BID SOLICITATION
FOR A CONTRACT AGAINST A SUPPLY ARRANGEMENT FOR TASK-BASED INFORMATICS PROFESSIONAL SERVICES (TBIPS) VARIOUS RESOURCE CATEGORIES - LEVEL 2 AND 3 UNDER TBIPS STREAM 6: CYBER PROTECTION SERVICES FOR CANADA BORDER SERVICES AGENCY (CBSA)

Table of Contents

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 - Resources Assessment Criteria and Response Table
Appendix D to Annex A - Certifications at the TA Stage

Annex A1: Glossary

Annex B: Basis of Payment

Annex C: Security Requirements Check List
Annex C1 Security Classification Guide

List of Attachments to Part 1
Attachment 1.1: Summary of changes from 47419-214911/A

List of Attachments to Part 3 (Bid Preparation Instructions)
Attachment 3.1: Bid Submission Form
Attachment 3.2: Electronic Payment Instruments

List of Attachments to Part 4 (Evaluation Procedures and Basis of Selection):
Attachment 4.1: Mandatory Technical Criteria
Attachment 4.2: Point-Rated Technical Criteria
Attachment 4.3: Forms (Corporate evaluation criteria)
Attachment 4.4: Pricing Schedule

List of Attachments to Part 5 (Certifications):
Attachment 5.1: Federal Contractors Program for Employment Equity – Certification

BID SOLICITATION
FOR A CONTRACT AGAINST A SUPPLY ARRANGEMENT FOR TASK-BASED INFORMATICS PROFESSIONAL SERVICES (TBIPS) VARIOUS RESOURCE CATEGORIES - LEVEL 2 AND 3 UNDER TBIPS STREAM 6: CYBER PROTECTION SERVICES FOR CANADA BORDER SERVICES AGENCY (CBSA)

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, the Basis of Payment, the Security Requirements Checklist and any other annexes

1.2 Summary

a. This bid solicitation cancels and supersedes previous bid solicitation number (47419-214911/A) dated May 7, 2021 with a bid closing date of May 27, 2021. this document replaces the previous version entirely. Summary of changes are provided in Attachment to Part 1

b. This bid solicitation is being issued to satisfy the requirement of CBSA (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 one (1) contract for one (1) year plus two (2) x 1 one-year irrevocable options allowing Canada to extend the term of the contract

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 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), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Canadian Free Trade Agreement (CFTA), the Canada-Ukraine Free Trade Agreement (CUFTA), the Canada-United Kingdom Trade Continuity Agreement (Canada-UK TCA) and the Canada-Korea Free Trade Agreement (CKFTA).

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 is to establish a contract with task authorizations for the delivery of the requirement detailed in the bid solicitation across Canada, excluding locations within Yukon, Northwest Territories, Nunavut, Quebec, and Labrador that are subject to Comprehensive Land Claims Agreements (CLCAs). Any requirement for deliveries within CLCAs areas within Yukon, Northwest Territories, Nunavut, Quebec, or Labrador will be treated as a separate procurement, outside the resulting contract.

h. Bidders must 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

(i) Only TBIPS SA Holders holding a TBIPS SA for Tier 2 at the time of bid closing, in all required resource categories in this solicitation, in the National Capital Region under the EN578-170432 series of SAs, with a Facility Security Clearance (FSC) at the Secret level, 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.

(j) 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 #EN578-055605 as that joint venture at the time of bid closing in order to submit a bid.

(k) 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":

Resources Categories	Level	Estimated number of resources required
TBIPS Stream 6: Cyber Protection Services		
C.1 Strategic Information Technology Security Planning & Protection Consultant	2	1
C.1 Strategic Information Technology Security Planning & Protection Consultant	3	1

Resources Categories	Level	Estimated number of resources required
C.3 Information Technology Security TRA and C&A Analyst	2	1
C.3 Information Technology Security TRA and C&A Analyst	3	1
C.7 Information Technology Security Design Specialist	2	2
C.7 Information Technology Security Design Specialist	3	2
C.8 Network Security Analyst	2	1
C.8 Network Security Analyst	3	1
C.9 Information Technology Security Systems Operator	2	2
C.9 Information Technology Security Systems Operator	3	1
C.11 Information Technology Security Vulnerability Analysis Specialist	2	1
C.11 Information Technology Security Vulnerability Analysis Specialist	3	1
C.14 Information Technology Security Research and Development Specialist	2	1
C.14 Information Technology Security Research and Development Specialist	3	3
C.16 Privacy Impact Assessment Specialist	2	1
C.16 Privacy Impact Assessment Specialist	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.

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 (2020-05-28) 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.

2.2 Submission of Bids

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

Note: For bidders needing to register with epost Connect the email address is: tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca.

Interested Bidders must register a few days prior to solicitation closing date.

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

2.3 Enquiries - Bid Solicitation

(a) All enquiries must be submitted in writing to the Contracting Authority no later than ten (10) 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;

(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 *(insert at contract if another province or territory has been selected by the bidder)*

***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 Improvement of Requirement During Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reasons for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled "Enquiries - Bid Solicitation". Canada will have the right to accept or reject any or all suggestions.

2.7 Basis for Canada's Ownership of Intellectual Property

Canada Border Services Agency (CBSA) has determined that any intellectual property rights arising from the performance of the Work under the resulting contract will belong to Canada, for the following reasons, as set out in the *Policy on Title to Intellectual Property Arising Under Crown Procurement Contracts*:

(i) statutes, regulations or prior obligations of Canada to a third party or parties preclude Contractor ownership of the Intellectual Property Rights in Foreground Information;

2.8 Volumetric Data

The estimated number of resources required per resource category data 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.

2.9 Bid Challenge and Recourse Mechanisms

(a) Several mechanisms are available to potential suppliers to challenge aspects of the procurement process up to and including contract award.

(b) Canada encourages suppliers to first bring their concerns to the attention of the Contracting Authority. Canada's Buy and Sell website, under the heading "Bid Challenge and Recourse Mechanisms" contains information on potential complaint bodies such as:

(i) Office of the Procurement Ombudsman (OPO)

(ii) Canadian International Trade Tribunal (CITT)

(c) Suppliers should note that there are strict deadlines for filing complaints, and the time periods vary depending on the complaint body in question. Suppliers should therefore act quickly when they want to challenge any aspect of the procurement process.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

(a) **Epost Connect Bid Submission**

a. Canada requires 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.

b. The bid must be gathered per section and separated as follows:

i. Section I: Technical Bid

ii. Section II: Financial Bid

iii. Section III: Certifications

iv. Section IV: Additional Information

c. 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) Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

(c) **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.

(d) **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.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32573)

(e) **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.

(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. .

(f) **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.

(C) **Corporate Experience for CM1 and CR5**

In evaluating corporate experience (CM1 and CR5), Canada will consider the corporate experience described by the Bidder that is:

a) the Bidder’s own corporate experience (including the experience of any one or more members of a joint venture bidder;
b) the experience of a parent corporation or partnership that controls the Bidder;
c) the experience of a subsidiary controlled by the Bidder; and
d) the experience of a corporation that is controlled by the same parent corporation or partnership that controls the Bidder,

where control means that the controlling entity owns a sufficient interest in the controlled entity that it is entitled to appoint or elect the majority of the board of directors. If the Bidder has relied on one of the entities listed in (b), (c), or (d), the Bidder must, upon request, provide Canada with documentation to demonstrate its relationship with the entity. PWGSC will not consider an entity to have corporate experience if the experience claimed is the result of having acquired the assets of another entity.

If the Bidder has relied on the experience of one of the entities listed in (b), (c), or (d), then, at contract award, the Bidder must, if requested by Canada, provide the guarantee of that entity for the performance of the resulting contract; if the Bidder cannot provide such a guarantee within 2 weeks of being advised that it has been recommended for contract award, Canada will be entitled to set aside its bid.

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

(A) In conducting its evaluation of the bids, Canada may, but will have no obligation to request that a bidder provide customer references. If Canada sends such a written request, the bidder will have 2 working days to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive. These customer references must each confirm if requested by PWGSC, the facts identified in the Bidder's bid, as required by Attachment "4.1" and "4.2".

(B) The form of question to be used to request confirmation from customer references is as follows:

For evaluation criteria CM1, CM2, CR1, CR2, CR3, CR5

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 4.4. The total amount of Applicable Taxes must be shown separately, if applicable. 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) **Variation in Resource Rates By Time Period**: For any given resource category, where the financial tables provided by Canada allow different firm rates to be charged for a resource category during different time periods:

(i) the rate bid must not increase by more than 5% from one time period to the next, and

(ii) the rate bid for the same resource category during any subsequent time period must not be lower than the rate bid for the time period that includes the first month of the Initial Contract Period.

(c) **Variation in Resource Rates By Level:** Where the financial tables provided by Canada allow different firm rates to be charged for different levels of experience within the same resource category and time period, for any such resource category and time period:

(i) the rate bid for level three must be the same or higher than that bid for level two, and

(ii) the rate bid for level two must be the same or higher than the rate bid for level one.

(d) **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.

(e) **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.

Note to Bidders: If Canada receives 4 or fewer Bids [the same number of bids as in the article entitled “Phased Bid Compliance Process”] by the bid solicitation closing date, the above sub-article entitled “Blank Prices” will not apply.

(f) **Electronic Payment of Invoices – Bid**: If you are willing to accept payment of invoices by Electronic Payment Instruments, complete Attachment “3.2” Electronic Payment Instruments, to identify which ones are accepted. If Attachment “3.2” Electronic Payment Instruments is not completed, it will be considered as if Electronic Payment Instruments are not being accepted for payment of invoices. Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

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 Canada will evaluate the bids.

(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) Canada will conduct the Phased Bid Compliance Process (PBCP) described below for this requirement ONLY if Canada receives four or fewer bids in response to the requirement 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 (2020-05-28) 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) **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 only to mandatory technical criteria identified by the superscript (^{PB}). Mandatory technical criteria not identified by the superscript (^{PB}) will not be subject to the Phased Bid Compliance Process.

CM1 (PB)	**Bidder's (*) billable ($) providing IM/IT *Cyber Security* Professional Services involving Public Cloud infrastructure.** **(*) In evaluating corporate experience for this criteria, Canada will consider the corporate experience referred to in:** **Part 3, Section 3.2** **Section I: Technical Bid** **Substantiation of Technical Compliance** **Paragraph C (page 14-15)**

(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) **Resources Evaluation at TA Stage**

(i) Resources will not be evaluated as part of this bid solicitation.

(ii) Resources will only be assessed after contract award once specific tasks are requested of the Contractor. After contract award, the Task Authorization process will be in accordance with Part 7 – Resulting Contract Clauses, the Article titled "Task Authorization". When a Task Authorization Form (TA Form) is issued, the Contractor will be requested to propose a resource to satisfy the specific requirement based on the TA Form's Statement of Work. The proposed resource will then be assessed against the criteria identified in the Contract's Statement of Work in accordance with Appendix C of Annex A.

(d) **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) On the third working day after sending out the reference check request, if Canada has not received a response, Canada will notify the Bidder by email, to allow the Bidder to contact its reference directly to ensure that it responds to Canada within 5 working days. If the individual named by a Bidder is unavailable when required during the evaluation period, the Bidder may provide the name and email address of an alternate contact person from the same customer. Bidders will only be provided with this opportunity once for each customer, and only if the originally named individual is unavailable to respond (i.e., the Bidder will not be provided with an opportunity to submit the name of an alternate contact person if the original contact person indicates that he or she is unwilling

or unable to respond). The 5 working days will not be extended to provide additional time for the new contact to respond.

(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

Highest Responsive Combined Rating of Technical Merit and Price

(a) The financial evaluation will be conducted using the firm per diem rates provided by the responsive bid(s).

(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, 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 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.

TABLE 1 - MAXIMUM POINTS ASSIGNED					
Resource Category	**Level of Expertise**	**Initial Period**	**Option 1**	**Option 2**	**TOTAL**
TBIPS Stream 6: Cyber Protection Services					
C.1 Strategic Information Technology Security Planning & Protection Consultant	2	20	20	20	**60**
C.1 Strategic Information Technology Security Planning & Protection Consultant	3	20	20	20	**60**
C.3 Information Technology Security TRA and C&A Analyst	2	20	20	20	**60**
C.3 Information Technology Security TRA and C&A Analyst	3	20	20	20	**60**
C.7 Information Technology Security Design Specialist	2	20	20	20	**60**
C.7 Information Technology Security Design Specialist	3	20	20	20	**60**
C.8 Network Security Analyst	2	20	20	20	**60**
C.8 Network Security Analyst	3	20	20	20	**60**
C.9 Information Technology Security Systems Operator	2	20	20	20	**60**
C.9 Information Technology Security Systems Operator	3	20	20	20	**60**
C.11 Information Technology Security Vulnerability Analysis Specialist	2	20	20	20	**60**
C.11 Information Technology Security Vulnerability Analysis Specialist	3	20	20	20	**60**
C.14 Information Technology Security Research and Development Specialist	2	20	20	20	**60**
C.14 Information Technology Security Research and Development Specialist	3	20	20	20	**60**
C.16 Privacy Impact Assessment Specialist	2	20	20	20	**60**
C.16 Privacy Impact Assessment Specialist	3	20	20	20	**60**
TOTAL		320	320	320	**960**

(iii) **STEP 3 - FINANCIAL SCORE**: Points allocated under STEP 2 for each period and Resource Category 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
Programmer	150 (75 pts. per year)	$400.00	$400.00	$420.00	$440.00	$450.00	$450.00
Business Analyst	100 (50 pts. per year)	$600.00	$600.00	$600.00	$620.00	$650.00	$680.00
Project Manager	50 (25 pts. per year)	$555.00	$580.00	$750.00	$785.00	$700.00	$735.00
TOTAL	300						

STEP 1 - Establishing the lower and upper median band limits for each year and each resource category

(Median 1) For the Programmer Resource Category, the year 1 median would be $420.00. The lower median band limit would be $378.00 and higher median band limit would be $546.00.

(Median 2) For the Programmer Resource Category, the year 2 median would be $440.00. The lower median band limit would be $396.00 and higher median band limit would be $572.00.

(Median 3) For the Business Analyst Resource Category, the year 1 median would be $600.00. The lower median band limit would be $540.00 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 $558.00 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 $630.00 and higher median band limit would be $910.00.

(Median 6) For the Project Manager Resource Category, the year 2 median would be $735.00. The lower median band limit would be $661.50 and higher median band limit would be $955.50.

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 = 0 points (outside the lower and higher median band limits)

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 = 68.18 points (based on the following calculation = (Lowest rate of $400.00 / Bidder's proposed rate of $440.00) 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 = 23.41 points (based on the following calculation = (Lowest rate of $735.00 / Bidder's proposed rate of $785) Multiplied by 25 pts)

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 50 pts)
Business Analyst Year 2 = 44.12 points (based on the following calculation = (Lowest rate of $600 / Bidder's proposed rate of $680.00) Multiplied by 50 pts)

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 + 0 = Total Financial Score of 250.00 points out of a possible 300 points

Bidder 2: 71.43 + 68.18 + 50 + 48.39 + 23.33 + 23.41 = Total Financial Score of 284.74 points out of a possible 300 points

Bidder 3: 66.67 + 66.67 + 46.15 + 44.12 + 25 + 25 = Total Financial Score of 273.61 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 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.

TABLE 3 - MAXIMUM POINTS ASSIGNED					
Resource Category	**Level of Expertise**	**Initial Period**	**Option 1**	**Option 2**	**TOTAL**
TBIPS Stream 6: Cyber Protection Services					
C.1 Strategic Information Technology Security Planning & Protection Consultant	2	20	20	20	**60**
C.1 Strategic Information Technology Security Planning & Protection Consultant	3	20	20	20	**60**
C.3 Information Technology Security TRA and C&A Analyst	2	20	20	20	**60**
C.3 Information Technology Security TRA and C&A Analyst	3	20	20	20	**60**
C.7 Information Technology Security Design Specialist	2	20	20	20	**60**
C.7 Information Technology Security Design Specialist	3	20	20	20	**60**
C.8 Network Security Analyst	2	20	20	20	**60**
C.8 Network Security Analyst	3	20	20	20	**60**
C.9 Information Technology Security Systems Operator	2	20	20	20	**60**
C.9 Information Technology Security Systems Operator	3	20	20	20	**60**
C.11 Information Technology Security Vulnerability Analysis Specialist	2	20	20	20	**60**
C.11 Information Technology Security Vulnerability Analysis Specialist	3	20	20	20	**60**
C.14 Information Technology Security Research and Development Specialist	2	20	20	20	**60**
C.14 Information Technology Security Research and Development Specialist	3	20	20	20	**60**
C.16 Privacy Impact Assessment Specialist	2	20	20	20	**60**
C.16 Privacy Impact Assessment Specialist	3	20	20	20	**60**
TOTAL		320	320	320	**960**

(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

(a) Evaluation of Bid

Selection Process: The following selection process will be conducted :

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. One contract may be awarded in total as a result of this bid solicitation.

iii. 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: 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:

$$\frac{\text{Technical Score}}{\text{Maximum Technical Points (Bidders, please refer to the maximum technical points}} \times 70 = \text{Total Technical Score}$$

(B) Calculation of Total Financial Score: 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:

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

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

Total Technical Score + Total Financial Score = Total Bidder Score

iv. 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.

v. If more than one Bidder is ranked first because of identical overall scores, then the Bidder with the higher Technical Score will become the top-ranked bidder

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" 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" 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" 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 5.1, Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

(b) 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;

(ii) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses.

(b) Before issuance of a Task Authorization, the following conditions must be met:

(i) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses.

(ii) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites.

(c) 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.

(d) 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.

(e) 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.*

Delete this title and the following sentence at contract award.

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 Canada Border Services Agency (CBSA)

(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) **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.

(c) **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 Appendix B of Annex A.

(ii) The draft Task Authorization will contain the details of the activities to be performed, and must also contain the following information:

(A) the contract number;

(B) the task number;

(C) 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);

(D) the categories of resources and the number required;

(E) a description of the work for the task outlining the activities to be performed and identifying any deliverables (such as reports);

(F) the start and completion dates;

(G) any option(s) to extend initial end date (if applicable);

(H) milestone dates for deliverables and payments (if applicable);

(I) the number of person-days of effort required;

(J) whether the work requires on-site activities and the location;

(K) the language profile of the resources required;

(L) the level of security clearance required of resources;

(M) 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

(N) any other constraints that might affect the completion of the task.

(d) **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.

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

To be validly issued, all TA must include the following signatures:

(i) for any TA, inclusive of revisions, the TA must be signed by the Technical Authority, the Contractor and the PSPC Contracting Authority.

Any TA that does not bear the appropriate signature(s) 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 sub-article (i) above; any suspension or reduction notice is effective upon receipt.

(f) **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) 1st quarter: April 1 to June 30;

(B) 2nd quarter: July 1 to September 30;

(C) 3rd quarter: October 1 to December 31; and

(D) 4th quarter: January 1 to March 31.

The data must be submitted to the Contracting Authority no later than 15 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.

(g) **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.

(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. Each time the Contractor does not submit a valid response, the Contractor agrees Canada may at its option decrease the Minimum Contract Value in the clause titled "Minimum Work Guarantee" by 2%. This decrease will be evidenced for administrative purposes only through a contract amendment issued by the Contracting Authority (which does not require the agreement of the Contractor).

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 $20,000.00 (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 (2020-05-28), 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 Common #19 and related clauses provided by the Contract Security Program) as set out under Annex “B” to the Supply Arrangement EN578-170432, applies to and forms part of the Contract.

1. The contractor/offeror must, at all times during the performance of the contract/standing offer, hold a valid facility security clearance at the level of secret, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC)
2. The contractor/offeror 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 reliability status or secret as required, granted or approved by the CSP, PWGSC
3. The contractor/offeror must not remove any protected/classified information from the identified work site(s), and the contractor/offeror 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 the CSP, PWGSC
5. The contractor/offeror must comply with the provisions of the:
    a. Security Requirements Check List and security guide (if applicable), attached at Annex C
    b. Contract Security Manual (latest edition)

(a) Additionally, resources may be assessed for Reliability or Secret, or a combination as applicable, Status by the Technical Authority prior to commencing the Work, and from time to time throughout the Contract Period. The assessment may include a credit check. Upon request of the Technical Authority, in respect of any given resource, the Contractor must submit:

(i) the current level of security clearance granted or approved by CISD/PWGSC; and

(ii) a completed signed TBS 330-23 Form - Personnel Screening, Consent and Authorization Form (http://www.tbs-sct.gc.ca/tbsf-fsct/330-23-eng.pdf).

(b) In the event a resource does not pass the Technical Authority's assessment, Canada may immediately, and without further notice, terminate the Contract for default in accordance with the *General Conditions.*

7.6 Use of Personal Protective Equipment and Occupational Health and Safety (OHS) Guideline(s)

(a) The Contractor must comply with Government of Canada onsite requirements in respect of Personal Protective Equipment (PPE) and adhere to Occupational Health and Safety (OHS) guidelines in force in the workplace.

(b) The Contractor will provide its resources the following individual PPE for working on site: prescribed face covering mask, gloves, protective shield, and anything else that is required as a pre-requisite to entry and to work on Government of Canada premises. Canada reserves the right to modify the list of PPE and OHS guidelines, if required, to include any future recommendations proposed by the Public Health Agencies.

(c) The Contractor warrants that its resources will wear the PPE mentioned above when onsite and follow at all times the Occupational Health and Safety (OHS) guidelines in force in the workplace during the contract period. If resources are not wearing the prescribed PPE and/or are not following the Occupational Health and Safety (OHS) guidelines in force in the workplace, they will not be permitted access to government of Canada sites.

7.7 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 one (1) year 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 (2) additional 1 year periods 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.

7.8 Authorities

(a) Contracting Authority

The Contracting Authority for the Contract is:

Name: Sylvain Desbois
Title: Supply specialist
Public Works and Government Services Canada
Professional Services Procurement Directorate
Professional Services Division ZV
Telephone: (819) 962-8660
E-mail address: sylvain.desbois@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 *(Insert at contract award)*

The Technical Authority for the Contract is:

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.

In its absence,

The Technical Authority for the Contract is *(Insert 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** *(Insert at contract award)*

7.9 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.

7.10 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.

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 included 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) **Electronic Payment of Invoices – Contract**

The Contractor accepts to be paid using any of the following Electronic Payment Instrument(s):

(i) Visa Acquisition Card;

(ii) MasterCard Acquisition Card;

(iii) Direct Deposit (Domestic and International);

(iv) Electronic Data Interchange (EDI);

(v) Wire Transfer (International Only);

(vi) Large Value Transfer System (LVTS) (Over $25M)

Note to Bidders: *If applicable, the Electronic Payment Instrument(s) indicated by the Bidder in Attachment 3.2 will be included in any resulting contract.*

(f) **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.

(g) **Payment Credits**

(i) **Failure to Provide Resource**:

(A) If the Contractor does not provide a required professional services resource that has all the required qualifications within the time prescribed by the Contract, the

Contractor must credit to Canada an amount equal to the per diem rate (based on a 7.5-hour workday) of the required resource for each day (or partial day) of delay in providing the resource, up to a maximum of 10 days.

(B) Corrective Measures: If credits are payable under this Article for two consecutive months or for three months in any 12-month period, the Contractor must submit a written action plan describing measures it will implement or actions it will undertake 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 20 working days to rectify the underlying problem.

(C) **Termination for Failure to Meet Availability Level**: In addition to any other rights it has under the Contract, Canada may terminate the Contract for default in accordance with the General Conditions by giving the Contractor three months' written notice of its intent, if any of the following apply:

(1) the total amount of credits for a given monthly billing cycle reach a level of 10% of the total billing for that month; or

(2) the corrective measures required of the Contractor described above are not met.

This termination will be effective when the three month notice period expires, unless Canada determines that the Contractor has implemented the corrective measures to Canada's satisfaction during those three months.

(ii) **Credits Apply during Entire Contract Period**: The Parties agree that the credits apply throughout the Contract Period.

(iii) **Credits represent Liquidated Damages**: The Parties agree that the credits are liquidated damages and represent their best pre-estimate of the loss to Canada in the event of the applicable failure. No credit is intended to be, nor will it be construed as, a penalty.

(iv) **Canada's Right to Obtain Payment**: The Parties agree that these credits are a liquidated debt. To collect the credits, Canada has the right to hold back, draw back, deduct or set off from and against any money Canada owes to the Contractor from time to time.

(v) **Canada's Rights & Remedies not Limited**: The Parties agree that nothing in this Article limits any other rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default) or under the law generally.

(vi) **Audit Rights**: The Contractor's calculation of credits under the Contract is subject to verification by government audit, at the Contracting Authority's discretion, before or after payment is made to the Contractor. The Contractor must cooperate fully with Canada during the conduct of any audit by providing Canada with access to any records and systems that Canada considers necessary to ensure that all credits have been accurately credited to Canada in the Contractor's invoices. If an audit demonstrates that past invoices contained errors in the calculation of the credits, the Contractor must pay to Canada the amount the audit reveals was required to be credited to Canada, plus interest, from the date Canada remitted the excess payment until the date of the refund (the interest rate is the Bank of Canada's discount annual rate of interest in effect on the date the credit was first owed to Canada, plus 1.25% per year). If, as a result of conducting an audit, Canada determines that the Contractor's records or systems for identifying, calculating or recording the credits are inadequate, the Contractor must implement any additional measures required by the Contracting Authority.

(h) **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, closure or there are enhanced measures to restrict access to 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, closure or restricted access.

(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

7.11 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 of each invoice to the Technical Authority and *(Insert at contract award)* and a copy to the Contracting Authority.

7.12 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.

7.13 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.

7.14 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario. *(or if different, insert at contract award)*

7.15 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 (2020-05-28), 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 _____ *(insert date of bid)* *(if the bid was clarified or amended, insert the time of contract award)*, as clarified on _____ "or" as amended _____ *(insert date(s) of clarification(s) or amendment(s) if applicable.)*

7.16 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.*

7.17 Foreign Nationals (Foreign Contractor)

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

7.18 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.

7.19 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).

7.20 Joint Venture Contractor *(Delete if N/A)*

(a) The Contractor confirms that the name of the joint venture is _____ and that it is comprised of the following members: *[list all the joint venture members named in the Contractor's original bid]*.

(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.*

7.21 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.

7.22 Professional Services for Pre-Existing Software

(a) **Pre-Existing Software**: The "**Pre-Existing Software**" consists of the computer programs listed in Annex A, which are either proprietary to Canada or licensed to Canada by a third party, in respect of which Canada requires certain professional services.

(b) **Software Services**: During the Contract Period, the Contractor must provide the Client with the following "**Services for Pre-Existing Software**" as and when requested by Canada through a Task Authorization:

(i) accessing, downloading, storing, installing, loading, processing, configuring and implementing any additional software code related to the Pre-Existing Software (such as new releases, versions, patches, and bug fixes), as soon as it becomes available;

(ii) keeping track of the software publisher's software releases for the purpose of configuration control; and

(c) **No Software Development**: The Contractor is not required to develop, program or provide additional software code related to the Pre-Existing Software as part of the Work performed under the Contract.

(d) **Title**: Except as otherwise specifically provided in these Articles of Agreement, title to the Pre-Existing Software will be unaffected by the performance of the Services for Pre-Existing Software and, to the extent that the Pre-Existing Software is subject to a license for use from a third party, its use will remain subject to the conditions of Canada's license.

(e) **Access**: Canada will provide to the Contractor any information regarding any passwords, authorization codes or similar information that might be necessary to perform the Software Services, provided that in doing so Canada is not in default of any obligations regarding the use of the Pre-Existing Software. The Contractor agrees that it is a term of the Contract that it will not

disclose or distribute any part of the Pre-Existing Software to any other person or entity or otherwise violate the proprietary rights of the owner of the Pre-Existing Software.

7.23 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.

7.24 Reporting Requirements

The Contractor must provide the following reports to the Contracting Authority at the following times:

- Quarterly Task Authorization Usage Report

In addition, the Contractor must provide the following reports to the Technical Authority:

- Defects, change requests and outstanding items tracking status reports;
- Monthly project progress reports;
- Guides, manuals, reports to be disseminated to various stakeholders as required;
- Synthesis report of facilitated meetings;
- Activity reports; and
- Conversation notes, design documentation, change management documentation, site inspection reports and other reports requested under the Task Authorization.

7.25 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.

7.26 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.

7.27 Government Property

Canada agrees to supply the Contractor with the items listed below (the "**Government Property**").The section of the General Conditions entitled "Government Property" also applies to the use of the Government Property by the Contractor.

(a) Refer to Annex A.

7.28 Dispute Resolution

(a) The parties agree to maintain open and honest communication about the Work throughout and after the performance of the contract.

(b) The parties agree to consult and co-operate with each other in the furtherance of the contract and promptly notify the other party or parties and attempt to resolve problems or differences that may arise.

(c) If the parties cannot resolve a dispute through consultation and cooperation, the parties agree to consult a neutral third party offering alternative dispute resolution services to attempt to address the dispute.

(d) Options of alternative dispute resolution services can be found on Canada's Buy and Sell website under the heading "Dispute Resolution".

7.29 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. Title

Information Technology (IT) Cyber Security Professional Services

2. Objective

Canada Border Services Agency (CBSA) is seeking the services of an organization to provide professional IM/IT cyber security resources with particular expertise in compliance and security of the public cloud and emerging technologies as described further in this Statement of Work.

The Canadian Center for Cyber Security's IT Security Risk Management: A Lifecycle Approach (ITSG-33)[1] and the Government of Canada (GC) Cloud Security Risk Management Approach and Procedures consist of the following activities:

- Perform security categorization (in terms of confidentiality, integrity, and availability) of each GC service being deployed on a cloud service;
- Select an appropriate set of security controls based on the GC service's security category;
- Select the right cloud deployment model and cloud service model for the GC service;
- Assess the implementation of the security controls in the supporting cloud service;
- Implement the required security controls in the GC service;
- Assess the implementation of the security controls in the GC service;
- Authorize operations of the resulting cloud-based GC service;
- Continuously monitor the security of the cloud-based GC service during the operation phase; and
- Maintain the authorization state of the cloud-based GC service.

The approach and supporting procedures help to ensure that cloud service providers (CSPs) understand the GC's security requirements, and that GC departments and agencies (or GC consumer organizations), and CSPs understand their shared responsibility in implementing the security controls with the appropriate rigor to allow the hosting of GC services and related information in various cloud environments.

This contract will ensure that CBSA's cloud and emerging technology based solutions in use by CBSA are protected from cyber-attacks and data theft and that they are fully in accordance and remain in compliance with the Government of Canada's ITSG-33 Risk Management Approach, GC Cloud Security Guidelines, and the Communications Security Establishment (CSE)'s Canadian Center for Cyber Security Standards, Directives, Advisories and Alerts.

3. Background

Canada Border Services Agency (CBSA) is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods

[1] Created prior to the creation of the Canadian Centre for Cyber Security by one of the entities that became part of the Cyber Centre. This content remains relevant to current discussions about cyber security.

across the Canadian Border. Information technology (IT) is key to meeting the Agency's obligation to administer over 90 Acts, Regulations and International Agreements .

The nature of CBSA's business dictates that we collect and use information about travelers and goods crossing the Canadian border, information that can be sensitive and private. We are entrusted with these details and managing this information requires robust privacy and security controls, and processes.

The CBSA has made commitments to modernization and renewal both internally (through its CBSA Renewal Agenda[2]) and in agreements with partners including the "Border Five", an international forum on customs and border management policy issues with participation from Australia, Canada, New Zealand, the United Kingdom and the United States.

Prior to the World Health Organization's declaration of COVID-19 as a pandemic in March 2020, in alignment with its Renewal Agenda, CBSA was embarking on leveraging innovative technologies using a phased approach to initiate the migration of many of its over 180 legacy Shared Services Canada (SSC)-managed applications to a modern hosting environment based in the cloud. A target of twenty-five percent of CBSA's existing national applications are to be migrated to the cloud by the end of March 2022. Modernizing CBSA applications and moving them to the cloud will deliver numerous benefits to the Agency and for the security of the country.

However, the pandemic required the CBSA to make a number of significant changes to its plans escalating its Cloud presence and leveraging other emerging technologies to urgently respond and meet new and immediate requirements the situation brought forward, such as tracking information on travelers required to self-isolate according to Canada's Emergency Order under the *Quarantine Act*, and to cope with significantly increased volumes of importation of commercial low-value goods.

The work done under the Renewal Agenda by CBSA to ramp up on the new technologies and cloud environments was essential in facilitating the rapid response the Agency has been able to make so far but these new tools and ways of doing business bring about new complex and unfamiliar areas of risk that are stretching the available capacity and expertise of the Agency's IT Security resources, including a gap of familiarity and skills with newer technologies.

This gap could be raising the Agency's technology risk exposure. The risks include but are not limited to: Compliance violations (i.e. not meeting regulated or policy requirements); Identity theft; Malware infections and data breaches; Diminished public trust and potential monetary loss. Each technology involves its own unique and complex risks and vulnerabilities. With so many potential threats entering the digital hemisphere, cyber risk management must be dynamic to respond to the ever-evolving threat landscape

In order to continue with the new pace and be able to safely but rapidly respond to new situations, new volumes and other new unknowns, CBSA requires IT Cyber security Professional Services to address cyber security vulnerabilities in order to protect and safeguard private and confidential data on Canadian citizens, Canadian businesses, other international citizens and businesses

[2] See "*Executive Vice-President's Transition Binder 2019: Strategic Policy Branch (SPB) International Strategic Framework for Fiscal Years 2019 to 2022*".

4. Reference Documents

Government of Canada IT Security Risk Management: A Lifecycle Approach (ITSG-33)
https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33

Government of Canada Cloud Security Risk Management Approach and Procedures
https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-security-risk-management-approach-procedures.html

Canadian Center for Cyber Security Directives
https://cyber.gc.ca/en/directives

Government of Canada Direction for Electronic Data Residency (ITPIN 2017-02, archived)
https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-electronic-data-residency.html#:~:text=Direction%20for%20Electronic%20Data%20Residency%20-%20Canada.ca.%20The,ownership%20of%20Government%20of%20Canada%20%28GC%29%20electronic%20data.

Executive Vice-President's Transition Binder 2019: Strategic Policy Branch (SPB)
International Strategic Framework for Fiscal Years 2019 to 2022
https://www.cbsa-asfc.gc.ca/pd-dp/tb-ct/evp-pvp/spb-dgps-isf-csi-eng.html#04-1

National Cyber Security Strategy
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Accessibility for Ontarians with Disabilities Act (AODA) - Accessible Customer Service Standard
https://www.ontario.ca/page/accessibility-ontario-what-you-need-to-know

Town of East Gwillimbury - Accessibility Standards for Customer Service
http://www.eastgwillimbury.ca/About_Us/About_the_Town/Accessibility_Standards_for_Customer_Service.htm

In addition to these reference documents, the Contractor must also refer to Annex A1: Glossary

5. Scope of Work

The Contractor must assist and support CBSA in the following 4 work areas:

a) Cloud Security Assessment Services
   i. Review CBSA and its Cloud Service Providers' implementation and operation of policies, standards, procedures, guidelines, processes, mechanisms and controls against all applicable Government of Canada security policies, directives and guidelines to assure the integrity, confidentiality and availability of information, applications and workloads throughout their lifecycle.
   ii. Review and advise on Cloud Security Scope, Shared Responsibilities & Models, including Cloud service provider contract documentation, reviewing architecture and design documentation and preparing or reviewing a cloud security responsibility matrix, cloud controls matrix, etc.
   iii. Assess the Security Operations Team(s), advise on the readiness of responsible areas to

manage and fulfill their responsibilities; elaborate and develop specific management actions with respect to tools, training, personnel, collaboration and communication required.

iv. Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings

v. Conduct Certification & Accreditation activities

vi. Conduct technical security assessments against CBSA assets including:
- Protected B/Medium Integrity/Medium Availability (PBMM) level and unclassified workloads
- Dev/Test environments and data (data masking, obfuscation or encryption)
- Solutions deployed as IaaS, PaaS and SaaS – inside and outside of Canada
- Tailoring security control profiles
- Reviewing and incorporating third party assessment evidence (CCCS, SOC, FedRAMP, ISO, etc..)

b) Vulnerability Assessments

i. Performed as part of security testing of a solution during development to validate the effectiveness of the security design and identify gaps in the configuration or inclusion of controls, including:
- Static code analysis
- Static and Dynamic testing
- Network Penetration testing
- Application & product security testing
- Tests all architectural stacks: network, application, database, infrastructure

ii. Performed periodically against deployed solutions to ensure continued compliance and adequacy of controls in light of new threats

c) Cloud Security Operations

i. Assist CBSA in the selection, deployment, integration, configuration and maintenance of best-in-class monitoring and other cyber security tools; Develop and integrate security processes into cloud service management; Establish strategic and operational security metrics;

ii. Perform security systems monitoring and incident response; conduct incident investigations; prepare security briefings, reports and action plans.

iii. Compliance monitoring to ensure continued adherence and vigilance.

iv. Transition and knowledge transfer of security operations to CBSA

d) Provide technical guidance, support, engineering and research in the design, development and securing of solutions based on emerging or evolving technologies (such as public-cloud networks, mobile applications, biometrics, robotic process automation, APIs, artificial intelligence/machine learning, and RFID):

i. Research and identify specific threats involved in deploying Government of Canada IT solutions based on or incorporating emerging technologies

ii. Provide technical expertise to influence, guide and assist solution design and development using these technologies;

iii. Review and advise on solution designs, development (including code review), configuration and operations;

iv. Provide instructive analysis, advice, engineering and design support to CBSA on feasible methods to enable and facilitate the adoption and use of innovative technologies while strengthening their security posture and/or aiding to mitigate the threat exposure(s) such technologies present
v. Provide updates as the technology security risks evolve
vi. Provide advice on how CBSA can assess and implement measures to constantly adjust to new technologies and development in the cyber security domain.

6. Resource Tasks and Deliverables

To address the work areas from Section 5, the Contractor must provide CBSA with IT Cyber security Professional Resources in the following, but not limited to, TBIPS categories on an 'as and when' requested basis as initiated through Task Authorizations (TAs).

Resource Categories	Levels
C.1 Strategic IT Security Planning & Protection Consultant	2, 3
C.3 Information Technology Security TRA and C&A Analyst	2, 3
C.7 Information Technology Security Design Specialist	2, 3
C.8 Network Security Analyst	2, 3
C.9 Information Technology Security Systems Operator	2, 3
C.11 Information Technology Security Vulnerability Analysis Specialist	2, 3
C.14 Information Technology Security Research and Development Specialist	2, 3
C.16 Privacy Impact Assessment Specialist	2, 3

The following are the tasks and deliverables associated with resource-specific requirements. Each Task Authorization will identify the tasks and the deliverables.

6.1 C.1 Strategic Information Technology Security Planning and Protection Consultant, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. Review, analyze, and/or apply the Information Technology (IT) Security Policies, Procedures and Guidelines of International government, Federal, Provincial or Territorial government.
b. Review, analyze, and apply the best practices, national or international computer law and ethics, IT Security architecture, and IT Security Risk Management Methodology
c. Develop vision papers delineating the way ahead to ensure that IT Security and cyber protection are business enablers
d. Provide IT Security strategic planning and advice.
e. Conduct feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security
f. Develop advanced R&D policy/strategy
g. Collect, collate and prioritize client IT Security and Information Infrastructure Protection requirements
h. Review and prioritize IT Security and Information Infrastructure Protection programs

i. Develop strategic IT Security architecture vision, strategies and designs using the Business Transformation Enablement Program (BTEP) methodology and the Government Strategic Reference Model (GSRM)
j. Develop IT Security programs and service designs using the following GSRM models: Program Logic Model, Program and Service Alignment Model, Service Integration and Accountability Model, State Transition Model, Information Model and Performance Model

6.2 C.3 Information Technology Security TRA and C&A Analyst, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. Review, analyze, and/or apply Federal IT Security policies, System IT Security Certification & Accreditation processes, IT Security products, safeguards and best practices, and the IT Security risk mitigation strategies
b. Identify threats to, and vulnerabilities of operating systems and wireless architectures
c. Identify personnel, technical, physical, and procedural threats to and vulnerabilities of Federal IT systems
d. Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings
e. Conduct Certification activities such as: Develop Security Certification 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
f. Conduct Accreditation activities such as: Review of the certification results in the design review documentation by the Accreditation 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 Accreditation 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

6.3 C.7 Information Technology Security Design Specialist, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. Review, analyze, and/or apply: Architectural methods, frameworks, and models such as TOGAF, US Government Federal Enterprise Architecture Profile (FEAP), the Government of Canada Enterprise Security Architecture Program, Zachman Framework, Universal Modeling Methodology (UMM).
b. 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)
c. Review, analyze, and/or apply Secure IT architectures, standards, communications, and security protocols such as IPSec, TLS, SSH, S-MIME, HTTPS.
d. 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.
e. 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, API security, incident management, identity management).
f. Review, analyze, and/or apply best practices and standards related to the concept of network zoning and defence in-depth principles.
g. Analyze IT Security statistics, tools and techniques.
h. Analyze security data and provide advisories and reports.
i. Provide security architecture design and engineering support.
j. Conduct data security designation/classification studies.
k. Prepare tailored IT Security alerts and advisories from open and closed sources.

and

l. Review, analyze, and/or apply Identity, Credential, and Access Management practices, technologies and architectures.
m. Develop and deliver presentation materials to support engagement with IT security practitioners, senior level executives, etc.
n. Research and identify specific threats involved in deploying Government of Canada IT solutions based on or incorporating emerging technologies (including Cloud, Mobile, RFID, Artificial intelligence, robotic process automation, biometrics, APIs, etc.)
o. Provide instructive advice, engineering and design support to CBSA on feasible methods to enable and facilitate the adoption and use of emerging technologies while strengthening their security posture and/or aiding to mitigate the threat exposure(s) such technologies present
p. Review, analyze and identify the technical threats to and vulnerabilities of cloud infrastructure, databases and emerging technologies
q. Provide updates as the technology security risks evolve

6.4 C.8 Network Security Analyst, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. Review, analyze, and/or apply:
    - Internet security protocols such as TLS, HTTPS, S-MIME, IPSec, SSH
    - TCP/IP, UDP, DNS, SMTP, SNMP
    - Approved GC Cryptographic Algorithms
    - Directory Standards such as X.400, X.500, and SMTP
    - Networking Protocols (for example, HTTP, FTP, Telnet)
    - Network hardening (for example: shell scripting, service identification)
    - Technical IT Security safeguards
    - IT Security tools and techniques
    - Operating Systems such as MS, Unix, Linux, and Novell
    - Intrusion detection systems and firewalls
    - Network routers, multiplexers and switches
    - Wireless technology
b. Analyze security data and provide advisories and reports
c. Conduct impact analysis for new software implementations, major configuration changes and patch management
d. Develop proof-of-concept models and trials for IT Security involving emerging technologies
e. Design/develop IT Security protocols
f. Identify and analyze technical threats to, and vulnerabilities of, networks
g. Analyze IT Security tools and techniques
h. Complete tasks related to authorization and authentication in physical and logical environments
i. Prepare tailored IT Security alerts and advisories from open and closed sources
j. Complete tasks directly supporting the departmental IT Security and Cyber Protection Program

and

k. Review, analyze and identify the technical threats to and vulnerabilities of cloud infrastructure, databases and emerging technologies

6.5 C.9 Information Technology Security Systems Operator, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. Review, analyze and/or apply:
    - Networking Protocols (HTTP, FTP, Telnet)
    - Internet security protocols (for example: TLS, HTTPS, S-MIME, IPSec, SSH)
    - TCP/IP, UDP, DNS, SMTP
    - Directory Standards such as X.400, X.500, and SMTP
    - Network routers, multiplexers and switches
    - Network hardening (for example: shell scripting, service identification)
    - Wireless technology
    - Technical threats to, and vulnerabilities of, networks
    - Technical IT Security safeguards

- IT software and hardware security products

b. Configure operating systems such as MS, Unix, Linux and Novell
c. Configure IT Security management
d. Configure intrusion detection systems, firewalls and content checkers, extracting and analyzing reports and logs, and responding to security incidents
e. Configure/update virus scanners
f. Complete tasks directly supporting the departmental IT Security and Cyber Protection Program

and

g. Use Security Information and Event Management (SIEM) tools and Cloud security monitoring tools such as AWS Security Hub or Azure Sentinel

6.6 C.11 Information Technology Security Vulnerability Analysis Specialist, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. 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 TLS, HTTPS, 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
b. Identify threats to, and technical vulnerabilities of, networks
c. Conduct on-site reviews and analysis of system security logs
d. Collect, collate, analyze and disseminate public domain information related to networked computer threats and vulnerabilities, security incidents and incident responses
e. Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings
f. Completed tasks directly supporting the departmental IT Security and Cyber Protection Program

and

g. Review, analyze and identify the technical threats to and vulnerabilities of cloud infrastructure, databases and emerging technologies

6.7 C.14 Information Technology Security Research and Development Specialist, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. Review, analyze, and/or apply:
   - Canadian universities and industrial IT Security R and D capabilities

- Directory Standards such as X.400, X.500, and SMTP
- Networking Protocols such as HTTP, FTP, Telnet
- Internet security protocols such as TLS, HTTPS, S-MIME, IPSec, SSH
- Wireless Security, Bluetooth standards
- TCP/IP, UDP, DNS, SMTP, SNMP standards and protocols
- Intrusion detection systems, firewalls and content checkers;
- Cryptographic Algorithms
- Security best practices

b. Develop and implement Security Programs such as: biometrics, digital rights management, RFID, access control, removable media management, etc
c. Design and develop prototypes, proof-of-concept models and trials including security functionality and emerging technologies
d. Analyze Research & Development reports from an IT Security perspective
e. Participate in national/international Research & Development forums
f. Complete tasks directly supporting the departmental IT Security and Cyber Protection Program

and

g. Review, analyze and research the technical threats to and vulnerabilities of cloud infrastructure, databases and emerging technologies
h. Conduct requirements analysis from an IT Security perspective of user requirements, system requirements, and capability requirements involving emerging technologies;
i. Provide subject matter expertise on security of emerging technologies such as: biometrics, artificial intelligence, RFID, mobile, wireless, access control, sensor technologies, robotic process automation, APIs etc.
j. Provide advice, engineering, design and development support to CBSA on feasible methods to enable and facilitate the adoption and use of emerging technologies while strengthening their security posture and/or aiding to mitigate the threat exposure(s) such technologies present
k. Provide updates as the technology security risks evolve

6.8 C.16 Privacy Impact Assessment Specialist, Levels 2 & 3

This resource category will be responsible for, but not limited to, doing the following:

a. 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
b. 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

c. Analyze the flow of information using the PIA model provided by the client
d. Conduct privacy analysis to provide evidence of compliance with privacy principles and to identify privacy risks
e. Develop Privacy Risk Management Plans
f. Develop recommendations as to possible privacy risk mitigation strategies
g. Complete tasks directly supporting the departmental IT Security and Cyber Protection Program

and

h. Conduct privacy analysis to identify privacy risks and provide evidence of compliance with the data privacy requirements of Canada's international partners, where applicable.

6.9 Common

- Perform technical analysis and technical impact assessments
- Provide strategic assessments on technology trends and emerging technologies
- Evaluate and assist in the selection of enterprise-wide technology tools
- Prepare technical documents such as requirement analysis, options analysis, technical architecture documents, mathematical risk modeling.
- Research of open source material with a view to analyzing trends and emerging technologies
- Project oversight
- Prepare briefings for senior managers
- Develop and deliver training knowledge transfer documentation relevant to the resource category

7. Deliverables

The Contractor must provide and submit deliverables to the Technical Authority and/or as identified/required in the TA. The individual Task Authorization (TA) will define the documents and deliverables required for the specific project/requirement.

Deliverables can include but are not limited to the following:

a. A work plan for the work to be undertaken;
b. Progress report on a bi-weekly or monthly basis on activities undertaken which includes the following:
    1. Activities completed within the reporting period;
    2. Planned activities for the next reporting period;
    3. Risks/issues that will require the attention of the Technical Authority; and
    4. Corrective actions required.
c. Documents, presentations and other materials, as requested by the Technical Authority;
d. Quarterly Task Authorization Usage Report

Documents can include, but are not limited to:

1. Cloud Risk Management Review
2. Cloud Security Assessment
3. Cloud Security Responsibilities Matrix

4. Cloud Security Design
5. Cloud Controls Matrix
6. Data security analysis;
7. Concepts of operation;
8. Statements of Sensitivity (SoSs);
9. Threat assessments;
10. Preliminary Privacy Impact Assessments (PPIAs);
11. Privacy Impact Assessments (PIAs);
12. Privacy Risk Management Plans;
13. Non-technical Vulnerability Assessments;
14. Threat & Risk assessments;
15. IT Security threat, vulnerability and/or risk briefings and reports;
16. IT Security Solutions option analysis and implementation plans;
17. Surveys, Requirements studies;
18. Research, Options analysis;
19. Conceptual and logical architecture designs;
20. Technical Security design documentation;
21. Change Management documentation;
22. Configuration Management documentation;
23. IT Security requirements;
24. Algorithms, mathematical risk modeling;
25. System controls;
26. Proof of concept models
27. IT Security Test strategies;
28. IT Security Test plans, scripts and reports;
29. Defects, change requests and outstanding items tracking status reports;
30. Implementation plans and guides;
31. Standard operating procedures guides;
32. Impact analysis and strategies;
33. Project plans;
34. Analysis documents;
35. Conceptual and logical system security designs;
36. Written and verbal advice;
37. Knowledge transfer and training material;
38. Issues papers/Briefing Notes;
39. IT Security Alerts & Advisories
40. Process maps, decision and data flows
41. Presentation decks and materials;
42. Meeting facilitation and reports (e.g. monthly progress reports);
43. Metrics;
44. Security Incident Reports;
45. Operational Reports
46. Conversation notes

Deliverables must be submitted in electronic copies in the appropriate formats (e.g. MS Project or MS Office Suite applications as identified in the TA. All electronic deliverables must comply with departmental software standards, currently MS Office Suite latest version. Where required, CBSA will provide the Contractor with the required forms and templates to meet these standards.

There may be a requirement for the Contractor's resources to access information available exclusively at Canada's facilities in the NCR. All documents developed and/or updated by each of the Contractor's resources must be provided to the Project Authority for review, approval and signature (as required). All Work under this Contract must be accessible to the Project Authority at all times.

Each TA will identify the format and language in which the deliverables are required to be submitted.

8. Technical Environment

The technical environment at CBSA is comprised of several technologies including but not limited to:

Extensible Markup Language (XML)

- XAML
- XML Schema Definition (XSD)
- Document Type Definition (DTD)
- XPATH
- XSLT
- Xquery, JQuery
- JavaScript Object Notation (JSON)
- JavaScript Frameworks – REACT, Node.js,
- HTML, HTML5
- Java
- Python
- VB.Net
- TypeScript (Angular)
- Hibernate

Mobile Specific Development Languages

- Swift, Swift UI
- Kotlin
- Coca and Coca Touch
- Ionic
- React Native
- JQuery Mobile
- Objective-C
- Java
- Xamarin

Cloud Specific Development Languages

- Ancible Scripting
- AWS CloudFormation Scripting
- Azure Resource Manager (ARM) Scripting
- Terraform Scripting
- Development tools and Frameworks
- Eclipse IDE, Visual Studio Code, Visual Studio Enterprise IDEs
- AWS Cloud 9 IDE

- GitHub Desktop
- Microsoft Teams
- Swagger / Open API editor
- Xcode
- JEE (WebSphere)
- JMS (WebsphereMQ)
- WebSphere Application Server (WAS), Tomcat Application Server, JBoss Application
- Spring and Spring Integration Framework, Spring Boot Framework
- Jersey REST, Apache REST
- ANT, Apache Maven, SVN, git
- Azure DevOps
- AWS DevOps – CodeCommit, CodePipeline, etc.
- AWS Command Line Interface
- Windows PowerShell
- AWS Cloud Development Kit (CDK)
- UIPath Orchestrator

Communication Protocols

- TCP/IP
- File Transfer Protocol (FTP)
- Secure File Transfer Protocol (SFTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Managed File Transfer including PWGSC's MSFT solution
- Secure Socket Layer (SSL) / Transport Layer Security (TSL)

Electronic Data Interchange (EDI)

- ANSI X.12
- EDIFACT
- IATA Standards
- World Customs Organization (WCO) Data Model
- Financial, Transportation data models

Interoperability & Integration

- Web Services standards – SOAP and REST
- Web Services Definition Language (WSDL)
- JavaScript Object Notation (JSON)
- Business Rules Management Solution
- Enterprise Service Bus
- PKI Encryption/Decryption
- CA-Idm/SM
- IBM DataPower
- GatewayScript
- IBM Sterling Transformation
- IBM Transformation Extender Maps

Data & Analytics

- IBM DB2 on UNIX, z/OS
- Sybase, Oracle Database
- SAP HANA
- SAP Business Suite
- IBM PureData
- IBM DataStage
- IBM Infosphere Suite
- IBM SPSS
- IBM Cognos Suite
- Erwin Data Modeler
- Cloud Databases – AWS DynamoDB, AWS RDS Postgress SQL, AWS RDS MySQL
- AWS RedShift, AWS DataLake, AWS Glue (ETL tool), AWS Athena
- Azure Analytics

Operating Systems and other Platforms

- Android
- iOS
- Unix Solaris
- Linux Red Hat
- Amazon Linux
- Windows Server 2016, Server 2019
- VMWare
- Z-OS
- Microsoft Windows 10 (Desktop)
- AWS Public Cloud
- Azure Public Cloud

AWS

- AWS Security Hub
- AWS Guard Duty
- AWS CloudTrail
- AWS Web Application Firewall
- AWS Identity and Access Management
- Amazon Detective
- Amazon Macie
- AWS Systems Manager Ops Center

Azure

- Azure Sentinel
- Azure Monitor
- Azure Network Monitor
- Azure Security Center
- Azure Log Analytics Workspace

Other

- UIPath, UiPath Studio, UIPath Robot/Assistant
- IBM Data Studio
- Spring Tool Suite
- Netezza
- SSAName3
- COBOL
- OS/360
- OCR
- SQL
- R
- Python
- Scala
- ArcGIS
- MS Dynamics
- OpenText GCDocs
- SAP SuccessFactors
- Citrix
- IBM Rational Software Architect
- Archimate, Qualiware
- Adobe
- MS Office / Office 365
- Microsoft Active Directory
- CA APM Introscope
- Vue.js
- Apache Jmeter
- SmartBear SoapUI

Other new and emerging technologies and software
Any other IM/IT software application, language or database utilized within CBSA

9. Location of Work

The Contractor personnel may be requested to work both onsite at CBSA premises in the NCR and/or remotely offsite at the Contractor's site. The location where services will be conducted, will be identified in each Task Authorization (TA).

Certain services, (5) b) in particular, may partially be executed outside of the CBSA environments using the Supplier's equipment and/or CBSA equipment, however at no time is protected data to be stored externally to CBSA infrastructure. The remaining services and work will be conducted and integrated within CBSA environments using CBSA equipment.

10. Language Requirements

While proposed resources must be fluent in English, there may be a requirement for specific resources to be fluent in both official languages, which will be specified in the TA.

11. Operational Working Hours

Operational working hours will be from 07:00 to 18:00 Monday through Friday where the Contractor's resources will be expected to work 7.5 hours each day between those hours or as otherwise indicated in the Task Authorization. The Contractor's resources must be available to work outside normal operational hours during the duration of the Contract. The Contractor may need to provide the resources on evenings, weekends and/or holidays. Any time worked over the number of billable hours/days in a month must be pre-approved by the Technical Authority.

12. Meetings

Unless otherwise indicated in this Statement of Work or in a Task Authorization issued by the Project Authority or otherwise agreed to by the Project Authority, meetings will be convened in the National Capital Region between Canada and the Contractor at a time mutually agreed-upon by both parties. Canada will determine the location of the meetings. Meetings will be chaired by Canada. Canada will provide the facilities, materiel and services reasonably required to facilitate the meetings.

The Contractor must ensure that personnel responsible for work under discussion, or a suitable representative authorized to conduct the work under the Contract, attend the meetings. In order to reduce travel and work flow interruptions, Canada and the Contractor, by mutual agreement, can convene video or telephone conferences in lieu of face-to-face meetings.

13. Travel Requirements

There are no travel requirements.

14. Constraints, Standards and Specifications

The Contractor must work within constraints imposed by the department, such as government policies and mandatory procedures, current and proposed related activities, security, sensitivity to other interest, protection of the environment, conservation of resources and other relevant restrictions and work space as required.

Specific Government of Canada and CBSA internal security policies, directives, standards, and guidelines applicable to this requirement include but are not limited to the following (refer to section 4, Reference documents):

I. Government of Canada IT Security Risk Management: A Lifecycle Approach (ITSG-33)
II. Government of Canada Cloud Security Risk Management Approach and Procedures
III. Canadian Center for Cyber Security Directives
IV. Government of Canada Direction for Electronic Data Residency (ITPIN 2017-02, archived)

All work must be conducted within Canada and all CBSA technology and information is to remain resident within Canada

The Government of Canada strives to ensure that the goods and services it procures are inclusive by design and accessible by default, in accordance with the Accessible Canada Act, its associated regulations and standards, and Treasury Board Contracting Policy. The following accessibility standards are applicable to this requirement:

I. Accessibility for Ontarians with Disabilities Act (AODA) - Accessible Customer Service Standard
II. Town of East Gwillimbury - Accessibility Standards for Customer Service

15. Government Furbished Equipment and Information

CBSA will provide subject to pre-defined security requirements, and only to the specified Contractor personnel, access to identified databases or applications resident on CBSA computers or networks for the sole purpose of executing the tasks associated with this contract. The nature and characteristic of such access will be at the sole discretion of the Technical Authority.

CBSA will also provide the Contractor personnel with the following:

- Relevant internal documentation;
- Office space and building pass (if required and will be identified in each Task Authorization); and
- Computer equipment such as a laptop, etc. (if required and will identified in each Task Authorization).

ANNEX A1 : GLOSSARY

Term	Context
Artificial Intelligence (AI)	**Artificial intelligence** addresses the use of computers to mimic the cognitive functions of humans, thus the way the systems can respond and behave in certain circumstances. When machines carry out tasks based on algorithms in an "intelligent" manner, that is AI. The goal is to simulate natural intelligence to solve complex problems and is used primarily in decision making. AI's main aim is to increase the chances of success and not necessarily accuracy. Sources: DataScienceCentral.com, Hackernoon.com
Border Five Countries	**Border Five** is an informal forum on customs and border management policy issues with participation from Australia, Canada, New Zealand, the United Kingdom and the United States. Source: Wikipedia
Business-critical	A **business-critical** application is an application that is critical or important to keep the organization running. In other words it is a vital application to a business line, which if interrupted could result in serious financial, legal loss; customer dissatisfaction; loss in productivity. Business Critical Applications can range from small tools to specialized tools to major LoB (Line of Business) systems. These applications can be either running on the client's system or servers or can include off the shelf products or even can be a third party system or an application or it can be any internally developed system.
Canadian academic credentials assessment	A **Canadian academic credentials assessment** is a statement of the general comparability of international educational credentials to a completed Canadian educational credential. The Canadian Information Centre for International Credentials (CICIC) assists persons who wish to obtain an assessment of their educational, professional, and occupational credentials by referring them to the appropriate organizations.
Cloud-Computing	**Cloud computing** is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Term	Context
Configuration[1]	**Configuration** is the arrangement, relationships and customizations of hardware and/or software components that make up a computer system to enable the system to perform its intended use based on given requirements.
Configuration[2] / Configuring[2]	**Configuration/configuring** is the activity of arranging and/or customizing the hardware and/or software components that make up a computer system to enable the system to perform its intended use based on given requirements.
Cyber Security / Cybersecurity	**Cyber security** refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber Security may also be referred to as Information Technology Security. Source: DigitalGuardian.com
Emerging Technology	For the purpose of this procurement, **emerging technologies** are Information Technology characterized by radical novelty (in the ***public sector organizations*** context), relatively fast growth, coherence, prominent impact, and uncertainty and ambiguity. They include: ***Artificial Intelligence (AI)***, Augmented Intelligence, ***Machine Learning (ML)***, Deep Learning (DL), Neural Networks (NN), Robotic Process Automation (RPA), Biometrics, Big Data/Predictive Analytics, Radio Frequency Identification (RFID), Natural language computing, Mobile applications, Voice recognition, Chatbots. For the purpose of this procurement, they exclude any form of cloud computing without the above-mentioned technologies.
Enterprise Solution	**Enterprise solutions** are designed to integrate multiple facets of a company's business through the interchange of information from various business process areas and related databases. These solutions enable companies to retrieve and disseminate mission-critical data throughout the organization, providing managers with real-time operating information.
IT Enterprise Security Risk Assessment	**IT enterprise security risk assessments** are performed to allow organizations to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker's perspective. This process is required to obtain organizational management's commitment to allocate resources and implement the appropriate security solutions. A comprehensive enterprise security risk assessment also helps determine the value of the various types of data generated and stored

Term	Context
	across the organization. Without valuing the various types of data in the organization, it is nearly impossible to prioritize and allocate technology resources where they are needed the most. To accurately assess risk, management must identify the data that are most valuable to the organization, the storage mechanisms of said data and their associated vulnerabilities. Source: ISACA
Machine Learning (ML)	**Machine learning** is a subset of AI and focuses on the ability of machines to receive a set of data and learn for themselves, changing algorithms as they learn more about the information they are processing. Using an algorithm to predict an outcome of an event is not machine learning. Using the outcome of the prediction to improve future predictions is. The goal is to learn from data for a certain task to maximize the performance of the machine on the task. ML's main aim focuses on accuracy rather than success. Sources: DataScienceCentral.com, Hackernoon.com
Next-Generation Firewall NextGen Firewall	**Next-generation firewalls** are a class of firewall that are implemented in either software or hardware and are capable of detecting and blocking complicated attacks by enforcing security measures at the protocol, port and application level. The difference between a standard firewall and next-generation firewalls is that the latter performs a more in-depth inspection and in smarter ways. Next-generation firewalls also provide additional features like active directory integration support, SSH and SSL inspection, and malware filtering based on reputation. Source: Techopedia
OWASP Top 10	The **OWASP Top 10** is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. Source: OWASP
Penetration Testing	Penetration testing is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (vulnerabilities), including the potential for unauthorized parties to gain access to the

Term	Context
	system's features and data, as well as strengths, enabling a full risk assessment to be completed. …The National Cyber Security Center describes penetration testing as the following: "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might." Source: Wikipedia
Protected Data	For the purpose of this procurement, **Protected Data** is application data which has been assessed as sensitive and requiring security features meeting any of the following control profiles: i. Protected B Medium Integrity Medium Availability (PBMM) or SECRET Medium Integrity Medium Availability ii. FEDRAMP Moderate or High iii. NIST SP 800-53 Moderate or High
Public Cloud	**Public Cloud** refers to a style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies—i.e., public cloud computing uses cloud computing technologies to support customers that are external to the provider's organization. Using public cloud services generates the types of economies of scale and sharing of resources that can reduce costs and increase choices of technologies. From a government organization's perspective, using public cloud services implies that any organization (in any industry sector and jurisdiction) can use the same services (e.g., infrastructure, platform or software), without guarantees about where data would be located and stored Source: Gartner For the purpose of this procurement, Public Cloud includes services and virtual infrastructure provided by a Cloud Service Provider (such as AWS, Microsoft Azure, Google Cloud, etc.) accessible over the public internet.
Public Sector Organization	For the purpose of this procurement, a **Public Sector Organization** is defined as: any Federal-level Department, Agency or Crown Corporation; Provincial or State level Government; and Municipal governments (representing Pop. 500,000+).
Secure	For the purpose of this procurement, **Secure** refers to environments and/or infrastructure required to meet any of the following security control profiles: • the Government of Canada Protected B Medium integrity Medium availability (PBMM) Profile or higher

Term	Context
	• the Government of Canada SECRET Medium Integrity Medium Availability (SMM) Profile or higher • FEDRAMP Moderate or High Level • NIST SP 800-53 Moderate or High Level • ISO 27001 and ISO 27017
Security Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Source: NIST Computer Security Resource Center
Security Assessment & Authorization (SA&A) Review	The process by which departments ensure that only authorized software and hardware are implemented in their information technology (IT) environment. Security Assessment is an ongoing process that evaluates security practices and controls to determine if these are implemented correctly, operating as intended, and achieving the desired outcome. Security Authorization involves obtaining and maintaining a security risk management decision which explicitly accepts the related residual risk, based on the results of a security assessment. This authorization is referred to as “the Authority to Operate” (ATO). The procedure is further described by the ITSG-33 Source: Shared Services Canada, Audit of Security Assessment and Authorization
Security Audit	A **Security Audit** is an in-depth examination of an organization’s IT/Cyber Security program to provide assurance that internal controls within the organization’s responsibility are in place to prevent or adequately mitigate the risks of cyber attacks by: • assessing the extent of compliance with policies, standards, procedures, and processes for documenting, communicating, and addressing security incidents; and • assessing the monitoring and reporting mechanisms in place for key activities of cyber security.
Security Operations Center (SOC)	A **Security Operations Center** (SOC) includes an information security team responsible and infrastructure, tools and processes required for monitoring and analyzing an organization’s security posture on an ongoing basis. The SOC team’s goal is to detect, analyze, and respond

Term	Context
	to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery. Typical SOC infrastructure includes firewalls, IPS/IDS (Intrusion Prevention Systems/Intrusion Detection Systems), breach detection solutions, probes, and a security information and event management (SIEM) system. Technology should be in place to collect data via data flows, telemetry, packet capture, syslog, and other methods so that data activity can be correlated and analyzed by SOC staff. The security operations center also monitors networks and endpoints for vulnerabilities in order to protect sensitive data and comply with industry or government regulations. Source: Digital Guardian
Security Risk Management	**Security risk management** is the practice of prioritizing cyber security defensive measures based on the potential adverse impact of the threats they're designed to address. Establishing a risk management approach to cyber security investment acknowledges that no organization can completely eliminate every system vulnerability or block every cyber-attack. Through cyber security risk management, an organization attends first to the flaws, the threat trends, and the attacks that matter most to their business. Source: https://cybersecurity.att.com
Threat & Risk Assessment	A **Threat & Risk Assessment** is a process of identifying system assets and how these assets can be compromised, assessing the level of risk that threats pose to assets, and recommending security measures to mitigate threats. The term is also used to refer to the output (deliverable) created through this process. Source: https://cyber.gc.ca/en/glossary/TRA
Vulnerability Scan	A **vulnerability scan** is an automated security scan designed to assess computers, networks or applications for known weaknesses. They are utilized in the identification and detection of vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners allow for both authenticated and unauthenticated scans. … The modern vulnerability scanner often

Term	Context
	has the ability to customize vulnerability reports as well as the installed software, open ports, certificates and other host information that can be queried as part of its workflow. • Authenticated scans allow for the scanner to directly access network based assets using remote administrative protocols such as secure shell (SSH) or remote desktop protocol (RDP) and authenticate using provided system credentials. This allows the vulnerability scanner to access low-level data, such as specific services and configuration details of the host operating system. It's then able to provide detailed and accurate information about the operating system and installed software, including configuration issues and missing security patches. • Unauthenticated scans is a method that can result in a high number of false positives and is unable to provide detailed information about the assets operating system and installed software. This method is typically used by threat actors or security analyst trying determine the security posture of externally accessible assets. Source: Wikipedia

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. 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.

APPENDIX B TO ANNEX A

TASK AUTHORIZATION (TA) FORM

Contractor:	Contract No.
Task Authorization No.:	Date:
Financial coding:	Amendment #:

1. STATEMENT OF WORK (WORK ACTIVITIES, CERTIFICATIONS AND DELIVERABLES)

BACKGROUND

TASKS

DELIVERABLES

RESOURCE ESSENTIAL TECHNOLOGY REQUIREMENT(S)

( ) (To be identified in TA)
( ) (To be identified in TA)
( ) (To be identified in TA)
( ) (To be identified in TA)
( ) (To be identified in TA)

Technical Authority:
Email:

The Technical Authority is the TC Representative (or delegated representative) responsible for the management of this TA. Any changes to the TA must be authorized in writing by the Technical Authority and the Contracting Authority when applicable. The Contractor is not to perform work in excess of or outside the scope of this TA based on verbal or written requests or instructions from any government personnel other than the aforementioned officer.

PLEASE SEND INVOICES TO:

The Technical\Authority:
Email:

The Technical Authority (or delegated representative) is responsible for all matters concerning the technical content of the Work under this TA. Any proposed changes to the scope of the Work are to be discussed with the Technical Authority, but any resulting change is only effective and enforceable if a written TA amendment is issued by the Technical Authority or the PWGSC Contracting Authority.

2. PERIOD OF SERVICES:	**FROM (**DATE):	**TO (**DATE):
3. WORK LOCATION:		

4. TRAVEL REQUIREMENTS:				
5. LANGUAGE REQUIREMENTS:				
6. LEVEL OF SECURITY CLEARANCE REQUIRED				
7. COST				
CATEGORY	**NAME OF RESOURCE**	**PER DIEM RATE**	**ESTIMATED # OF DAYS**	**TOTAL COST**
				$
			ESTIMATED COST	**$**
			APPLICABLE TAX	$
			Sub Total	$
			TOTAL TRAVEL & LIVING COST (INCLUDING APPLICABLE TAX)	$
			TOTAL	$

8 SIGNATURES		
Technical Authority:	**Signature:** **On File**	**Date:**
Contracting Authority:	**Signature:**	**Date:**

Check Either Option

___ The Contractor hereby accepts this task authorization

___ The Contractor does not accept this task authorization

Name of Contractor authorized to sign (type or print):	**Title of Contractor authorized to sign (type or print):**	**Date:**
Signature:		

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.

To demonstrate compliance with all criteria, the Contractor must include the following information:

- Project name.
- (*) Client organization
  Client (*) information including organization name, Contact Reference name, title, address, phone number and email address.

  (*) The Contact Reference must be an individual who is or was at the time an employee of the client organization who can provide confirmation of all information;
- Project start /end dates and duration.
- Project description.
- Description of role and tasks performed by the resource.

The following terms are used in the evaluation criteria:

*__demonstrate__: the candidate must clearly demonstrate in the resume how she/he meets the criteria. Stating only that he/she meets it will not be sufficient to meet the criteria.

*__Hands-on experience__: When used within a criteria, this means that the resource personally and independently performed or executed an activity or task. He/she was not contributing to, participating in, leading or overseeing (or other similar-meaning verbs) the task, unless otherwise explicitly stated within the criteria. The resource worked directly performing the activity with the technology “at the keyboard”.

NOTE TO CONTRACTOR: Where indicated by ***bold italics***, those terms are defined within the Glossary.

1.0 MANDATORY RESOURCE ASSESSMENT CRITERIA:

TBIPS Stream 6: Cyber Protection Services

C.1 Strategic Information Technology Security Planning and Protection Consultant, Level 2

Resource Category: C.1 Strategic Information Technology Security Planning and Protection Consultant, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M1.1	The Contractor must demonstrate that the proposed resource has experience in the last five (5) years with one (1) project involving Software Development & Application Security and one of the following areas: • Cloud security • Endpoint Security • Identity & Access Management To qualify, a project must have a minimum duration of four (4) months.	
M1.2	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years' experience in the last ten (10) years in performing all of the following activities: • Providing IT Security strategic planning and advice • Conducting feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security • Supporting the development of strategic IT Security architecture vision, strategies and designs • Supporting the development of IT Security programs and service designs Note: The experience required is a combined total, however a minimum of 1 year must be demonstrated for each activity. To qualify, a project must have a minimum duration of four (4) months.	
M1.3	The Contractor must demonstrate that the proposed resource has experience in the past ten (10) years working with CSEC's Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33) security	

Resource Category: C.1 Strategic Information Technology Security Planning and Protection Consultant, Level 2 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	guidelines to generate project-specific security requirements for two (2) IM/IT projects that involved processing ***Protected data***. To qualify, a project must have a minimum duration of four (4) months.	

C.1 Strategic Information Technology Security Planning and Protection Consultant, Level 3

Resource Category: C.1 Strategic Information Technology Security Planning and Protection Consultant – Level 3 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M2.1	The Contractor must demonstrate that the proposed resource has experience in the last five (5) years with two (2) projects involving Software Development & Application Security and one of the following areas: • Cloud security • Endpoint Security • Identity & Access Management To qualify, a project must have a minimum duration of four (4) months.	
M2.2	The Contractor must demonstrate that the proposed resource has a minimum of seven (7) years' experience in the last ten (10) years in performing all of the following activities: • Providing IT Security strategic planning and advice • Conducting feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security • Developing strategic IT Security architecture vision, strategies and designs • Developing IT Security programs and service designs	

Resource Category: C.1 Strategic Information Technology Security Planning and Protection Consultant – Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	Note: The experience required is a combined total, however a minimum of 1 year must be demonstrated for each activity. To qualify, a project must have a minimum duration of four (4) months.	
M2.3	The Contractor must demonstrate that the proposed resource has experience in the past ten (10) years working with CSEC's Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33) security guidelines to generate project-specific security requirements for three (3) IM/IT projects that involved processing ***Protected data.*** To qualify, a project must have a minimum duration of four (4) months.	

C.3 Information Technology Security TRA and C&A Analyst, Level 2

Resource Category: C.6 IT Security TRA and C&A Specialist, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M3.1	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years' experience in the last ten (10) years, performing IT Risk Management (*) activities involving three of the following areas: • Software Development & Application Security • Cloud security • Endpoint Security • Identity & Access Management • Communications and Network Security (*) See CSEC's Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33)	

Resource Category: C.6 IT Security TRA and C&A Specialist, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	To qualify, a project must have a minimum duration of four (4) months.	
M3.2	The Contractor must demonstrate that the proposed resource has twelve (12) months' experience in completing IT Security Threat and Risk Assessments (TRA) for ***secure*** IT systems using CSEC's Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1) and CSEC's Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33). To qualify, a project must have a minimum duration of four (4) months.	

C.3 Information Technology Security TRA and C&A Analyst, Level 3

Resource Category: Information Technology Security TRA and C&A Analyst, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M4.1	The Contractor must demonstrate that the proposed resource has a minimum of seven (7) years' experience in the last fifteen (15) years, performing IT Risk Management (*) activities involving the following areas: • Software Development & Application Security • Cloud security • Endpoint Security • Identity & Access Management • Communications and Network Security (*) See CSEC's Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33) Note: The experience required is a combined total, however a minimum of 6 months must be demonstrated for each area.. To qualify, a project must have a minimum duration of four (4) months.	

Resource Category: Information Technology Security TRA and C&A Analyst, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M4.2	The Contractor must demonstrate that the proposed resource has three (3) years' experience in completing IT Security Threat and Risk Assessments (TRA) for ***secure*** IT systems using CSEC's Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1) and CSEC's Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33). To qualify, a project must have a minimum duration of four (4) months.	

C.7 Information Technology Security Design Specialist, Level 2

Resource Category: C.7 Information Technology Security Design Specialist, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M5.1	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years' hands-on experience (*) in the last ten (10) years, planning, developing and implementing IT security architectures or IT security designs for complex (**) applications or information systems, involving the following areas: • Software Development & Application Security • Cloud security • Endpoint Security • Identity & Access Management • Communications and Network Security (*)The experience required is a combined total, however a minimum of one (1) year is required with Software Development & Application Security. (**) Complex is defined as a group of interacting, interrelated systems. To qualify, a project must have a minimum duration of four (4) months.	

Resource Category: C.7 Information Technology Security Design Specialist, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M5.2	The Contractor must demonstrate that the proposed resource has hands-on experience in at least two (2) projects, having developed at least three (3) of the following types of system engineering artifacts: • Architecture documents; • System Requirements Specifications; • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans To qualify, a project must have a minimum duration of four (4) months.	

C.7 Information Technology Security Design Specialist, Level 3

Resource Category: C.7 Information Technology Security Design Specialist, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M6.1	The Contractor must demonstrate that the proposed resource has a minimum of seven (7) years' hands-on experience (*) in the last fifteen (15) years, planning, developing and implementing IT security architectures or IT security designs for complex (**) applications or information systems, involving the following areas: • Software Development & Application Security • Cloud security • Endpoint Security • Identity & Access Management • Communications and Network Security (*)The experience required is a combined total, however a minimum of two (2) years is required with Software Development & Application Security.	

Resource Category: C.7 Information Technology Security Design Specialist, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	(**) Complex is defined as a group of interacting, interrelated systems. To qualify, a project must have a minimum duration of four (4) months.	
M6.2	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of hands-on experience in the last six (6) years with the development and delivery of IT security strategies, solutions and proposals to solving IT and security problems affecting multiple stakeholders and security architectures. To qualify, a project must have a minimum duration of four (4) months.	
M6.3	The Contractor must demonstrate that the proposed resource has hands-on experience in at least two (2) projects, having developed at least three (3) of the following types of system engineering artifacts: • Architecture documents; • System Requirements Specifications; • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans To qualify, a project must have a minimum duration of four (4) months.	

C.8 Network Security Analyst, Level 2

Resource Category: C.8 Network Security Analyst, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M7.1	The Contractor must demonstrate that the Proposed Resource has five (5) years hands-on experience performing all of the following activities: • ***Configuring[2]*** and supporting automated IT Security management software; • ***Configuring[2]*** and supporting firewalls, routers and load balancers; • Designing and supporting network failover and recovery using infrastructure-as-code; • ***Configuring[2]*** and supporting Elastic Computing; • ***Configuring[2]*** and supporting Security Groups and Access Control Lists (ACLs) for incoming and outgoing packets; • Designing User Defined Routes (UDRs) to force tunneling; • ***Configuring[2]*** and integrating network infrastructures using a hybrid cloud ***configuration[1]*** Note: Projects do not require all activities however **all** activities must be demonstrated. To qualify, a project must have a minimum duration of four (4) months.	
M7.2	The Contractor must demonstrate that the Proposed Resource has six (6) months hands-on experience in the last five (5) years ***configuring[2]*** and supporting ***secure*** Production ***Cloud-Computing*** environments. To qualify, a project must have a minimum duration of four (4) months.	
M7.3	The Contractor must demonstrate that the Proposed Resource has eighteen (18) months hands-on experience in the last eight (8) years deploying and supporting network security on outsourced ***Public Cloud*** service provider infrastructure. To qualify, a project must have a minimum duration of four (4) months.	

Resource Category: C.8 Network Security Analyst, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M7.4	The Contractor must demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Technology Infrastructure Library (ITIL) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Cloud+ • CompTIA Network+ • CompTIA Security+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher	

C.8 Network Security Analyst, Level 3

Resource Category: C.8 Network Security Analyst, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M8.1	The Contractor must demonstrate that the Proposed Resource has seven (7) years hands-on experience performing all of the following activities : • ***Configuring***[2]and supporting automated IT Security management software; • ***Configuring***[2]and supporting firewalls, routers and load balancers;	

Resource Category: C.8 Network Security Analyst, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Designing and supporting network failover and recovery using infrastructure-as-code; • ***Configuring[2]*** and supporting Elastic Computing; • ***Configuring[2]*** and supporting Security Groups and Access Control Lists (ACLs) for incoming and outgoing packets; • Designing User Defined Routes (UDRs) to force tunneling; • ***Configuring[2]*** and integrating network infrastructures using a hybrid cloud ***configuration[1]*** Note: Projects do not require all activities however **all** activities must be demonstrated. To qualify, a project must have a minimum duration of four (4) months.	
M8.2	The Contractor must demonstrate that the Proposed Resource has eighteen (18) months in the past five (5) years hands-on experience designing or assessing network security architectures or security products for ***secure*** Production ***Cloud-computing*** environments. To qualify, a project must have a minimum duration of four (4) months.	
M8.3	The Contractor must demonstrate that the Proposed Resource has three (3) years experience in the last eight (8) years designing, deploying and supporting network security on outsourced ***public cloud*** service provider infrastructure. To qualify, a project must have a minimum duration of four (4) months.	
M8.4	The Contractor must demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Technology Infrastructure Library (ITIL)	

Resource Category: C.8 Network Security Analyst, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Information Systems Security Architecture Professional (ISSAP) • CompTIA Cloud+ • CompTIA Network+ • CompTIA Security+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher	

C.9 Information Technology Security Systems Operator, Level 2

Resource Category: C.9 Information Technology Security Systems Operator, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M9.1	The Contractor must demonstrate that the Proposed Resource has five (5) years' hands-on experience (*) in the following: • Using Security Incident and Event Management tools • Using Cloud Monitoring tools including AWS Security Hub or Azure Sentinel (*)The experience required is a combined total, however a minimum of eighteen (18) months is required for each. To qualify, a project must have a minimum duration of four (4) months.	
M9.2	The Contractor must demonstrate that the Proposed Resource has six (6) months in the past five (5) years hands-on experience monitoring security for ***secure*** Production ***Cloud-computing*** environments. To qualify, a project must have a minimum duration of four (4) months.	

Resource Category: C.9 Information Technology Security Systems Operator, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M9.3	The Contractor must demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Technology Infrastructure Library (ITIL) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Cloud+ • CompTIA Network+ • CompTIA Security+ • CompTIA Server+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher • Certified Windows Security Administrator • Certified UNIX Security Administrator • Certified Detection Analyst • Certified Incident Handler	

C.9 Information Technology Security Systems Operator, Level 3

Resource Category: C.9 Information Technology Security Systems Operator, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M10.1	The Contractor must demonstrate that the Proposed Resource has ten (10) years' hands-on experience (*) in the following:	

Resource Category: C.9 Information Technology Security Systems Operator, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Using Security Incident and Event Management tools • Using Cloud Monitoring tools including AWS Security Hub or Azure Sentinel (*)The experience required is a combined total, however a minimum of three (3) years is required for each. To qualify, a project must have a minimum duration of four (4) months.	
M10.2	The Contractor must demonstrate that the Proposed Resource has eighteen (18) months' hands-on experience in the past five (5) years monitoring security for ***secure*** Production ***Cloud-computing*** environments. To qualify, a project must have a minimum duration of four (4) months.	
M10.3	The Contractor must demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Technology Infrastructure Library (ITIL) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Cloud+ • CompTIA Network+ • CompTIA Security+ • CompTIA Server+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher • Certified Windows Security Administrator • Certified UNIX Security Administrator • Certified Detection Analyst • Certified Incident Handler	

Resource Category: C.9 Information Technology Security Systems Operator, Level 3 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**

C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M11.1	The Contractor must demonstrate that the Proposed Resource has a minimum of two (2) years' hands-on experience in the last five (5) years conducting IT Security ***vulnerability scans*** and ***penetration testing***.	
M11.2	The Contractor must demonstrate that the proposed resource possesses a current professional certification from any of the following: • AWS Certified Security Specialty • Microsoft Azure Security Technologies • MCSE: Cloud Platforms and Infrastructure • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • System Security Certified Practitioner (SSCP) d'ISC2 • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+ • CompTIA PenTest+ • Certified Wireless Security Professional (CWSP) • GIAC any Cloud Security certification • GIAC any Cyber Defense certification • GIAC any Offensive Operations certification • GIAC Security Expert (GSE) Certification • Certified Windows Security Administrator • Certified UNIX Security Administrator • Certified Vulnerability Assessor (CVA)	

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• EC Council Certified Ethical Hacker	
M11.3	The Contractor must demonstrate that the Proposed Resource has hands-on experience in the past three (3) years performing ***vulnerability scans*** and ***penetration testing*** for a ***secure Public Cloud*** computing environment, service or solution for a ***public sector organization*** including **all** of the following activities: • Conducting an assessment of the assets and data involved; • Conducting thorough vulnerability scans and penetration testing to identify vulnerabilities that may leave the organization or data open to threats or theft; • Using automated vulnerability assessment tools; • Producing an actionable and prioritized list of deficiencies with explanations and technical recommendations. To qualify, a project must contain all activities.	

C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M12.1	The Contractor must demonstrate that the Proposed Resource has a minimum of five (5) years' hands-on experience in the last eight (8) years conducting IT Security ***vulnerability scans*** and ***penetration testing***.	
M12.2	The Contractor must demonstrate that the proposed resource possesses a current professional certification from any of the following: • AWS Certified Security Specialty • Microsoft Azure Security Technologies • MCSE: Cloud Platforms and Infrastructure • Certified Cloud Security Professional (CCSP)	

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Certified Information System Security Professional (CISSP) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • System Security Certified Practitioner (SSCP) d'ISC2 • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+ • CompTIA PenTest+ • Certified Wireless Security Professional (CWSP) • GIAC any Cloud Security certification • GIAC any Cyber Defense certification • GIAC any Offensive Operations certification • GIAC Security Expert (GSE) Certification • Certified Windows Security Administrator • Certified UNIX Security Administrator • Certified Vulnerability Assessor (CVA) • EC Council Certified Ethical Hacker • SANS Mobile Device Security and Ethical Hacking	
M12.3	The Contractor must demonstrate that the Proposed Resource has a minimum of one (1) year hands-on experience in the past three (3) years performing and completing ***Vulnerability scans*** and ***penetration testing*** for ***secure Public Cloud*** computing environments, services or solutions for two (2) or more distinct ***public sector organizations*** including **all** of the following activities: • Conducting an assessment of the assets and data involved; • Conducting thorough ***vulnerability scans*** and ***penetration testing*** to identify vulnerabilities that may leave the organization or data open to threats or theft; • Using automated vulnerability assessment tools; • Producing an actionable and prioritized list of deficiencies with explanations and technical recommendations. To qualify, a project must contain all activities.	

C.14 Information Technology Security R&D Specialist (SME), Level 2

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 2 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M13.1	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years' hands-on experience (*) in the last fifteen (15) years, planning, developing and implementing IT security architectures or IT security designs for complex (**) applications or information systems, involving three of the following areas: • Software Development & Application Security • Cloud infrastructure and/or platforms • Endpoint Security • Identity & Access Management • Communications and Network Security (*)The experience required is a combined total, however a minimum of eighteