or negatively impact completion of deliverables.
- Ensure and maintain an electronic library of work in progress, delivered items and review comments, and version control thereof.
- Meet with the TA on a weekly basis, or as requested, to review the status of work performed.
- Ensure the project team adheres to all relevant security, safety and environmental regulations, rules and good practices.
- Manage several Project Managers, each responsible for an element of the project and its associated project team.

- 
- Manage the project during the development, implementation and operations startup by ensuring that resources are made available and that the project is developed and is fully operational within previously agreed time, cost and performance parameters.
  - Formulate statements of problems; establish procedures for the development and implementation of significant, new or modified project elements to solve these problems, and obtain approval thereof.
  - Define and document the objectives for the project; determine budgetary requirements, the composition, roles and responsibilities and terms of reference for the project team.
  - Report progress of the project on an ongoing basis and at scheduled points in the life cycle.
  - Meet in conference with stakeholders and other project managers and states problems in a form capable of being solved.
  - Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools.
  - Complete project sign-off.

#### **5.7 P.12 Risk Management Specialist (Level 3)**

- Conduct risk assessments
- Identify project risks and overall project risks
- Recommend alternative solutions, methodologies and strategies for risk mitigation and management
- Produce risk management plans
- Conduct risk assessments for troubled projects to quickly assess associated risks and recommend courses of action to minimize inherent risks
- Assist in prioritization and assignment of risks
- Assist in the development and/or implementation of Risk Management Plans
- Manage the implementation of Risk Management Plans to identify, analyze, plan, track and control project risks on a continuous basis throughout the project life cycle
- Coach, mentor and train project teams in risk mitigation techniques

#### **5.8 B.1 Business Analyst (Level 3)**

- Develop, review and manage business requirements.
- Plan, coordinate, capture and follow up on meetings for business requirements gathering along with their prioritization, associated business impact, costs/cost models and business dependencies.
- Perform analysis of the business requirements to identify and document roles and responsibilities.
- Perform analysis of the business requirements to identify and document information, procedures and decision flows, and associated policies.
- Capture the current use cases associated with the business requirements.
- Obtain and manage formal written approvals of the business requirements specification document.
- Establish acceptance test criteria with client.
- Support and use the selected departmental methodologies.
- Document, review with stakeholders and track actions and meeting decisions.
- Identify and document current state business processes (business or operations).
- Provide guidance to technical architects and developers to meet requirements.
- Develop presentations for stakeholders or senior executives.

- 
- Perform business analysis of functional requirements to identify information, procedures and decision flows.
  - Identify and evaluate existing procedures, methods, and items such as database content and structure.
  - Define and document interfaces of manual to automated operations within application subsystems, to external systems and between new and existing systems.
  - Work with various stakeholders and other sources to understand and identify all requirements information that is relevant to the project. Facilitate cross-functional meetings and exercises to verify current state, to capture requirements and to ensure Cyber project(s) alignment to existing transformation initiatives/ programs.
  - Plan and implement all requirements-related activities, including elicitation, validation, reporting status, resolving conflicts, and gaining approval.
  - Develop and manage detailed business and functional requirements for cyber project(s), by preparing use cases, data models, and capturing existing business rules from various forms of documentation such as process maps and interviews with subject matter experts. Organize, structure and understand the elicited requirements; putting them into an appropriate form, and performing necessary verification and validation on them.
  - Manage the requirements themselves, including requirements change control and scope control.
  - Assist in detailed design and development by maintaining "To-Be" process models, undertaking issues analysis and ensuring security and technical teams understand the underlying business objectives and functional capabilities required for project success.

#### **5.9 B.14 Technical Writer (Level 3)**

- Document help text, user manuals, technical documentation, web page content, etc.
- Review documentation standards and the existing project documentation.
- Determine documentation requirements and makes plans for meeting them.
- Gather information concerning the features and functions provided by the developers.
- Assess the audience for the documents/manuals which are required and prepare a statement of purpose and scope for each.
- Develop a table of content for each document/manual and write or edit the required content.
- Investigate the accuracy of the information collected by making direct use of the material being documented.
- Prepare or coordinate the preparation of any required illustrations and diagrams.
- Design the layout of the documents/manuals.
- Use word-processing, desk-top publishing and graphics software packages to produce final camera-ready copy.

#### **5.10 A.7 Programmer/Analyst (Level 3)**

- Create and modify code and software.
- Create and modify screens and reports.
- Develop code based upon design and requirements documents.
- Gather and analyze data for the conduct of studies to establish the technical and economic feasibility of proposed computer systems, and for the development of functional and system design specifications.
- Design methods and procedures for small computer systems, and sub-system of larger systems.
- Develop, test and implement small computer systems, and sub-systems of larger systems.
- Produce forms, manuals, programs, data files, and procedures for systems and/or applications.
- Specialties could include but are not limited to:
  - Animation Tools

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

- 
- ActiveX
  - ADS
  - ASP
  - BPWin
  - C/C++
  - CICS
  - Cloud development including but not limited to:
    - Working with Virtual Machines (VMs);
    - Templating VM images;
    - Configuring infrastructure of various cloud service providers;
    - Template infrastructure as code;
    - Configuration of VMs;
  - Cold Fusion
  - CORBA
  - Crystal Reports
  - CSS
  - Delphi
  - EbXML
  - ERWin
  - HCI
  - HML
  - HTML
  - IBM DB2
  - Identity, Credential and Access Management (ICAM) technologies including but not limited to:
    - FIDO 2.0;
    - Gluu;
    - OAuth;
    - OpenID Connect;
    - SAML;
    - U2F;
    - WebAuthn;
  - IDMS
  - Impromptu
  - IMS
  - Informix
  - Ingres
  - IoT Application development
  - J2EE
  - Java
  - JavaScript
  - JDBC
  - JSP
  - JQuery
  - Linux
  - Mobile Application Development
  - MongoDB
  - MIL-STD-498
  - MS Access

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

- 
- MS SQL
  - .NET
  - Netron/CAP
  - ODBC
  - OLAP
  - Oracle
  - Oracle CASE
  - Oracle Financials
  - Perl
  - PHP
  - Photoshop/Illustrator/Lightbox
  - PL/SQL
  - Power BI
  - PowerBuilder Rational Rose
  - Powershell
  - Python
  - R
  - RPG
  - Ruby
  - RUP
  - SAP
  - SQL Suite
  - Sybase
  - Tableau, Lumeria (and other data visualization tools)
  - TCP/IP
  - Unisys DBII
  - Unix
  - UX
  - Visual Basic
  - Visual C++
  - Web based Analytic tools
  - XML

## 6. Deliverables

Each Task Authorization will identify the specific deliverables and schedule the Contractor will be expected to produce and meet.

The deliverables may include, but are not limited to:

- Written documents and individual and group training for transfer of functional knowledge.
- Weekly status report submitted by each resource in the format specified in each TA.
- Monthly Progress Report submitted by the Contractor. At a minimum, progress reports shall contain the following information:
  - All activities performed by the Contractor(s) during the period;
  - Status of all action/decision items, as well as a list of outstanding activities;
  - A description of any problems encountered which are likely to require the attention of the Technical Authority, and any recommendations relating to the conduct of the work;
  - Current milestones with planned dates, progress since last report, issues encountered, and next steps;

- 
- Hours expended by the Contractor against the tasks during the reporting period;
  - Expectations/deliverables for the coming month and quarter.

## **7. Method of Acceptance**

The Contractor must provide the deliverables (in draft, final or both forms) to the Technical Authority or their representative as specified in each TA. The scope and specific content of each deliverable will be submitted to the Technical Authority for review and to determine acceptance.

The final copies of the deliverables must incorporate the comments received and changes requested by the Technical Authority or their representative and will be delivered on or before the end date specified in each TA.

## **8. Format of Deliverables**

The schedule, format and content of each deliverable will be specified in each TA.

Documentation deliverables shall be in hard copy format and electronic copy format using Microsoft (MS) Office suite of products, or as specified in each TA.

Progress Reports must be submitted to the Technical Authority by email.

Unclassified and Protected-A documents can be submitted by email within the GC email system. Protected-B documents must be encrypted using GC-approved encryption means as prescribed by the Technical Authority then can be submitted within the GC email system. Secret documents (if applicable) must include one hard copy and one copy in electronic format (CD, DVD, or USB) and shall be hand delivered to the Technical Authority.

Electronic copy of the deliverables must be editable in Microsoft Office Suite (e.g., Word, Excel, PowerPoint and Visio) version 2007 or newer.

## **9. Constraints**

### **9.1 Regular Meetings**

The Contractor is required to meet with the Technical Authority or their representative as requested to discuss any issues associated with the provision of the required services.

### **9.2 Working Hours**

Normal working hours will be between 7:00 am and 6:00 pm Monday through Friday (with the exception of statutory holidays as defined by the province of work). The Contractor will be expected to work 7.5 hours/day within normal working hours, unless arrangements are made ahead of time with the approval of the Technical Authority. All resources must be available to work outside normal working hours as required.

## **10. Work location**

The majority of the work will be performed on site at TBS offices located in the National Capital Region but on occasion remote access may be permitted or required at the Technical Authority's discretion. Each Task Authorization will identify the work location(s). In the cases where the work is performed remotely, the resource(s) must be available for teleconference.

The Contractor is required to attend meetings at TBS and at the locations of Key GC Stakeholders. Occasional travel may be required.

A TA could require that work be performed off-site on infrastructure provided by the Contractor.

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

### **11. Language of Work**

The language of work is English. Translation of any deliverables will be the responsibility of the Technical Authority.

---

## APPENDIX A TO ANNEX A

### TASKING ASSESSMENT PROCEDURE

1. Where a requirement for a specific task is identified, a draft Task Authorization Form (TA Form) as attached at Appendix B to Annex A will be provided to the Contractor [in accordance with the allocation methodology stated in the Contract Article titled "Allocation of Task Authorizations".] Once a draft TA Form is received, the Contractor must submit to the Technical Authority a quotation of rates to supply the requested Resource Categories based on the information identified in the TA Form, as well as its corresponding proposed resource(s). The quotation must be signed and submitted to Canada within the time for response identified in the TA Form. The Contractor will be given a minimum of 2 working days (or any longer time period specified in the draft TA) turnaround time to submit a quotation.
2. With each quotation the Contractor must propose the required number of resources and for each proposed resource the Contractor must supply a résumé, the requested security clearance information and must complete the Response Tables at Appendix C of Annex A applicable to the Resource Categories identified in the draft TA. The same individual must not be proposed for more than one Resource Category. The résumés must demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to the proposed resources:
  - (i) Proposed resources may be employees of the Contractor or employees of a subcontractor, or these individuals may be independent contractors to whom the Contractor would subcontract a portion of the Work. (Refer to Appendix D to Annex A, Certifications).
  - (ii) For educational requirements for a particular degree, designation or certificate, Canada will only consider educational programmes that were successfully completed by the resource before the date the draft TA was first issued to the Contractor.
  - (iii) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of draft TA issuance and must continue, where applicable, to be a member in good standing of the profession or membership throughout the assessment period and Contract Period. Where the designation or membership must be demonstrated through a certification, diploma or degree, such document must be current, valid and issued by the entity specified in this Contract or if the entity is not specified, the issuer must have been an accredited or otherwise recognized body, institution or entity at the time the document was issued.
  - (iv) For work experience, Canada will not consider experience gained as part of an educational programme, except for experience gained through a formal co-operative programme at a post-secondary institution.
  - (v) For any requirements that specify a particular time period (e.g., 2 years) of work experience, Canada will disregard any information about experience if the résumé does not include the relevant dates (month and year) for the experience claimed (i.e., the start date and end date). Canada will evaluate only the duration that the resource actually worked on a project or projects (from his or her start date to end date), instead of the overall start and end date of a project or a combination of projects in which a resource has participated.
  - (vi) A résumé must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. Only listing experience without providing any supporting data to describe responsibilities, duties and

---

relevance to the requirement, or reusing the same wording as the TA Form, will not be considered "demonstrated" for the purposes of the assessment. The Contractor should provide complete details as to where, when, month and year, and how, through which activities/responsibilities, the stated qualifications / experience were obtained. In situations in which a proposed resource worked at the same time on more than one project, the duration of any overlapping time period will be counted only once toward any requirements that relate to the individual's length of experience.

3. The qualifications and experience of the proposed resources will be assessed against the requirements set out in Appendix C to Annex A to determine each proposed resource's compliance with the mandatory and rated criteria. Canada may request proof of successful completion of formal training, as well as reference information. Canada may conduct reference checks to verify the accuracy of the information provided. If reference checks are done, they will be conducted in writing by e-mail (unless the contact at the reference is only available by telephone). Canada will not assess any points or consider a mandatory criterion met unless the response is received within 5 working days. On the third working day after sending out the e-mails, if Canada has not received a response, Canada will notify the Contractor by e-mail, to allow the Contractor to contact its reference directly to ensure that it responds to Canada within 5 working days. Wherever information provided by a reference differs from the information supplied by the Contractor, the information supplied by the reference will be the information assessed. Points will not be allocated or a mandatory criteria considered as met if the reference customer is not a customer of the Contractor itself (for example, the customer cannot be the customer of an affiliate of the Contractor). Nor will points be allocated or a mandatory criteria considered as met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Contractor. Crown references will be accepted.
4. During the assessment of the resources proposed, should the references for two or more resources required under that TA either be unavailable or fail to substantiate the required qualifications of the proposed resources to perform the required services, the Contractor's quotation may be found to be non-responsive.
5. Only quotations that meet all of the mandatory criteria will be considered for assessment of the point rated criteria. Each resource proposed must attain the required minimum score for the point rated criteria for the applicable Resource Category. If the minimum score for any proposed resource is less than what is required, the Contractor's quotation will be found to be non-responsive.
6. Once the quotation has been accepted by the Technical Authority, the TA Form will be signed by Canada and provided to the Contractor for signature. The TA Form must be appropriately signed by Canada prior to commencement of any work. The Contractor must not commence work until a validly issued TA Form (the Task Authorization) has been received, and any work performed in its absence is done at the Contractor's own risk.

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

## **APPENDIX B TO ANNEX A**

### **TASK AUTHORIZATION FORM**



## TASK AUTHORIZATION FORM FORMULAIRE D'AUTORISATION DE TÂCHES

**PART 1** (completed by the Technical/Project Authority) / **PARTIE 1** (complété par le Responsable technique / Chargé du projet)

### A. General Information / Informations générales

Contract Number / Numéro du contrat :

Contractor Name / Nom du Contracteur :

Task Authorization (TA) No.  
N° de l'autorisation de tâches (AT) :

Commitment No.  
N° de l'engagement :

Financial Coding  
Code financier :

Date of Issuance  
Date d'émission :

Response required by  
Réponse requise  
d'ici le :

### B. For Amendments Only / Aux fins de modification seulement

Amendment No. / N° de la modification :

Reason for the Amendment / Raison pour la modification :

### C. TA Requirements / Exigences relatives à l'AT

Required Resource(s) / Ressource(s) requise(s)

Category and Level Catégorie et Niveau	Estimated Level of Effort (days) / Niveau d'effort estimatif (jours)	Linguistic Profile / Profile linguistique	Required Level(s) of Security / Niveau(x) de sécurité requis

Statement of Work (tasks, deliverables, reports, etc.) / Énoncé des travaux (tâches, livrables, rapports, etc.)

See attached / Voir pièce jointe

### Period of Services / Période de service:

Initial Start Date / Date de début initiale :

Initial End Date / Date de fin initiale :

Extended End Date (See Reason for the Amendment) / Date de fin prolongée (voir Raison pour la modification):

☐ Option To Extend Initial End Date / Option pour prolonger la date de fin initiale

Optional End Date(s) / Date(s) de fin optionnelle(s)	Status / Statut
	<input type="radio"/> In Effect / en vigueur

Travel Requirement(s) / Exigence(s) de voyage :

Work Location(s) / Lieu(x) de travail :

**PART 2** (completed by the Contractor and/or the Technical/Project Authority) / **PARTIE 2** (complété par le Contracteur et/ou le Responsable technique / Chargé du projet)

### Contractor Resource(s) and Estimated Cost / Ressource(s) du Contracteur et Coût total estimatif

Note: once approved, only the following resources may provide services under this TA. / Nota : une fois approuvée, seules les ressources suivantes peuvent fournir des services sous la présente AT

Name / Nom Category and Level / Catégorie et Niveau	PWGSC Security File No. / N° du dossier de sécurité TPSGC	Linguistic Profile / Profil linguistique	Per Diem Rate / Taux journalier	Estimated Level of Effort (days) / Niveau d'effort estimatif (jours)	Total Estimated Cost / Coût total estimatif

Estimated Cost / Coût estimatif					
Total Estimated Travel and Living Cost / Coût total estimatif de voyage et de vie					
Total Estimated Cost / Coût total estimatif					
Check applicable Basis of Payment / Cocher la Base de Paiement applicable :		Maximum Price / Prix Maximum :	<input type="checkbox"/>	Firm Price / Prix Ferme :	<input type="checkbox"/>

### PART 3 - TA APPROVAL BY CANADA / PARTIE 3 - APPROBATION DE L'AT PAR LE CANADA

By signing this TA, the authorized client authority and/or the PWGSC Contracting Authority certify(ies) that the content of this TA is in accordance with the conditions of the Contract.		En apposant sa signature sur l'AT, le client autorisé et/ou l'autorité contractante de TPSGC atteste(nt) que le contenu de cette AT est conforme aux conditions du contrat.	
The client's authorization limit is \$300,000. When the value of a TA and its amendments (excluding Applicable Taxes) is in excess of this limit, the TA must be signed by the authorized client and forwarded to the PWGSC Contracting Authority for authorization.		La limite d'autorisation du client est \$300,000. Lorsque la valeur de l'AT et ses modifications (excluant les taxes applicables) dépasse cette limite, l'AT doit être signée par le client autorisé et transmise à l'autorité contractante de TPSGC pour autorisation	
Name of Technical Authority / Nom de l'autorité technique	Date	Name of Contracting Authority / Nom de l'autorité contractante	Date
Signature		Signature	
[If applicable, insert the following] Name of the representative from (insert the Department name) [Ajouter ce qui suit, s'il y a lieu] Nom du représentant de (insérer le nom du Ministère)		Date	
Signature			

### PART 4 - CONTRACTOR SIGNATURE / PARTIE 4 - SIGNATURE DU CONTRACTEUR

Name and Title of individual authorized to sign on behalf of the Contractor / Nom et titre Signature de la personne autorisée à signer au nom de l'entrepreneur		Signature	Date
--	--	-----------	------

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

## **APPENDIX C TO ANNEX A**

### **RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLE**

To facilitate resource assessment, Contractors must prepare and submit a response to a draft Task Authorization using the tables provided in this Annex. When completing the resource grids, the specific information which demonstrates the requested criteria and reference to the page number of the résumé should be incorporated so that Canada can verify this information. The tables should not contain all the project information from the resume. Only the specific answer should be provided.

## **Workstream 1 – Strategy & Design**

### **RESOURCE MANDATORY REQUIREMENT**

#### **1. C.2 IT Security Methodology, Policy and Procedures Analyst, Level 3**

<b>Resource Name:</b>		
<b>Criteria</b>	<b>Mandatory Requirement</b>	<b>Demonstrated Experience</b> (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the last twelve (12) years prior to TA issuance date in the development of IT security methodologies, IT security policies and/or procedures, or IT standards and/or guidelines in at least two (2) of the following areas:</p> <ul style="list-style-type: none"><li>i. Cloud security</li><li>ii. Security and Risk Management</li><li>iii. Endpoint Security</li><li>iv. Communications &amp; Network Security</li><li>v. Identity &amp; Access Management</li><li>vi. Security Operations</li><li>vii. Software Development and Application Security</li></ul> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months.</p>	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has demonstrated experience in at least two (2) projects in developing IT security policy or related policy instruments for a large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a large commercial client. Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration and performed within the last five (5) years prior to the TA issuance date.</p>	

#### **2. C.3 IT Security TRA and C&A Analyst, Level 3**

<b>Resource Name:</b>		
<b>Criteria</b>	<b>Mandatory Requirement</b>	<b>Demonstrated Experience</b> (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the last twelve (12) years prior to TA issuance date in performing IT Security Threat Risk</p>	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
	<p>Analysis (TRA) and/or Certification and Accreditation or Security Assessment and Authorization (SA&amp;A).</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of five (5) years of demonstrated experience in the last eight (8) years prior to TA issuance date in the assessment of applied IT security controls, or the evaluation of threats and risks, or the interpretation and application of ITSG-33 IT Security Risk Management Framework, for complex*, enterprise-wide applications or information system.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p> <p>* Complex is defined as a group of interacting, interrelated systems.</p>	

**3. C.7 IT Security Design Specialist (General Stream), Level 3**

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the last twelve (12) years prior to the TA issuance date, planning, developing and implementing IT security architectures or IT security designs for complex*, enterprise-wide applications or information system, in at least two (2) of the following areas:</p> <ul style="list-style-type: none"><li>i. Cloud security</li><li>ii. Security and Risk Management</li><li>iii. Endpoint Security</li><li>iv. Communications &amp; Network Security</li><li>v. Identity &amp; Access Management</li><li>vi. Security Operations</li><li>vii. Software Development and Application Security</li></ul> <p>* Complex is defined as a group of interacting, interrelated systems.</p>	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
	To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of three (3) years of demonstrated experience in the last six (6) years prior to TA issuance date with the development and delivery of IT security strategies, white papers, standards, solutions/proposals to solving IT and security problems affecting multiple stakeholders and security architectures.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	
<b>M3</b>	<p>The Contractor must clearly demonstrate that the proposed resource has demonstrated combined experience in at least two (2) projects, having developed at least three (3) of the following types of system engineering artifacts:</p> <ul style="list-style-type: none"><li>a) Architecture documents;</li><li>b) System Requirements Specifications;</li><li>c) System Design Specifications;</li><li>d) Build / Configuration documents;</li><li>e) Concept of Operations (ConOps);</li><li>f) System Implementation Plans;</li><li>g) Test Plans/Test Reports; and</li><li>h) Life Cycle Support Plans</li></ul> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	

**4. C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM)), Level 3**

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	The proposed resource must have a minimum of three (3) years of experience in the last five (5) years prior to the TA issuance date developing ICAM architectures and processes.	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
	To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	
<b>M2</b>	<p>The proposed resource must have a minimum of two (2) years of experience in the last five (5) years developing ICAM architectures and processes for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.</p> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	
<b>M3</b>	The proposed resource must have experience writing technical documents. Specifically, the resource must have been one of the primary authors of at least five (5) technical documents, each consisting of at least 20 pages. Document title and length must be listed for at least five (5) such documents in the proposed resource's CV. In addition, high-level descriptions, including the number of pages of the documents must be provided.	
<b>M4</b>	The proposed resource must have a university degree in a computer-related discipline (e.g., Computer Science or Computer Engineering) or a college diploma in a Computer-related discipline with a minimum of fifteen (15) years of experience in the computer industry since graduation.	

#### 5. P.12 Risk Management Specialist, Level 3

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	<p>The Contractor must demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"><li>• Chartered Professional Accountant (CPA)</li><li>• Chartered Accountant (CA)</li><li>• Certified Management Accountant (CMA)</li><li>• Certified General Accountant (CGA)</li></ul>	

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
	A copy of the certification must be provided with the proposal.	
<b>M2</b>	<p>The Contractor must demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"> <li>• ICS2 Certified Information System Security Professional (CISSP)</li> <li>• Certified Information Systems Auditor (CISA)</li> </ul> <p>A copy of the certification must be provided with the proposal.</p>	
<b>M3</b>	<p>The Contractor must clearly demonstrate that the proposed resource has at least 2 years' experience in the last 5 years prior to the TA issuance date conducting IT security controls assessments (including production of third-party assessment reports) and providing advice on IT security controls for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.</p> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of six (6) consecutive months in duration.</p>	

#### 6. B.1 Business Analyst, Level 3

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of experience in the past twelve (12) years prior to the TA issuance date in developing business strategies and processes as a Business Analyst.	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has experience working as a Business Analyst on a minimum of one (1) IT security related projects for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client, performing at least three (3) of the following tasks:</p> <ul style="list-style-type: none"><li>• Defining business strategies in support of transformation and change management activities.</li><li>• Developing and documenting statements of requirements for considered alternatives.</li><li>• Performing business analyses of functional requirements to identify information, procedures, and decision flows.</li><li>• Evaluating existing procedures and methods, identifying and documenting items such as database content, structure, application subsystems.</li><li>• Defining and documenting interfaces between external and internal systems, or new and existing systems.</li><li>• Establishing acceptance test criteria with client.</li><li>• Supporting and using the selected departmental methodologies.</li></ul> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

**7. B.14 Technical Writer, Level 3**

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	The Contractor must clearly demonstrate that the proposed resource has a minimum of 10 years of combined experience in the last twelve (12) years prior to the TA issuance date as a Technical Writer for an information technology project or program.	
<b>M2</b>	The Contractor must clearly demonstrate that the proposed resource has experience writing large technical documents. Specifically, the resource must have been one of the primary authors of at least 5 technical documents, each consisting of at least 50 pages. Document title and length must be listed for at least 5 such documents in the proposed resource's résumé.	

## RESOURCE RATED REQUIREMENTS

### 1. C.2 IT Security Methodology, Policy and Procedures Analyst, Level 3

Criteria	Rated Requirement	Demonstrated Experience	Max Available Points	Points Received
<b>R1</b>	<p>The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.</p> <p>The additional years of experience is not required to fall within the past 12 years.</p>	<p>1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points</p>	5	
<b>R2</b>	<p>The Contractor should demonstrate the proposed resource's project experience in the development of IT security methodologies, IT security policies and/or procedures, or IT standards and/or guidelines in the financial services sector.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>0 projects = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points</p>	10	
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource, has a minimum of 6 months of project experience within the last 5 years prior to the TA issuance date with direct working knowledge of the Government of Canada standards, policies and guidelines and the principles of security and privacy by design.</p> <p>To qualify, the demonstrated experience must include acquired experience focused on IT Security service delivery as guided or aligned to the standards and policies published by Treasury Board of Canada Secretariat, Royal Canadian Mounted Police, Communication Security Establishment Canada, or the Canadian Centre for Cyber Security.</p> <p>A maximum of 4 projects is to be submitted. If more than 4 projects are submitted, only the first 4 projects will be evaluated.</p>	<p>1 point for each policy, directive, standard or guideline listed, for a maximum of 10 points.</p>	10	
<b>R4</b>	<p>The Contractor should demonstrate that the proposed resource holds a current and valid ICS2 Certified Information System Security Professional (CISSP) Certification.</p>	<p>No certification = 0 points CISSP Certification = 15 points</p>	15	

Criteria	Rated Requirement	Demonstrated Experience	Max Available Points	Points Received
	A copy of the certification must be provided with the proposal.			
<b>R5</b>	<p>The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"> <li>• Certified Cloud Security Professional (CCSP)</li> <li>• Certified Information Security Manager (CISM)</li> <li>• Certified Information Systems Auditor (CISA)</li> <li>• Certified in Risk and Information Systems Control (CRISC)</li> <li>• Certified Cyber Forensics Professional (CCFP)</li> <li>• Systems Security Certified Professional (SSCP)</li> <li>• Information Technology Infrastructure Library (ITIL)</li> <li>• Information Systems Security Architecture Professional (ISSAP)</li> <li>• CompTIA Security+</li> <li>• GIAC (Global Information Assurance Certification)</li> <li>• SABSA Chartered Security Architect Foundation (SCF) or higher</li> </ul> <p>A copy of the certification must be provided with the proposal.</p>	<p>0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points</p>	10	
<b>Maximum Points</b>			<b>50</b>	
<b>Minimum Required Points</b>			<b>25</b>	
<b>Total Points Received</b>				

## 2. C.3 IT Security TRA and C&A Analyst, Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	<p>The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.</p> <p>The additional years of experience is not required to fall within the past 12 years.</p>	<p>1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points</p>	5	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R2</b>	<p>The Contractor should demonstrate that the proposed resource has experience developing and documenting information system security assurance processes, guidance, or policies for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.</p> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points</p>	10	
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has recent (within last 7 years prior to TA issuance date) project experience validating the following:</p> <ol style="list-style-type: none"> <li>1. IT security controls (ITSG-33 based) and applicable safeguards</li> <li>2. Assessment of mitigation strategies</li> <li>3. Assessment of residual risk</li> </ol> <p>A maximum of 4 projects is to be submitted. If more than 4 projects are submitted, only the first 4 projects will be evaluated.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>1 project – 2 points 2 projects – 5 points 3 projects – 7 points 4 projects – 10 points</p>	10	
<b>R4</b>	<p>The Contractor should demonstrate that the proposed resource has experience in developing and delivering training on IT security risk management methodologies such as ITSG-33 IT Security Risk Management Framework.</p>	<p>2 points per training course up to a maximum of 5 courses</p>	10	
<b>R5</b>	<p>The Contractor should demonstrate that the proposed resource holds a current and valid ICS2 Certified Information System Security Professional (CISSP) Certification.</p> <p>A copy of the certification must be provided with the proposal.</p>	<p>No certification = 0 points CISSP Certification = 15 points</p>	15	
<b>R6</b>	<p>The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"> <li>• Certified Cloud Security Professional (CCSP)</li> </ul>	<p>0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points</p>	10	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<ul style="list-style-type: none"> <li>• Certified Information Security Manager (CISM)</li> <li>• Certified Information Systems Auditor (CISA)</li> <li>• Certified in Risk and Information Systems Control (CRISC)</li> <li>• Certified Cyber Forensics Professional (CCFP)</li> <li>• Systems Security Certified Professional (SSCP)</li> <li>• Information Technology Infrastructure Library (ITIL)</li> <li>• Information Systems Security Architecture Professional (ISSAP)</li> <li>• CompTIA Security+</li> <li>• SABSA Chartered Security Architect Foundation (SCF) or higher</li> </ul> <p>A copy of the certification must be provided with the proposal.</p>			
<b>Maximum Points</b>			<b>60</b>	
<b>Minimum Required Points</b>			<b>30</b>	
<b>Total Points Received</b>				

### 3. C.7 IT Security Design Specialist (General Stream), Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	<p>The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.</p> <p>The additional years of experience is not required to fall within the past 12 years.</p>	<p>1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points</p>	5	
<b>R2</b>	<p>The Contractor should demonstrate that the proposed resource has recent (within last 7 years prior to the TA issuance date) combined experience performing all of the following IT Security tasks:</p> <p>1. Analysis of IT Security tools and techniques</p>	<p>24 to 30 months = 2 points  &gt;30 to 36 months = 4 points  &gt;36 to 42 months = 6 points</p>	10	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<p>2. Analysis of security data and provision of advisories and reports</p> <p>3. Preparation of technical reports such as requirement analysis, options analysis, technical architecture documents, mathematical risk modeling</p> <p>4. Security architecture design and engineering support</p> <p>Reference projects do not require all listed tasks to qualify.</p> <p>A maximum of 6 projects is to be submitted. If more than 6 projects are submitted, only the first 6 projects will be evaluated.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>&gt;42 to 48 months = 8 points</p> <p>&gt;48 months = 10 points</p>		
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has recent (within last 7 years prior to TA issuance date) experience designing/architecting/engineering IT security components and architectures for enterprise solutions and/or coordinating development of design solutions across multiple teams for solving IT security problems involving multiple stakeholders, while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) guidelines.</p> <p>To qualify, an enterprise solution is considered to be a system that supports 4,000 users or more.</p> <p>A maximum of 6 projects is to be submitted. If more than 6 projects are submitted, only the first 6 projects will be evaluated.</p> <p>To qualify, the resource must have worked on the referenced projects for</p>	<p>24 to 30 months = 2 points</p> <p>&gt;30 to 36 months = 4 points</p> <p>&gt;36 to 42 months = 6 points</p> <p>&gt;42 to 48 months = 8 points</p> <p>&gt;48 months = 10 points</p>	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	a minimum of four (4) consecutive months in duration.			
<b>R4</b>	The Contractor should demonstrate that the proposed resource holds a current and valid ICS2 Certified Information System Security Professional (CISSP) Certification.  A copy of the certification must be provided with the proposal.	No certification = 0 points  CISSP Certification = 15 points	15	
<b>R5</b>	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications: <ul style="list-style-type: none"> <li>• Certified Cloud Security Professional (CCSP)</li> <li>• Certified Information Security Manager (CISM)</li> <li>• Certified Information Systems Auditor (CISA)</li> <li>• Certified in Risk and Information Systems Control (CRISC)</li> <li>• Certified Cyber Forensics Professional (CCFP)</li> <li>• Systems Security Certified Professional (SSCP)</li> <li>• Information Technology Infrastructure Library (ITIL)</li> <li>• Information Systems Security Architecture Professional (ISSAP)</li> <li>• CompTIA Security+</li> <li>• GIAC (Global Information Assurance Certification)</li> <li>• SABSA Chartered Security Architect Foundation (SCF) or higher</li> </ul> A copy of the certification must be provided with the proposal.	0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points	10	
<b>Maximum Points</b>			<b>50</b>	
<b>Minimum Required Points</b>			<b>25</b>	
<b>Total Points Received</b>				

**4. C.7 IT Security Design Specialist (ICAM Stream), Level 3**

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	The proposed resource should have experience developing identity management architectures and processes in the last five (5) years prior to the TA issuance date for large organizations of more than 40,000 users.	10 points/year	50	
<b>R2</b>	<p>The proposed resource should have experience developing identity management architectures and processes in the last five (5) years for enterprises with highly autonomous sub-units.</p> <p>Sub-units are considered highly autonomous if they have independent decision-making authority and are only loosely bound to a central decision-making authority at the enterprise level. For example, departments within the Federal Government of Canada have significant autonomy in relation to the central policy authorities.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	5 points/year	25	
<b>R3</b>	<p>The proposed resource should have demonstrated experience with any of the following technologies in the last five (5) years prior to the TA issuance date:</p> <ul style="list-style-type: none"> <li>• SAML;</li> <li>• OpenID Connect;</li> <li>• OAuth;</li> <li>• FIDO;</li> <li>• 201 (PIV) cards;</li> <li>• Directory Services (DS); and,</li> <li>• Identity management (IDM) suite of products and technologies.</li> </ul>	<p>SAML, OpenID Connect, OAuth or FIDO – 2 points per year</p> <p>PIV or DS – 1 point per year</p> <p>IDM – 3 points per year</p>	65	
<b>R4</b>	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:	<p>0 certifications = 0 points</p> <p>1 certification = 2 points</p>	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<ul style="list-style-type: none"> <li>ICS2 Certified Information System Security Professional (CISSP)</li> <li>Certified Cloud Security Professional (CCSP)</li> <li>Certified Information Security Manager (CISM)</li> <li>Certified Information Systems Auditor (CISA)</li> <li>Certified in Risk and Information Systems Control (CRISC)</li> <li>Certified Cyber Forensics Professional (CCFP)</li> <li>Systems Security Certified Professional (SSCP)</li> <li>Information Technology Infrastructure Library (ITIL)</li> <li>Information Systems Security Architecture Professional (ISSAP)</li> <li>CompTIA Security+</li> <li>GIAC (Global Information Assurance Certification)</li> <li>SABSA Chartered Security Architect Foundation (SCF) or higher</li> </ul> <p>A copy of the certification must be provided with the proposal.</p>	<p>2-3 certifications = 5 points 4 or more certifications = 10 points</p>		
Maximum Points			150	
Minimum Required Points			75	
Total Points Received				

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

**5. P.12 Risk Management Specialist, Level 3**

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	<p>The Contractor should demonstrate that the proposed resource has experience conducting System and Organization Controls (SOC) audits for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.</p> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points</p>	10 points	
<b>R2</b>	<p>The Contractor should demonstrate that the proposed resource has experience conducting System and Organization Controls II (SOC II) audits for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.</p> <p>**Large is defined as an organization with 5,000 employees or more.</p>	<p>0 audits = 0 points 1 audits = 1 point 2 audits = 2 points 3 audits = 3 points 4 audits = 4 points 5 audits = 5 points 6 or more audits = 10 points</p>	10 points	
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has experience preparing reports based on Statement on Standards for Attestation Engagements no.18 (SSAE 18) and/or Canadian Standard On Assurance Engagements (CSAE) 3000, or CSAE 3001 standards within one year prior to the TA issuance date.</p>	<p>0 report = 0 points 1 report = 1 point 2 reports = 2 points 3 reports = 3 points 4 reports = 4 points 5 reports = 5 points 6 or more reports = 10 points</p>	10 points	
<b>Maximum Points</b>			<b>30</b>	
<b>Minimum Required Points</b>			<b>15</b>	
<b>Total Points Received</b>				

**6. B.1 Business Analyst, Level 3**

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	<p>The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.</p> <p>The additional years of experience is not required to fall within the past 12 years.</p>	<p>1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points</p>	5	
<b>R2</b>	<p>The Contractor should demonstrate that the proposed resource has experience developing business strategies and processes, for a cyber security project or Information Management/Information Technology (IM/IT) program.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points</p>	10	
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has recent (within the last 3 years prior to TA issuance date) project experience, as the business analyst for at least one project related to securing an enterprise IT infrastructure of comparable (or greater) size, scope and complexity in an environment comparable in size, scope and complexity to the GC.</p> <p>The environment must include at least 5,000 employees and a distributed IT infrastructure environment supporting multiple business lines.</p> <p>Projects are deemed comparable when they meet all the following criteria:</p> <ol style="list-style-type: none"> <li>The total dollar value of the project was at least \$2M; and,</li> <li>The project required the active participation from at least two distinct organizations/divisions each under the control of separate management</li> </ol> <p>To qualify, the proposed resource must have performed four or more of the following tasks in each project:</p> <ul style="list-style-type: none"> <li>Develop, review and manage business requirements.</li> </ul>	<p>0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points</p>	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<ul style="list-style-type: none"><li>• Perform analysis of the business requirements to identify and document roles and responsibilities.</li><li>• Capture the current use cases associated with the business requirements.</li><li>• Establish acceptance test criteria with client.</li><li>• Identify and document current state business processes (business or operations).</li><li>• Perform business analysis of functional requirements to identify information, procedures and decision flows.</li><li>• Work with various stakeholders and other sources to understand and identify all requirements information that is relevant to the project. Facilitate cross-functional meetings and exercises to verify current state, to capture requirements and to ensure Cyber project(s) alignment to existing transformation initiatives/ programs.</li><li>• Plan and implement all requirements-related activities, including elicitation, validation, reporting status, resolving conflicts, and gaining approval.</li><li>• Develop and manage detailed business and functional requirements for cyber project(s), by preparing use cases, data models, and capturing existing business rules from various forms of documentation such as process maps and interviews with subject matter experts. Organize, structure and understand the elicited requirements; putting them into an appropriate form, and performing necessary verification and validation on them.</li></ul>			

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R4</b>	The Contractor should demonstrate that the proposed resource holds a current International Institute of Business Analysis Certified Business Analyst Professional (CBAP) Certification.  A copy of the certification must be provided with the proposal.	No certification = 0 points CBAP Certification = 5 points	5	
<b>R5</b>	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications: <ul style="list-style-type: none"> <li>• Certified Information System Security Professional (CISSP)</li> <li>• Certified Information Security Manager (CISM)</li> <li>• Certified Information Systems Auditor (CISA)</li> <li>• Certified in Risk and Information Systems Control (CRISC)</li> </ul> A copy of the current and valid certification must be provided with the proposal.	0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points	10	
<b>Maximum Points</b>			<b>40</b>	
<b>Minimum Required Points</b>			<b>20</b>	
<b>Total Points Received</b>				

**7. B.14 Technical Writer, Level 3**

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.  The additional years of experience is not required to fall within the past 12 years.	1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points	5	
<b>R2</b>	The Contractor should demonstrate that the proposed resource has experience as a Technical Writer for a cyber security project or program.  To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
R3	<p>The Contractor should demonstrate that the proposed resource has experience writing large technical documents.</p> <p>Specifically, the resource must have been one of the primary authors of at least 5 technical documents, each consisting of at least 50 pages. Document title and length must be listed for at least 5 such documents in the proposed resource's résumé.</p>	<p>5 documents = 1 point 6-9 documents = 2 points 10 or more documents = 5 points</p>	5	
R4	<p>The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"><li>• Certified Information System Security Professional (CISSP)</li><li>• Certified Information Security Manager (CISM)</li><li>• Certified Information Systems Auditor (CISA)</li><li>• Certified in Risk and Information Systems Control (CRISC)</li></ul> <p>A copy of the current and valid certification must be provided with the proposal.</p>	<p>0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points</p>	10	
Maximum Points			30	
Minimum Required Points			15	
Total Points Received				

## **Workstream 2 – Security Assurance**

### **RESOURCE MANDATORY REQUIREMENT**

#### **1. C.3 IT Security TRA and C&A Analyst, Level 3**

<b>Resource Name:</b>		
<b>Criteria</b>	<b>Mandatory Requirement</b>	<b>Demonstrated Experience</b> (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the last twelve (12) years prior to TA issuance date in performing IT Security Threat Risk Analysis (TRA) and/or Certification and Accreditation or Security Assessment and Authorization (SA&amp;A).</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of five (5) years of demonstrated experience in the last eight (8) years prior to TA issuance date in the assessment of applied IT security controls, or the evaluation of threats and risks, or the interpretation and application of ITSG-33 IT Security Risk Management Framework, for complex*, enterprise-wide applications or information system.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p> <p>* Complex is defined as a group of interacting, interrelated systems.</p>	

#### **2. C.7 IT Security Design Specialist (General Stream), Level 3**

<b>Resource Name:</b>		
<b>Criteria</b>	<b>Mandatory Requirement</b>	<b>Demonstrated Experience</b> (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the last twelve (12) years prior to the TA issuance date, planning, developing and implementing IT security architectures or IT security designs for complex*, enterprise-wide applications or</p>	

<b>Resource Name:</b>		
<b>Criteria</b>	<b>Mandatory Requirement</b>	<b>Demonstrated Experience</b> (Contractor to insert response)
	<p>information system, in at least two (2) of the following areas:</p> <ul style="list-style-type: none"> <li>viii. Cloud security</li> <li>ix. Security and Risk Management</li> <li>x. Endpoint Security</li> <li>xi. Communications &amp; Network Security</li> <li>xii. Identity &amp; Access Management</li> <li>xiii. Security Operations</li> <li>xiv. Software Development and Application Security</li> </ul> <p>* Complex is defined as a group of interacting, interrelated systems.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of three (3) years of demonstrated experience in the last six (6) years prior to TA issuance date with the development and delivery of IT security strategies, white papers, standards, solutions/proposals to solving IT and security problems affecting multiple stakeholders and security architectures.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	
<b>M3</b>	<p>The Contractor must clearly demonstrate that the proposed resource has demonstrated combined experience in at least two (2) projects, having developed at least three (3) of the following types of system engineering artifacts:</p> <ul style="list-style-type: none"> <li>i) Architecture documents;</li> <li>j) System Requirements Specifications;</li> <li>k) System Design Specifications;</li> <li>l) Build / Configuration documents;</li> <li>m) Concept of Operations (ConOps);</li> <li>n) System Implementation Plans;</li> <li>o) Test Plans/Test Reports; and</li> <li>p) Life Cycle Support Plans</li> </ul> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	

### 3. C.11 IT Security VA Specialist, Level 3

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the last twelve (12) years prior to TA issuance date in performing IT Security Vulnerability Assessments (VA).</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has experience working as a vulnerability specialist on a minimum of three (3) IT security projects for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client, performing at least three (3) of the following tasks across the referenced projects:</p> <ul style="list-style-type: none"><li>a) Performing vulnerability testing, risk analysis and security assessment;</li><li>b) Understanding various programming language environments and attacking simulation scenarios including performing vulnerability assessments on highly virtualized environments.</li><li>c) Understanding and implementing security policies and safeguards;</li><li>d) Conducting impact analysis for configuration changes and patch management.</li><li>e) Conducting analysis with network scanning and monitoring tools;</li><li>f) Conducting internal and external IT security audits; and,</li><li>g) Recommending appropriate tools and countermeasures to mitigate IT security vulnerabilities.</li></ul> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	

#### 4. C.16 PIA Specialist, Level 3

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	The Contractor must clearly demonstrate that the proposed resource has a minimum of 10 years of combined experience in the last twelve (12) years prior to the TA issuance date in performing privacy impact assessments (PIA).	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of three (3) years of experience, within the last six (6) years prior to the TA issuance date, performing all of the following tasks:</p> <ul style="list-style-type: none"> <li>Performing privacy impact assessment (PIA) on IT infrastructure and systems for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.</li> <li>Identifying and mitigating threats and risks associated with the handling of different information types including personal information, business information, financial information and other sensitive data.</li> <li>Application of policies and procedures regarding access, retention, storage, use, transfer and disposal of documentation related to personally identifiable information (PII).</li> <li>Developing and conducting PIA in accordance with best practices.</li> <li>Identification of privacy risks associated with the integration of data sets from different systems to obtain, retrieve and synchronize information for the purposes of data exploration and research</li> <li>Application of privacy legislation and regulations such as: <ul style="list-style-type: none"> <li>Freedom of Information and Privacy Protection Act (FIPPA)</li> <li>Municipal Freedom of Information and Protection of Privacy Act</li> <li>Personal Information Protection and Electronic Documents Act (PIPEDA)</li> </ul> </li> <li>Application of privacy and security concepts; user authentication processes along with identification, definition and assignment of security roles.</li> </ul> <p>**Large is defined as an organization with 5,000 employees or more.</p>	

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
	To qualify, the resource must have worked on the referenced projects for minimum of six (6) consecutive months in duration.	

### 5. P.9 Project Manager, Level 3

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten(10) years of combined experience in the last twelve (12) years prior to the TA issuance date as a Project Manager with at least one (1) of the following recognized professional certifications:</p> <ul style="list-style-type: none"> <li>• Project Management Professional (PMP);</li> <li>• Certified Associate in Project Management (CAPM);</li> <li>• Program Management Professional (PgMP);</li> <li>• Portfolio Management Professional (PfMP);</li> <li>• Project Management Institute (PMI) Agile</li> <li>• Certified Practitioner (PMI-ACP);</li> <li>• PMI Professional in Business Analysis (PMIPBA);</li> <li>• PMI Risk Management Professional (PMIRMP);</li> <li>• and</li> <li>• PMI Scheduling Professional (PMI-SP);</li> </ul> <p>A copy of the resource's valid certification must be submitted.</p> <p>To qualify, the project management experience must include all of the following tasks:</p> <ul style="list-style-type: none"> <li>• Manage the project by ensuring that resources are made available and that the project is developed and is on track to be fully operational within previously agreed time, cost and performance parameters.</li> <li>• Define and document the objectives for the project; determine budgetary requirements, the</li> </ul>	

<b>Resource Name:</b>		
<b>Criteria</b>	<b>Mandatory Requirement</b>	<b>Demonstrated Experience</b> (Contractor to insert response)
	<p>composition, roles and responsibilities and terms of reference for the project team.</p> <ul style="list-style-type: none"> <li>Report progress of the project on an ongoing basis and at scheduled points in the life cycle.</li> <li>Meet in conference with stakeholders and other project managers and states problems in a form capable of being solved.</li> <li>Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools.</li> </ul>	
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has at least 2 years' experience in the last 5 years working as a Project Manager on a minimum of one (1) IT security related project for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.</p> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the project management experience must include all of the following tasks:</p> <ul style="list-style-type: none"> <li>Manage the project by ensuring that resources are made available and that the project is developed and is on track to be fully operational within previously agreed time, cost and performance parameters.</li> <li>Define and document the objectives for the project; determine budgetary requirements, the composition, roles and responsibilities and terms of reference for the project team.</li> <li>Report progress of the project on an ongoing basis and at scheduled points in the life cycle.</li> <li>Meet in conference with stakeholders and other project managers and states problems in a form capable of being solved.</li> <li>Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools.</li> </ul> <p>To qualify, the resource must have worked on the referenced projects for a minimum of six (6) consecutive months in duration.</p>	
<b>M3</b>	The Contractor must clearly demonstrate that the proposed resource has experience working as a Project	

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
	<p>Manager on a minimum of five (5) IT security related projects, where each project must have had a budget of at least \$2M.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of six (6) consecutive months in duration.</p> <p>To qualify, the project management experience must include all of the following tasks:</p> <ul style="list-style-type: none"> <li>• Manage the project by ensuring that resources are made available and that the project is developed and is on track to be fully operational within previously agreed time, cost and performance parameters.</li> <li>• Define and document the objectives for the project; determine budgetary requirements, the composition, roles and responsibilities and terms of reference for the project team.</li> <li>• Report progress of the project on an ongoing basis and at scheduled points in the life cycle.</li> <li>• Meet in conference with stakeholders and other project managers and states problems in a form capable of being solved.</li> <li>• Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools.</li> </ul>	

## 6. B.1 Business Analyst, Level 3

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of experience in the past twelve (12) years prior to the TA issuance date in developing business strategies and processes as a Business Analyst.	

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M2</b>	<p>The Contractor must clearly demonstrate that the proposed resource has experience working as a Business Analyst on a minimum of one (1) IT security related projects for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client, performing at least three (3) of the following tasks:</p> <ul style="list-style-type: none"> <li>Defining business strategies in support of transformation and change management activities.</li> <li>Developing and documenting statements of requirements for considered alternatives.</li> <li>Performing business analyses of functional requirements to identify information, procedures, and decision flows.</li> <li>Evaluating existing procedures and methods, identifying and documenting items such as database content, structure, application subsystems.</li> <li>Defining and documenting interfaces between external and internal systems, or new and existing systems.</li> <li>Establishing acceptance test criteria with client.</li> <li>Supporting and using the selected departmental methodologies.</li> </ul> <p>**Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	

## 7. A.7 Programmer/Analyst, Level 3

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M1</b>	<p>The Contractor must clearly demonstrate that the proposed resource has a minimum of ten (10) years of experience in the past twelve (12) years prior to the TA issuance date in developing software as a Programmer/Analyst.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M2</b>	The proposed resource must have a university degree in a computer-related discipline (e.g., Computer Science or Computer Engineering) or a college diploma in a Computer-related discipline with a minimum of ten years of experience in the computer industry since graduation.	
<b>M3</b>	<p>The Contractor must clearly demonstrate that the proposed resource has experience working as a Programmer/Analyst on a minimum of one (1) IT security related project for a large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a large commercial client, performing the following tasks:</p> <ul style="list-style-type: none"><li>• Developing and maintaining software code for three-tier (presentation, application, data) applications.</li><li>• Drafting, reviewing, or editing technical and end-user documentation.</li><li>• Developing test cases for applications.</li></ul> <p>Large is defined as an organization with 5,000 employees or more.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Resource Name:		
Criteria	Mandatory Requirement	Demonstrated Experience (Contractor to insert response)
<b>M4</b>	<p>The proposed resource must have a minimum of five years' programming experience, within the last eight years prior to the TA issuance date, with at least five of the following technologies:</p> <ul style="list-style-type: none"><li>• Oracle</li><li>• SQL</li><li>• PL/SQL</li><li>• ASP</li><li>• .Net</li><li>• C++</li><li>• C#</li><li>• Java</li><li>• Perl</li><li>• PHP</li><li>• Python</li><li>• JavaScript</li><li>• JQuery</li><li>• HTML</li><li>• XML</li><li>• JSON</li><li>• Ruby</li><li>• Android development</li><li>• iOS development</li></ul>	

## RESOURCE RATED REQUIREMENTS

### 1. C.3 IT Security TRA and C&A Analyst, Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
R1	The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.  The additional years of experience is not required to fall within the past 12 years.	1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points	5	
R2	The Contractor should demonstrate that the proposed resource has experience developing and documenting information system security assurance processes, guidance, or policies for a **large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a **large commercial client.  **Large is defined as an organization with 5,000 employees or more.  To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points	10	
R3	The Contractor should demonstrate that the proposed resource has recent (within last 7 years prior to TA issuance date) project experience validating the following:  1. IT security controls (ITSG-33 based) and applicable safeguards 2. Assessment of mitigation strategies 3. Assessment of residual risk  A maximum of 4 projects is to be submitted. If more than 4 projects are submitted, only the first 4 projects will be evaluated.  To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	1 project – 2 points 2 projects – 5 points 3 projects – 7 points 4 projects – 10 points	10	
R4	The Contractor should demonstrate that the proposed resource has experience in developing and delivering training on IT security risk management methodologies such as ITSG-33 IT Security Risk Management Framework.	2 points per training course up to a maximum of 5 courses	10	
R5	The Contractor should demonstrate that the proposed resource holds a current and valid	No certification = 0 points	15	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	ICS2 Certified Information System Security Professional (CISSP) Certification.  A copy of the certification must be provided with the proposal.	CISSP Certification = 15 points		
<b>R6</b>	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications: <ul style="list-style-type: none"> <li>• Certified Cloud Security Professional (CCSP)</li> <li>• Certified Information Security Manager (CISM)</li> <li>• Certified Information Systems Auditor (CISA)</li> <li>• Certified in Risk and Information Systems Control (CRISC)</li> <li>• Certified Cyber Forensics Professional (CCFP)</li> <li>• Systems Security Certified Professional (SSCP)</li> <li>• Information Technology Infrastructure Library (ITIL)</li> <li>• Information Systems Security Architecture Professional (ISSAP)</li> <li>• CompTIA Security+</li> <li>• SABSA Chartered Security Architect Foundation (SCF) or higher</li> </ul> A copy of the certification must be provided with the proposal.	0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points	10	
<b>Maximum Points</b>			<b>60</b>	
<b>Minimum Required Points</b>			<b>30</b>	
<b>Total Points Received</b>				

## 2. C.7 IT Security Design Specialist (General Stream), Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.	1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points	5	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	The additional years of experience is not required to fall within the past 12 years.			
<b>R2</b>	<p>The Contractor should demonstrate that the proposed resource has recent (within last 7 years prior to the TA issuance date) combined experience performing all of the following IT Security tasks:</p> <ol style="list-style-type: none"> <li>1. Analysis of IT Security tools and techniques</li> <li>2. Analysis of security data and provision of advisories and reports</li> <li>3. Preparation of technical reports such as requirement analysis, options analysis, technical architecture documents, mathematical risk modeling</li> <li>4. Security architecture design and engineering support</li> </ol> <p>Reference projects do not require all listed tasks to qualify.</p> <p>A maximum of 6 projects is to be submitted. If more than 6 projects are submitted, only the first 6 projects will be evaluated.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>24 to 30 months = 2 points</p> <p>&gt;30 to 36 months = 4 points</p> <p>&gt;36 to 42 months = 6 points</p> <p>&gt;42 to 48 months = 8 points</p> <p>&gt;48 months = 10 points</p>	10	
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has recent (within last 7 years prior to TA issuance date) experience designing/architecting/engineering IT security components and architectures for enterprise solutions and/or coordinating development of design solutions across multiple teams for solving IT security problems involving multiple stakeholders, while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) guidelines.</p>	<p>24 to 30 months = 2 points</p> <p>&gt;30 to 36 months = 4 points</p> <p>&gt;36 to 42 months = 6 points</p> <p>&gt;42 to 48 months = 8 points</p> <p>&gt;48 months = 10 points</p>	10	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<p>To qualify, an enterprise solution is considered to be a system that supports 4,000 users or more.</p> <p>A maximum of 6 projects is to be submitted. If more than 6 projects are submitted, only the first 6 projects will be evaluated.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>			
<b>R4</b>	<p>The Contractor should demonstrate that the proposed resource holds a current and valid ICS2 Certified Information System Security Professional (CISSP) Certification.</p> <p>A copy of the certification must be provided with the proposal.</p>	<p>No certification = 0 points</p> <p>CISSP Certification = 15 points</p>	15	
<b>R5</b>	<p>The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"> <li>• Certified Cloud Security Professional (CCSP)</li> <li>• Certified Information Security Manager (CISM)</li> <li>• Certified Information Systems Auditor (CISA)</li> <li>• Certified in Risk and Information Systems Control (CRISC)</li> <li>• Certified Cyber Forensics Professional (CCFP)</li> <li>• Systems Security Certified Professional (SSCP)</li> <li>• Information Technology Infrastructure Library (ITIL)</li> <li>• Information Systems Security Architecture Professional (ISSAP)</li> <li>• CompTIA Security+</li> <li>• GIAC (Global Information Assurance Certification)</li> </ul>	<p>0 certifications = 0 points</p> <p>1 certification = 2 points</p> <p>2-3 certifications = 5 points</p> <p>4 or more certifications = 10 points</p>	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<ul style="list-style-type: none"> <li>SABSA Chartered Security Architect Foundation (SCF) or higher</li> </ul> <p>A copy of the certification must be provided with the proposal.</p>			
<b>Maximum Points</b>			<b>50</b>	
<b>Minimum Required Points</b>			<b>25</b>	
<b>Total Points Received</b>				

### 3. C.11 IT Security VA Specialist, Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	<p>The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.</p> <p>The additional years of experience is not required to fall within the past 12 years.</p>	<p>1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points</p>	5	
<b>R2</b>	<p>The Contractor should demonstrate that the proposed resource has a minimum of five (5) years of combined experience reviewing, analyzing, and supporting any combination of at least two (2) of the following technologies:</p> <p>1) Internet Security Protocols; 2) Networking Protocols; 3) Wireless Networking; 4) Directory Standards; 5) Networking Hardening; and/or 6) Operating Systems.</p>	<p>two of the listed technologies = 1 point three of the listed technologies = 2 points four of the listed technologies = 3 points five of the listed technologies = 4 points six of the listed technologies = 5 points</p>	5	
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has experience documenting and delivering IT security threat, vulnerability and/or risk briefings.</p>	<p>1 to 3 years of experience = 1 point &gt;3 to 5 years of experience = 2 points &gt;5 to 8 years of experience = 3 points &gt;8 years of experience = 5 points</p>	5	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R4</b>	The Contractor should demonstrate that the proposed resource holds a current and valid ICS2 Certified Information System Security Professional (CISSP) Certification.  A copy of the certification must be provided with the proposal.	No certification = 0 points CISSP Certification = 15 points	15	
<b>R5</b>	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications: <ul style="list-style-type: none"> <li>• GIAC Certified Incident Handler (GCIH)</li> <li>• GIAC Penetration Tester (GPEN)</li> <li>• GIAC Web Application Penetration Tester (GWAPT)</li> <li>• GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)</li> <li>• GIAC Certified Intrusion Analyst (GCIA)</li> <li>• GIAC Security Essentials (GSEC)</li> <li>• Offensive Security Certified Professional (OSCP)</li> <li>• OSSTMM Professional Security Analyst Accredited Certification (OPSA)</li> </ul> A copy of the current and valid certification must be provided with the proposal.	0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points	10	
<b>Maximum Points</b>			<b>40</b>	
<b>Minimum Required Points</b>			<b>20</b>	
<b>Total Points Received</b>				

#### 4. C.16 PIA Specialist, Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.  The additional years of experience is not required to fall within the past 12 years.	1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points	5	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R2</b>	The Contractor should demonstrate that the proposed resource holds a current and valid Holistic Information Security Practitioner (HISP) Certification or Certified Information Privacy Professional (CIPP).  A copy of the certification(s) should be provided with the proposal.	No certification = 0 point 1 Certification = 10 points 2 Certifications = 20 points	20	
<b>R3</b>	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:  <ul style="list-style-type: none"> <li>• Certified Internal Auditor (CIA); and</li> <li>• Certified Information Systems Auditor (CISA).</li> </ul> A copy of the current and valid certification must be provided with the proposal.	0 certifications = 0 points 1 certification = 5 points 2 certifications = 10 points	10	
<b>Maximum Points</b>			<b>35</b>	
<b>Minimum Required Points</b>			<b>18</b>	
<b>Total Points Received</b>				

#### 5. P.9 Project Manager, Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.  The additional years of experience is not required to fall within the past 12 years.	1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points	5	
<b>R2</b>	The Contractor should demonstrate that the proposed resource has project experience for a cyber security project or program, performing two or more the following tasks:  <ul style="list-style-type: none"> <li>• Manage the project by ensuring that resources are made available and that the project is developed and is on track to be fully operational within previously agreed time, cost and performance parameters.</li> </ul>	0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points	10	

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<ul style="list-style-type: none"> <li>Define and document the objectives for the project; determine budgetary requirements, the composition, roles and responsibilities and terms of reference for the project team.</li> <li>Report progress of the project on an ongoing basis and at scheduled points in the life cycle.</li> <li>Prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools.</li> </ul> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>			
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has experience within the last 3 years prior to TA issuance date, managing at least one project related to securing an enterprise IT infrastructure in an environment that includes at least 5,000 employees and a complex and international or country-wide distributed IT infrastructure environment supporting multiple business lines and including classified environments.</p> <p>To qualify, the project must meet all the following criteria:</p> <ol style="list-style-type: none"> <li>The total dollar value of the project elements that were managed by the resource was at least \$10M; and,</li> <li>The project required the active participation from at least three distinct organizations/divisions each under the control of separate management.</li> </ol>	<p>0 project = 0 points 1 project = 2 point 2 projects = 4 points 3 projects = 6 points 4 projects = 8 points 5 or more projects = 10 points</p>	10	
<b>R4</b>	<p>The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"> <li>Certified Information System Security Professional (CISSP)</li> <li>Certified Information Security Manager (CISM)</li> </ul>	<p>0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 certifications = 10 points</p>	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<ul style="list-style-type: none"> <li>Certified Information Systems Auditor (CISA)</li> <li>Certified in Risk and Information Systems Control (CRISC)</li> </ul> <p>A copy of the current and valid certification must be provided with the proposal.</p>			
<b>Maximum Points</b>			<b>35</b>	
<b>Minimum Required Points</b>			<b>18</b>	
<b>Total Points Received</b>				

#### 6. B.1 Business Analyst, Level 3

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	<p>The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.</p> <p>The additional years of experience is not required to fall within the past 12 years.</p>	<p>1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points</p>	5	
<b>R2</b>	<p>The Contractor should demonstrate that the proposed resource has experience developing business strategies and processes, for a cyber security project or Information Management/Information Technology (IM/IT) program.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points</p>	10	
<b>R3</b>	<p>The Contractor should demonstrate that the proposed resource has recent (within the last 3 years prior to TA issuance date) project experience, as the business analyst for at least one project related to securing an enterprise IT infrastructure of comparable (or greater) size, scope and complexity in an environment comparable in size, scope and complexity to the GC.</p> <p>The environment must include at least 5,000 employees and a distributed IT infrastructure environment supporting multiple business lines.</p>	<p>0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points</p>	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<p>Projects are deemed comparable when they meet all the following criteria:</p> <ul style="list-style-type: none"><li>c) The total dollar value of the project was at least \$2M; and,</li><li>d) The project required the active participation from at least two distinct organizations/divisions each under the control of separate management</li></ul> <p>To qualify, the proposed resource must have performed four or more of the following tasks in each project:</p> <ul style="list-style-type: none"><li>• Develop, review and manage business requirements.</li><li>• Perform analysis of the business requirements to identify and document roles and responsibilities.</li><li>• Capture the current use cases associated with the business requirements.</li><li>• Establish acceptance test criteria with client.</li><li>• Identify and document current state business processes (business or operations).</li><li>• Perform business analysis of functional requirements to identify information, procedures and decision flows.</li><li>• Work with various stakeholders and other sources to understand and identify all requirements information that is relevant to the project. Facilitate cross-functional meetings and exercises to verify current state, to capture requirements and to ensure Cyber project(s) alignment to existing transformation initiatives/ programs.</li><li>• Plan and implement all requirements-related activities, including elicitation, validation, reporting status, resolving conflicts, and gaining approval.</li></ul>			

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	<ul style="list-style-type: none"><li>Develop and manage detailed business and functional requirements for cyber project(s), by preparing use cases, data models, and capturing existing business rules from various forms of documentation such as process maps and interviews with subject matter experts. Organize, structure and understand the elicited requirements; putting them into an appropriate form, and performing necessary verification and validation on them.</li></ul>			
<b>R4</b>	<p>The Contractor should demonstrate that the proposed resource holds a current International Institute of Business Analysis Certified Business Analyst Professional (CBAP) Certification.</p> <p>A copy of the certification must be provided with the proposal.</p>	<p>No certification = 0 points CBAP Certification = 5 points</p>	5	
<b>R5</b>	<p>The Contractor should demonstrate that the proposed resource holds one or more of the following certifications:</p> <ul style="list-style-type: none"><li>Certified Information System Security Professional (CISSP)</li><li>Certified Information Security Manager (CISM)</li><li>Certified Information Systems Auditor (CISA)</li><li>Certified in Risk and Information Systems Control (CRISC)</li></ul> <p>A copy of the current and valid certification must be provided with the proposal.</p>	<p>0 certifications = 0 points 1 certification = 2 points 2-3 certifications = 5 points 4 or more certifications = 10 points</p>	10	
<b>Maximum Points</b>			<b>40</b>	
<b>Minimum Required Points</b>			<b>20</b>	
<b>Total Points Received</b>				

**7. A.7 Programmer/Analyst, Level 3**

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
<b>R1</b>	The Contractor should demonstrate the proposed resource's experience above the minimum required under M1 for this resource category.  The additional years of experience is not required to fall within the past 12 years.	1 year above = 1 point 2 years above = 2 points 3 years above = 3 points 4 years above = 4 points 5 or more years above = 5 points	5	
<b>R2</b>	The Contractor should demonstrate the proposed resource's project experience in applying Web Content Accessibility Guidelines (WCAG 2.0) in developing web content, such as the GC Web Experience Toolkit (WET) accessibility standard.  To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 or more projects = 5 points	5	
<b>R3</b>	The Contractor should demonstrate that the proposed resource has experience developing software and associated documentation, for an Identity, Credential and Access Management (ICAM) solution.  To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points	10	
<b>R4</b>	The Contractor should demonstrate that the proposed resource has experience developing software and associated documentation, for a cloud-based information system or application.  To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.	0 project = 0 points 1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 projects = 4 points 5 projects = 5 points 6 or more projects = 10 points	10	
<b>R5</b>	The Contractor should demonstrate that the proposed resource has experience has a minimum of five years' experience programming in a combination of C++, C#, and Java.	5 to 7 years = 6 points 7+ years = 10 points	10	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Demonstrated Experience (Contractor to insert response)	Max Available Points	Points Received
	To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.			
<b>R6</b>	<p>The Contractor should demonstrate that the proposed resource has experience has a minimum of five years' experience programming in a combination of Perl, PHP, and Python.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>5 to 7 years = 6 points 7+ years = 10 points</p>	10	
<b>R7</b>	<p>The Contractor should demonstrate that the proposed resource has experience has a minimum of five years' experience programming in a combination of SQL, .NET, and JavaScript.</p> <p>To qualify, the resource must have worked on the referenced projects for a minimum of four (4) consecutive months in duration.</p>	<p>5 to 7 years = 6 points 7+ years = 10 points</p>	10	
<b>Maximum Points</b>			<b>60</b>	
<b>Minimum Required Points</b>			<b>36</b>	
<b>Total Points Received</b>				

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

## **APPENDIX D TO ANNEX A**

### **CERTIFICATIONS AT THE TA STAGE**

The following Certifications are to be used, as applicable. If they apply, they must be signed and attached to the Contractor's quotation when it is submitted to Canada.

#### **1. CERTIFICATION OF EDUCATION AND EXPERIENCE**

The Contractor certifies that all the information provided in the résumés and supporting material proposed for completing the subject work, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Contractor to be true and accurate. Furthermore, the Contractor warrants that every individual proposed by the Contractor for the requirement is capable of performing the Work described in the Task Authorization.

---

Print name of authorized individual & sign above

---

Date

#### **2. CERTIFICATION OF AVAILABILITY OF PERSONNEL**

The Contractor certifies that, should it be authorized to provide services under this Task Authorization, the persons proposed in the quotation will be available to commence performance of the work within a reasonable time from the date of issuance of the valid Task Authorization, or within the time specified in the TA Form, and will remain available to perform the work in relation to the fulfillment of the requirement.

---

Print name of authorized individual & sign above

---

Date

#### **3. CERTIFICATION OF STATUS OF PERSONNEL**

If the Contractor has proposed any individual who is not an employee of the Contractor, the Contractor certifies that it has permission from that individual to propose his/her services in relation to the Work to be performed under this TA and to submit his/her résumé to Canada. At any time during the Contract Period the Contractor must, upon request from the Contracting Authority, provide the written confirmation, signed by the individual, of the permission that was given to the Contractor of his/her availability. Failure to comply with the request may result in a default under the Contract in accordance with the General Conditions.

---

Print name of authorized individual & sign above

---

Date

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

4. CERTIFICATION OF LANGUAGE

The Contractor certifies that the proposed resource(s) in response to this draft Task Authorization is/are fluent in English. The individual(s) proposed must be able to communicate orally and in writing in English without any assistance and with minimal errors.

---

Print name of authorized individual & sign above

---

Date

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

## ANNEX B

### BASIS OF PAYMENT

#### WORKSTREAM 1

##### INITIAL CONTRACT PERIOD:

Initial Contract Period (Date of Contract award to 3 years later)		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.2 IT Security Methodology, Policy and Procedures Analyst	LEVEL 3	
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	LEVEL 3	
P.12 Risk Management Specialist	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
B.14 Technical Writer	LEVEL 3	

##### OPTION PERIODS:

Option Period 1		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.2 IT Security Methodology, Policy and Procedures Analyst	LEVEL 3	
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	LEVEL 3	
P.12 Risk Management Specialist	LEVEL 3	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

B.1 Business Analyst	LEVEL 3	
B.14 Technical Writer	LEVEL 3	

Option Period 2		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.2 IT Security Methodology, Policy and Procedures Analyst	LEVEL 3	
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	LEVEL 3	
P.12 Risk Management Specialist	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
B.14 Technical Writer	LEVEL 3	

## **WORKSTREAM 2**

### **INITIAL CONTRACT PERIOD:**

Initial Contract Period (Date of Contract award to 3 years later)		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.11 IT Security VA Specialist	LEVEL 3	
C.16 PIA Specialist	LEVEL 3	
P.9 Project Manager	LEVEL 3	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

B.1 Business Analyst	LEVEL 3	
A.7 Programmer/Analyst	LEVEL 3	

**OPTION PERIODS:**

Option Period 1		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.11 IT Security VA Specialist	LEVEL 3	
C.16 PIA Specialist	LEVEL 3	
P.9 Project Manager	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
A.7 Programmer/Analyst	LEVEL 3	

Option Period 2		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.11 IT Security VA Specialist	LEVEL 3	
C.16 PIA Specialist	LEVEL 3	
P.9 Project Manager	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
A.7 Programmer/Analyst	LEVEL 3	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

## **ANNEX C**

### **SECURITY REQUIREMENTS CHECK LIST**

Government  
of CanadaGouvernement  
du Canada

Contract Number / Numéro du contrat

24062-190077

Security Classification / Classification de sécurité  
UNCLASSIFIED

## SECURITY REQUIREMENTS CHECK LIST (SRCL)

## LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE		
1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine		2. Branch or Directorate / Direction générale ou Direction
TBS		CIOB
3. a) Subcontract Number / Numéro du contrat de sous-traitance		3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
4. Brief Description of Work / Brève description du travail		
Support to Cyber Security Division		
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?		<input checked="" type="checkbox"/> No Non <input type="checkbox"/> Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?		<input checked="" type="checkbox"/> No Non <input type="checkbox"/> Yes Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)		<input type="checkbox"/> No Non <input checked="" type="checkbox"/> Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.		<input checked="" type="checkbox"/> No Non <input type="checkbox"/> Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?		<input checked="" type="checkbox"/> No Non <input type="checkbox"/> Yes Oui
7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès		
Canada <input checked="" type="checkbox"/>	NATO / OTAN <input type="checkbox"/>	Foreign / Étranger <input type="checkbox"/>
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion <input checked="" type="checkbox"/>	All NATO countries Tous les pays de l'OTAN <input type="checkbox"/>	No release restrictions Aucune restriction relative à la diffusion <input type="checkbox"/>
Not releasable À ne pas diffuser <input type="checkbox"/>		
Restricted to: / Limité à: <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>
Specify country(ies): / Préciser le(s) pays:	Specify country(ies): / Préciser le(s) pays:	Specify country(ies): / Préciser le(s) pays:
7. c) Level of information / Niveau d'information		
PROTECTED A PROTÉGÉ A <input type="checkbox"/>	NATO UNCLASSIFIED NATO NON CLASSIFIÉ <input type="checkbox"/>	PROTECTED A PROTÉGÉ A <input type="checkbox"/>
PROTECTED B PROTÉGÉ B <input type="checkbox"/>	NATO RESTRICTED NATO DIFFUSION RESTREINTE <input type="checkbox"/>	PROTECTED B PROTÉGÉ B <input type="checkbox"/>
PROTECTED C PROTÉGÉ C <input type="checkbox"/>	NATO CONFIDENTIAL NATO CONFIDENTIEL <input type="checkbox"/>	PROTECTED C PROTÉGÉ C <input type="checkbox"/>
CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>	NATO SECRET NATO SECRET <input type="checkbox"/>	CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>
SECRET SECRET <input checked="" type="checkbox"/>	COSMIC TOP SECRET COSMIC TRÈS SECRET <input type="checkbox"/>	SECRET SECRET <input type="checkbox"/>
TOP SECRET TRÈS SECRET <input type="checkbox"/>		TOP SECRET TRÈS SECRET <input type="checkbox"/>
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>



Government of Canada  
Gouvernement du Canada

COMMON-PS-SRCL#34

Contract Number / Numéro du contrat

24062-190077

Security Classification / Classification de sécurité  
UNCLASSIFIED

**PART A (continued) / PARTIE A (suite)**

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?

Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?

☒ No ☐ Yes  
Non Oui

If Yes, indicate the level of sensitivity:

Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?

Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

☒ No ☐ Yes  
Non Oui

Short Title(s) of material / Titre(s) abrégé(s) du matériel :

Document Number / Numéro du document :

**PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)**

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

- |  |   |  |  |
|--|---|--|--|
| <input type="checkbox"/> RELIABILITY STATUS<br>COTE DE FIABILITÉ     | <input type="checkbox"/> CONFIDENTIAL<br>CONFIDENTIEL           | <input checked="" type="checkbox"/> SECRET<br>SECRET | <input type="checkbox"/> TOP SECRET<br>TRÈS SECRET               |
| <input type="checkbox"/> TOP SECRET - SIGINT<br>TRÈS SECRET - SIGINT | <input type="checkbox"/> NATO CONFIDENTIAL<br>NATO CONFIDENTIEL | <input type="checkbox"/> NATO SECRET<br>NATO SECRET  | <input type="checkbox"/> COSMIC TOP SECRET<br>COSMIC TRÈS SECRET |
| <input type="checkbox"/> SITE ACCESS<br>ACCÈS AUX EMPLACEMENTS       |   |  |  |

Special comments:

Commentaires spéciaux :

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.

REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?

Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

☒ No ☐ Yes  
Non Oui

If Yes, will unscreened personnel be escorted?

Dans l'affirmative, le personnel en question sera-t-il escorté?

☒ No ☐ Yes  
Non Oui

**PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)**

**INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS**

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?

Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

☒ No ☐ Yes  
Non Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?

Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

☒ No ☐ Yes  
Non Oui

**PRODUCTION**

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?

Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

☒ No ☐ Yes  
Non Oui

**INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)**

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?

Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

☒ No ☐ Yes  
Non Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?

Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

☒ No ☐ Yes  
Non Oui

**PART C - (continued) / PARTIE C - (suite)**

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.

Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.

Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

**SUMMARY CHART / TABLEAU RÉCAPITULATIF**

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL  CONFIDENTIEL	SECRET	TOP SECRET  TRÈS SECRET	NATO RESTRICTED  NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL  NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET  COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ			CONFIDENTIAL	SECRET	TOP SECRET  TRÈS SECRET
											A	B	C			
Information / Assets Renseignements / Biens Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?

La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

No  
Non
☐ Yes  
Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".

Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée

« Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?

La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

No  
Non
☐ Yes  
Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).

Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée

« Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).



Government of Canada  
Gouvernement du Canada

COMMON-PS-SRCL#34

Contract Number / Numéro du contrat 24062-190077
Security Classification / Classification de sécurité UNCLASSIFIED

PART D AUTHORIZATION / PARTIE D AUTORISATION			
13. Organization Project Authority / Chargé de projet de l'organisme			
Name (print) - Nom (en lettres moulées) Imraan Bashir	Title - Titre Sr Director, Cyber Security	Signature 	
Telephone No. - N° de téléphone 613-369-7677	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel imraan.bashir@tbs-sct.gc.ca	Date Aug 8, 2018
14. Organization Security Authority / Responsable de la sécurité de l'organisme			
Name (print) - Nom (en lettres moulées) Mélanie Bussière	Title - Titre MAN, Sec. Serv.	Signature 	
Telephone No. - N° de téléphone 613-365-3063	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date 2018/08/21
15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?			
			<input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> Oui
16. Procurement Officer / Agent d'approvisionnement			
Name (print) - Nom (en lettres moulées) Lan Mao	Title - Titre Supply Team Lead	Signature 	
Telephone No. - N° de téléphone 613-858-9980	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel lan.mao@pwgsc.gc.ca	Date Aug 24, 2018
17. Contracting Security Authority / Autorité contractante en matière de sécurité			
Name (print) - Nom (en lettres moulées)	Title - Titre	Signature Saumur, Jacques O	
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

Jacques Saumur  
Contract Security Officer  
Contracts Security Division / Division des contrats sécurité /  
Contract Security Program / Programme de sécurité des contrats /  
Public Services and Procurement Canada / Services publics et Approvisionnement Canada  
Jacques.Saumur@psg-sc.gc.ca  
Telephone / Téléphone 613-948-1732  
Facsimile / Télécopieur 613-948-1712

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité  
UNCLASSIFIED

Canada

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

### ATTACHMENT 3.1

### BID SUBMISSION FORM

BID SUBMISSION FORM		
<b>Bidder's full legal name</b>		
<b>Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)</b>	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
<b>Bidder's Procurement Business Number (PBN)</b> [see the Standard Instructions 2003]  <b>[Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]</b>		
<b>Jurisdiction of Contract:</b> Province or territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
<b>Former Public Servants</b>  See the Article in Part 2 of the bid solicitation entitled Former Public Servant for a definition of "Former Public Servant".	Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
	Is the Bidder a FPS who received a lump sum payment under the terms of the Work Force Adjustment Directive? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

<b>Security Clearance Level of Bidder</b> [include both the level and the date it was granted] <b>[Note to Bidders: Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]</b>				
<b>workstream covered by this bid:</b> Bidders should indicate which Workstream they are proposing to supply in this bid (If the bidder has submitted bid for one or more Workstreams, please only indicate the Workstream covered by this bid).	<b>Workstream</b>		<b>Yes/No</b>	
	Workstream 1			
	Workstream 2			
On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:  1. The Bidder considers itself and its proposed resources able to meet all the mandatory requirements described in the bid solicitation; 2. This bid is valid for the period requested in the bid solicitation; 3. All the information provided in the bid is complete, true and accurate; and 4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.				
<b>Signature of Authorized Representative of Bidder</b>				

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

---

## ATTACHMENT 3.2

### PRICING SCHEDULE

#### WORKSTREAM 1

##### INITIAL CONTRACT PERIOD:

Initial Contract Period (Date of Contract award to 3 years later)		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.2 IT Security Methodology, Policy and Procedures Analyst	LEVEL 3	
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	LEVEL 3	
P.12 Risk Management Specialist	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
B.14 Technical Writer	LEVEL 3	

##### OPTION PERIODS:

Option Period 1		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.2 IT Security Methodology, Policy and Procedures Analyst	LEVEL 3	
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	LEVEL 3	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

P.12 Risk Management Specialist	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
B.14 Technical Writer	LEVEL 3	

Option Period 2		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.2 IT Security Methodology, Policy and Procedures Analyst	LEVEL 3	
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.7 IT Security Design Specialist (Identity, Credential, and Access Management Stream (ICAM) Stream)	LEVEL 3	
P.12 Risk Management Specialist	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
B.14 Technical Writer	LEVEL 3	

## **WORKSTREAM 2**

### **INITIAL CONTRACT PERIOD:**

Initial Contract Period (Date of Contract award to 3 years later)		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.11 IT Security VA Specialist	LEVEL 3	
C.16 PIA Specialist	LEVEL 3	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

P.9 Project Manager	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
A.7 Programmer/Analyst	LEVEL 3	

**OPTION PERIODS:**

Option Period 1		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.11 IT Security VA Specialist	LEVEL 3	
C.16 PIA Specialist	LEVEL 3	
P.9 Project Manager	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
A.7 Programmer/Analyst	LEVEL 3	

Option Period 2		
Resource Category	Level of Expertise	Firm Per Diem Rate
C.3 IT Security TRA and C&A Analyst	LEVEL 3	
C.7 IT Security Design Specialist (General Stream)	LEVEL 3	
C.11 IT Security VA Specialist	LEVEL 3	
C.16 PIA Specialist	LEVEL 3	
P.9 Project Manager	LEVEL 3	
B.1 Business Analyst	LEVEL 3	
A.7 Programmer/Analyst	LEVEL 3	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

## ATTACHMENT 4.1

### MANDATORY EVALUATION CRITERIA

#### Workstream 1 – Strategy & Design

#### CORPORATE MANDATORY REQUIREMENTS

	Mandatory Corporate Requirement	Bidder's Response	
		Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
<b>M.1</b>	<p>The Bidder must demonstrate that it has been awarded a minimum 3 contracts where the bidder provided IT security professional services to a Government (Federal, Provincial, Territorial, Municipal, Crown Corporation) client or a commercial client. At least one contract must be for a large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a large commercial client. Large is defined as an organization with 5,000 employees or more.</p> <p>The Bidder must provide a minimum of 3 contract references and up to 6 contract references to demonstrate its compliance with Criteria ID M1. If more than 6 contract references were provided, only the first 6 will be evaluated. The aggregate value of the compliant contracts must be at least \$10M.</p> <p>Each referenced contract must be related to the delivery of IT security services in at least one of the following cyber security areas:</p> <ul style="list-style-type: none"><li>a) Cloud Security</li><li>b) Security and Risk Management</li><li>c) Endpoint Security</li><li>d) Communications &amp; Network Security</li></ul>	<p>The Bidder's substantiation of technical compliance with Criteria M.1 must be demonstrated by completing the Bidder Response Template in Attachment 4.3.</p> <p>The information contained in the completed response template in Attachment 4.3 in response to Criteria M.1 will also be used to evaluate R.1, R.2, R.3, and R.4.</p>	

	<p>e) Identity &amp; Access Management f) Security Operations g) Software Development and Application Security</p> <p>For each referenced contract, the Bidder must demonstrate the following:</p> <ul style="list-style-type: none"><li>a. The contract must have been with a single client.</li><li>b. The IT security services provided under the contract must have been performed within the 5 years prior to the solicitation publication date.</li><li>c. Referenced contract must have been a minimum of six (6) months in duration.</li><li>d. The scope of the services provided under each contract must include the following activities:<ul style="list-style-type: none"><li>i. Applying a security risk management methodology based on industry standards such as ISO, NIST, ISACA, AICPA, COBIT, or ITSG-33 in the development* of at least three of the following artifacts, in support of organizational transformation initiatives related to cyber security, where an organizational transformation initiative is the process of migrating an organization from an "as is" state to a "to be" state:<ul style="list-style-type: none"><li>1. Security strategy</li><li>2. Roadmap</li><li>3. System/security architecture</li><li>4. System design</li><li>5. Implementation strategy and plan</li><li>6. Migration/transition plans</li></ul></li></ul></li></ul> <p>OR</p> <ul style="list-style-type: none"><li>ii. Applying a security risk management methodology based on industry standards such as ISO, NIST, ISACA, AICPA, COBIT, or ITSG-33 in the implementation** of a cyber security operations program where a cyber security operations program includes integration of technical and process controls to safeguard organizational assets and systems as part of an identify-prevent-detect-respond-recover approach;</li></ul>		
--	---	--	--

	<p>e. The contract must have included the provision of resources in at least two out of the following four Resource Categories:</p> <table><tr><td><b>TBIPS RESOURCE CATEGORY</b></td></tr><tr><td>IT Security TRA and C&amp;A Analyst</td></tr><tr><td>IT Security Design Specialist</td></tr><tr><td>IT Security Methodology, Policy and Procedures Analyst</td></tr><tr><td>Risk Management Specialist</td></tr></table> <p>If the Bidder is using TBIPS contracts to demonstrate the above resource category experience, listing the TBIPS resource categories will suffice if the resource categories used to demonstrate are the same as the resource categories required in the solicitation as listed above. For other contracts, including TBIPS contracts with other resource categories different from the ones identified above, the work delivered under each resource category must include at least 50% of the associated tasks listed in Annex A – Statement of Work for that Resource Category.</p> <p>* Development is the process of creating or altering systems, along with the processes, practices, models, and methodologies used to develop them to ensure that a conformant system satisfies a specified set of requirements.</p> <p>** Implementation is defined as the realization of a system (or an application, execution of a plan, idea, model, design, specification, standard, algorithm, or policy) into an operational environment.</p>	<b>TBIPS RESOURCE CATEGORY</b>	IT Security TRA and C&A Analyst	IT Security Design Specialist	IT Security Methodology, Policy and Procedures Analyst	Risk Management Specialist	
<b>TBIPS RESOURCE CATEGORY</b>							
IT Security TRA and C&A Analyst							
IT Security Design Specialist							
IT Security Methodology, Policy and Procedures Analyst							
Risk Management Specialist							

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

### **Workstream 2 – Security Assurance**

#### **CORPORATE MANDATORY REQUIREMENTS**

	<b>Mandatory Corporate Requirement</b>	<b>Bidder's Response</b>	
		<b>Substantiation of Technical Compliance</b>	<b>Reference to Additional Documentation within the Bid</b>
<b>M.1</b>	<p>The Bidder must demonstrate that is has been awarded a minimum 3 contracts where the bidder provided IT security professional services to a Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a commercial client. At least one contract must be for a large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a large commercial client. Large is defined as an organization with 5,000 employees or more.</p> <p>The Bidder must provide a minimum of 3 contract references and up to 6 contract references to demonstrate its compliance with Criteria ID M1. If more than 6 contract references were provided, only the first 6 will be evaluated. The aggregate value of the compliant contracts must be at least \$3M.</p> <p>Each reference contract must be related to the delivery of IT security services in at least one of the following cyber security areas:</p> <ul style="list-style-type: none"><li>i. Cloud Security</li><li>ii. Security and Risk Management</li><li>iii. Endpoint Security</li><li>iv. Communications &amp; Network Security</li><li>v. Identity &amp; Access Management</li><li>vi. Security Operations</li><li>vii. Software Development and Application Security</li></ul>	<p>The Bidder's substantiation of technical compliance with Criteria M.1 must be demonstrated by completing the Bidder Response Template in Attachment 4.3.</p> <p>The information contained in the completed response template in Attachment 4.3 in response to Criteria M.1 will also be used to evaluate R.1, R.2 and R.3.</p>	

Solicitation No. - N° de l'invitation 24062-190077/B		Amd. No. - N° de la modif.  638el		Buyer ID - Id de l'acheteur 638el							
Client Ref. No. - N° de réf. du client 24062-190077		File No. - N° du dossier 638el24062-190077		CCC No./N° CCC - FMS No./N° VME							
		<p>For each referenced contract, the Bidder must demonstrate the following:</p> <ul style="list-style-type: none"><li>a) The contract must have been with a single client.</li><li>b) Referenced contracts must have been a minimum of six months in duration.</li><li>c) The IT security services provided under the contract must have been performed within the 5 years prior to the solicitation publication date.</li><li>d) The contract must have included the provision of resources in at least three out of the following four Resource Categories, or equivalent:</li></ul> <table><tr><th>RESOURCE CATEGORY</th></tr><tr><td>IT Security TRA and C&amp;A Analyst</td></tr><tr><td>IT Security Design Specialist</td></tr><tr><td>IT Security VA Specialist</td></tr><tr><td>PIA Specialist</td></tr></table> <p>If the Bidder is using TBIPS contracts to demonstrate the above resource category experience, listing the TBIPS resource categories will suffice if the resource categories used to demonstrate are the same as the resource categories required in the solicitation as listed above. For other contracts, including TBIPS contracts with other resource categories different from the ones identified above, the work delivered under each resource category must include at least 50% of the associated tasks listed in Annex A – Statement of Work for that Resource Category.</p> <ul style="list-style-type: none"><li>e) Each category referenced must include a minimum of 150 billable days. If any of the resources were provided in the same resource category, the 150 billable days would apply for</li></ul>		RESOURCE CATEGORY	IT Security TRA and C&A Analyst	IT Security Design Specialist	IT Security VA Specialist	PIA Specialist			
RESOURCE CATEGORY											
IT Security TRA and C&A Analyst											
IT Security Design Specialist											
IT Security VA Specialist											
PIA Specialist											

Solicitation No. - N° de l'invitation 24062-190077/B	Amd. No. - N° de la modif. 638el	Buyer ID - Id de l'acheteur 638el
Client Ref. No. - N° de réf. du client 24062-190077	File No. - N° du dossier 638el24062-190077	CCC No./N° CCC - FMS No./N° VME
	<p>each resource in the same resource category.</p> <p>A minimum of three different resource categories from the table above must be demonstrated across the compliant contracts. Each of these 3 different resource categories must have a minimum of 300 billable days demonstrated across the compliant contracts.</p>	

## ATTACHMENT 4.2

### RATED EVALUATION CRITERIA

#### Workstream 1 – Strategy & Design

#### CORPORATE POINT-RATED REQUIREMENTS

Corporate Rated Criteria	Maximum Points	Bidder Points
R1	25	
R2	30	
R3	15	
R4	30	
Total Maximum Points	100	
Minimum Pass Mark (60%)	60	

Criteria	Rated Requirement	Point Allocation	Max Points	Bidder's Response	
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
R.1	The Bidder should demonstrate that it has been awarded one or more contracts where the bidder provided IT security professional services as required in M1 to a large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a large commercial client, in addition to the one contract demonstrated in M1. Large is defined as an organization with 5,000 employees or more.	5 points per additional contract for a maximum of 25 points	25	The Bidder's substantiation of technical compliance with Criteria R.1 should be demonstrated using the response templates in Attachment 4.3, completed by the Bidder to substantiate its compliance with Criteria M.1. Any referenced contract that does not meet the requirements established in Criteria M.1 pertaining to	

Criteria	Rated Requirement	Point Allocation	Max Points	Bidder's Response	
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
				individual contract will not be considered.  Criteria R.1 will be evaluated using the information contained in the completed response templates in Attachment 4.3 in response to Criteria M.1. The Bidder must not submit additional contracts to demonstrate its compliance with Criteria R.1.	
<b>R.2</b>	The Bidder should demonstrate that it has been awarded contracts where the Bidder delivered IT security professional services as required in M1, which is related to Cloud Security or Identity and Access Management.	5 points per contract related to Cloud Security for a maximum of 15 points  5 points per contract related to Identity and Access Management for a maximum of 15 points	30	The Bidder's substantiation of technical compliance with Criteria R.2 should be demonstrated using the response templates in Attachment 4.3, completed by the Bidder to substantiate its compliance with Criteria M.1. Any referenced contract that does not meet the requirements established in Criteria M.1 pertaining to individual contract will not be considered.  Criteria R.2 will be evaluated using the information contained in the completed response templates in Attachment 4.3 in response to Criteria M.1.	

Criteria	Rated Requirement	Point Allocation	Max Points	Bidder's Response	
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
				The Bidder must not submit additional contracts to demonstrate its compliance with Criteria R.2.	
<b>R.3</b>	The Bidder should demonstrate that it has been awarded contracts where the Bidder provided IT security professional services as required in M1, which is related to the implementing of a cyber security operations program including integration of technical and process controls to safeguard organizational assets and systems as part of an identify-prevent-detect-respond-recover approach.	5 points per contract for a maximum of 15 points	15	<p>The Bidder's substantiation of technical compliance with Criteria R.3 should be demonstrated using the response templates in Attachment 4.3, completed by the Bidder to substantiate its compliance with Criteria M.1. Any referenced contract that does not meet the requirements established in Criteria M.1 pertaining to individual contract will not be considered.</p> <p>Criteria R.3 will be evaluated using the information contained in the completed response templates in Attachment 4.3 in response to Criteria M.1.</p> <p>The Bidder must not submit additional contracts to</p>	

Criteria	Rated Requirement	Point Allocation	Max Points	Bidder's Response	
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
<b>R.4</b>	<p>The Bidder should demonstrate that it has been awarded one or more contracts where the Bidder has provided a resource who has played a lead role in delivering the IT security services as required in M1. A lead role is defined as a role with the following responsibilities:</p> <ul style="list-style-type: none"> <li>a) Serving as the primary point of contact for the delivery of the deliverables;</li> <li>b) Providing technical and strategic leadership;</li> <li>c) Reporting to and providing briefings to senior management (Director level or above);</li> <li>d) Planning, assigning, and managing work;</li> <li>e) Tracking risks and issues;</li> <li>f) Resolving issues and monitoring progress on deliverables; and</li> <li>g) Accountable for the final product delivered to the client organization including sign-off on the final product.</li> </ul>	5 points per contract where it is demonstrated that the Bidder has provided resources with a lead role for a maximum of 30 points	30	<p>demonstrate its compliance with Criteria R.3.</p> <p>The Bidder's substantiation of technical compliance with Criteria R.4 should be demonstrated using the response templates in Attachment 4.3, completed by the Bidder to substantiate its compliance with Criteria M.1. Any referenced contract that does not meet the requirements established in Criteria M.1 pertaining to individual contract will not be considered.</p> <p>Criteria R.4 will be evaluated using the information contained in the completed response templates in Attachment 4.3 in response to Criteria M.1.</p> <p>The Bidder must not submit additional contracts to demonstrate its compliance with Criteria R.4.</p>	

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

### Workstream 2 – Security Assurance

### CORPORATE POINT-RATED REQUIREMENTS

Corporate Rated Criteria	Maximum Points	Bidder Points
R1	25	
R2	30	
R3	30	
Total Maximum Points	85	
Minimum Pass Mark (60%)	51	

Criteria	Rated Requirement	Point Allocation	Max Available Points	Bidder's Response	
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
R.1	The Bidder should demonstrate that it has been awarded one or more contracts where the bidder provided IT security professional services to a large Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a large commercial client, in addition to the one contract demonstrated in M1. Large is defined as an organization with 5,000 employees or more.	5 points per additional contract for a maximum of 25 points	25	The Bidder's substantiation of technical compliance with Criteria R.1 should be demonstrated using the response templates in Attachment 4.3, completed by the Bidder to substantiate its compliance with Criteria M.1.  Any referenced contract that does not meet the requirements established in Criteria M.1 pertaining to individual contract will not be considered.	

Criteria	Rated Requirement	Point Allocation	Max Available Points	Bidder's Response	
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
				The Bidder must not submit additional contracts to demonstrate its compliance with Criteria R.1.	
<b>R.2</b>	The Bidder should demonstrate that it has been awarded contracts where the bidder delivered IT security services related to Cloud Security OR Identity and Access Management.	5 points per contract related to Cloud Security for a maximum of 15 points  5 points per contract related to Identity and Access Management for a maximum of 15 points	30	The Bidder's substantiation of technical compliance with Criteria R.2 should be demonstrated using the response templates in Attachment 4.3, completed by the Bidder to substantiate its compliance with Criteria M.1.  Any referenced contract that does not meet the requirements established in Criteria M.1 pertaining to individual contract will not be considered.  The Bidder must not submit additional contracts to demonstrate its compliance with Criteria R.2.	
<b>R.3</b>	The Bidder should demonstrate its contract experience in providing professional services supplying all the resource categories listed in the table below for the required minimum	5 points per category for a maximum of 30 points	30	The Bidder's substantiation of technical compliance with Criteria R.2 should be	

Criteria	Rated Requirement	Point Allocation	Max Available Points	Bidder's Response															
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid														
	<p>billable days per resource category. Billable days are defined as days worked and billed to clients.</p> <table><tr><th>Resource Category</th><th>Minimum Billable Days</th></tr><tr><td>IT Security TRA and C&amp;A Analyst</td><td>300</td></tr><tr><td>IT Security Design Specialist</td><td>300</td></tr><tr><td>IT Security VA Specialist</td><td>100</td></tr><tr><td>PIA Specialist</td><td>100</td></tr><tr><td>Project Manager</td><td>100</td></tr><tr><td>Business Analyst</td><td>100</td></tr></table> <p>To qualify, the bidder must demonstrate the following for each resource category:</p> <p>a) The demonstrated minimum billable days must fall within five years prior to the solicitation publication date. The minimum billable days can be demonstrated by the cumulative total of billable days under different contracts;</p> <p>b) If the Bidder is using TBIPS contracts to demonstrate the above resource category experience, listing the TBIPS resource categories will suffice if the resource categories used to demonstrate are the same as the resource categories required in the solicitation as listed above. For other contracts, including TBIPS</p>	Resource Category	Minimum Billable Days	IT Security TRA and C&A Analyst	300	IT Security Design Specialist	300	IT Security VA Specialist	100	PIA Specialist	100	Project Manager	100	Business Analyst	100			demonstrated using the response template in Attachment 4.3.	
Resource Category	Minimum Billable Days																		
IT Security TRA and C&A Analyst	300																		
IT Security Design Specialist	300																		
IT Security VA Specialist	100																		
PIA Specialist	100																		
Project Manager	100																		
Business Analyst	100																		

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Criteria	Rated Requirement	Point Allocation	Max Available Points	Bidder's Response	
				Substantiation of Technical Compliance	Reference to Additional Documentation within the Bid
	contracts with other resource categories different from the ones identified above, the work delivered under each resource category must include at least 50% of the associated tasks listed in Annex A – Statement of Work for that Resource Category.				

**ATTACHMENT 4.3 BIDDER RESPONSE TEMPLATES**  
**BIDDER RESPONSE TEMPLATES FOR WORKSTREAM 1**

(REPLICATE THE FOLLOWING FORM AS REQUIRED)

1. BIDDER'S RESPONSE TEMPLATE FOR M1	
Bidder Name: _____ Bidder Contract Reference #: _____	
SECTION 1: CUSTOMER CONTACT INFORMATION	
Client Organization Name	
Client Contact Name	
E-mail Address or Phone Number	
Number of employees	
SECTION 2: CONTRACT INFORMATION	
Contract Value	
Contract Award Date	
Contract End Date	
TBIPS Contract?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Cyber Security Areas the contract is related to:	<input type="checkbox"/> Cloud Security <input type="checkbox"/> Security and Risk Management <input type="checkbox"/> Endpoint Security <input type="checkbox"/> Communications & Network Security <input type="checkbox"/> Identity & Access Management

Solicitation No. - N° de l'invitation  
24062-190077/B

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

Client Ref. No. - N° de réf. du client  
24062-190077

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

	<input type="checkbox"/> Security Operations
	<input type="checkbox"/> Software Development and Application Security
Is this contract with a single client?	<input type="checkbox"/> Yes <input type="checkbox"/> No
The IT security services provided under the contract performed within the 5 years prior to the solicitation publication date?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Solicitation No. - N° de l'invitation  
24062-190077/B

Client Ref. No. - N° de réf. du client  
24062-190077

Amd. No. - N° de la modif.

File No. - N° du dossier  
638e124062-190077

Buyer ID - Id de l'acheteur  
638e1

CCC No./N° CCC - FMS No./N° VME

Contract Summary (up to one paragraph description of the key scope and responsibilities)

The scope of the services provided under this contract includes the following activities:

<b>(NOTE:</b> The substantiation must not simply be a repetition of the requirement but must explain and demonstrate how the Bidder meets the requirement. The Bidder can provide screen captures and technical or end-user documentation to supplement their responses.)	
<input type="checkbox"/> Applying a security risk management methodology based on industry standards such as ISO, NIST, ISACA, AICPA, COBIT, or ITSG-33 in the development of at least three of the following artifacts, in support of organizational transformation initiatives related to cyber security, where an organizational transformation initiative is the process of migrating an organization from an "as is" state to a "to be" state: <ul style="list-style-type: none"><li><input type="checkbox"/> Security strategy</li><li><input type="checkbox"/> Roadmap</li><li><input type="checkbox"/> System/security architecture</li><li><input type="checkbox"/> System design</li><li><input type="checkbox"/> Implementation strategy and plan</li><li><input type="checkbox"/> Migration/transition plans</li></ul>	<b>Substantiation</b>  To demonstrate, the bidder must: <ul style="list-style-type: none"><li>a) Describe the tasks where the Bidder demonstrated experience in developing artifacts that support organizational transformation initiatives related to cyber security;</li><li>b) Describe each of the artifacts developed and how it supported organizational transformation initiatives related to cyber security.</li><li>c) Describe the security risk management methodology implemented that is based on industry standards such as ISO, NIST, ISACA, AICPA, COBIT, or ITSG-33</li></ul>

<p><input type="checkbox"/> Applying a security risk management methodology based on industry standards such as ISO, NIST, ISACA, AICPA, COBIT, or ITSG-33 in the implementation of a cyber security operations program where a cyber security operations program includes integration of technical and process controls to safeguard organizational assets and systems as part of an identify-prevent-detect-respond-recover approach;</p>	<p><b>Substantiation</b></p> <p>To demonstrate, the bidder must:</p> <p>a) Describe the tasks where the Bidder demonstrated experience in the implementation a cyber security operations program;</p> <p>b) Describe how the identify-prevent-detect-respond-recover approach was implemented; and</p> <p>c) Describe the security risk management methodology implemented that is based on industry standards such as ISO, NIST, ISACA, AICPA, COBIT, or ITSG-33.</p>
---	--

Solicitation No. - N° de l'invitation  
24062-190077/B

Client Ref. No. - N° de réf. du client  
24062-190077

Amd. No. - N° de la modif.

Buyer ID - Id de l'acheteur  
638el

File No. - N° du dossier  
638el24062-190077

CCC No./N° CCC - FMS No./N° VME

Provided any resources who played a lead role as defined in R4?

- ☐ Yes  
☐ No

If Yes, please provide the name, resource category and description of responsibility of the lead resource. The substantiation must not be a repetition of the tasks required in R4, but must explain responsibilities and demonstrate how the resource carried out each responsibility.

To demonstrate, the Bidder must describe the tasks where the resource played a lead role. These tasks include the following:

- a) Serving as the primary point of contact for the delivery of the deliverables;
- b) Providing technical and strategic leadership;
- c) Reporting to and providing briefings to senior management (Director level or above);
- d) Planning, assigning, and managing work;
- e) Tracking risks and issues;
- f) Resolving issues and monitoring progress on deliverables; and
- g) Accountable for the final product delivered to the client organization including sign-off on the final product.

SECTION 3: RESOURCE DETAILS		
The contract includes the provision of resources in the following resource categories:		
Resource Category (as it appears in the referenced contract)	Resource Category required in M1	Non-M1-Matching Categories ONLY  Tasks performed under the Resource Category in the referenced contract, including substantiation (The substantiation must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.)

**BIDDER RESPONSE TEMPLATES FOR WORKSTREAM 2**

(REPLICATE THE FOLLOWING FORM AS REQUIRED)

<b>1. BIDDER'S RESPONSE TEMPLATE FOR M1</b>	
Bidder Name: _____ Bidder Contract Reference #: _____	
<b>SECTION 1: CUSTOMER CONTACT INFORMATION</b>	
Client Organization Name	
Client Contact Name	
E-mail Address or Phone Number	
Number of employees	
<b>SECTION 2: CONTRACT INFORMATION</b>	
Contract Value	
Contract Award Date	
Contract End Date	
TBIPS Contract?	<input type="checkbox"/> Yes <input type="checkbox"/> No
The IT security services provided under the contract performed within the 5 years prior to the solicitation publication date?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Cyber Security Areas the contract is related to:	<input type="checkbox"/> Cloud Security <input type="checkbox"/> Security and Risk Management

	<div><input type="checkbox"/> Endpoint Security</div> <div><input type="checkbox"/> Communications &amp; Network Security</div> <div><input type="checkbox"/> Identity &amp; Access Management</div> <div><input type="checkbox"/> Security Operations</div> <div><input type="checkbox"/> Software Development and Application Security</div>
Is this Contract with a single client?	<div><input type="checkbox"/> Yes</div> <div><input type="checkbox"/> No</div>

Solicitation No. - N° de l'invitation  
24062-190077/B

Client Ref. No. - N° de réf. du client  
24062-190077

Amd. No. - N° de la modif.

File No. - N° du dossier  
638e124062-190077

Buyer ID - Id de l'acheteur  
638e1

CCC No./N° CCC - FMS No./N° VME

Contract Summary (up to one paragraph description of the key scope and responsibilities)

SECTION 3: RESOURCE DETAILS				
The contract included the provision of resources in the following resource categories:				
Resource Name	Resource Category (as it appears in the referenced contract)	Resource Category required in M1	Billable Days for the referenced resource category	<u>Non-M1-Matching Categories</u> <u>ONLY</u>  Tasks performed under the Resource Category in the referenced contract, including substantiation (The substantiation must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.)

2. BIDDER'S RESPONSE TEMPLATE FOR R3

Resource Category	Resource Name	<u>B</u> Resource Category as it appears in the Contract	<u>Non-R3-Matching Categories ONLY</u> List of Tasks for the Resource Category in Column B	Number of Billable Days	Billable days start and end dates	Client Organization Name	Contract Number	Contract Period
IT Security TRA and C&A Analyst					(NOTE: all demonstrated billable days must fall within the 5 years prior to the solicitation publication date)  Start Date: dd/mm/yyyy  End Date: dd/mm/yyyy			Start Date: dd/mm/yyyy  End Date: dd/mm/yyyy
IT Security Design Specialist								
IT Security VA Specialist								
PIA Specialist								
Project Manager								
Business Analyst								

## ATTACHMENT 5.1

### FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY - CERTIFICATION

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit [Employment and Social Development Canada \(ESDC\) - Labour's](#) website.

Date: \_\_\_\_\_ (YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

- ☐ A1. The Bidder certifies having no work force in Canada.
- ☐ A2. The Bidder certifies being a public sector employer.
- ☐ A3. The Bidder certifies being a federally regulated employer being subject to the [Employment Equity Act](#).
- ☐ A4. The Bidder certifies having a combined work force in Canada of less than 100 permanent full-time and/or permanent part-time employees.

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

- ☐ A5.1 The Bidder certifies already having a valid and current [Agreement to Implement Employment Equity](#) (AIEE) in place with ESDC-Labour.

OR

- ☐ A5.2 The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC-Labour.

B. Check only one of the following:

- ☐ B1. The Bidder is not a Joint Venture.

OR

- ☐ B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions).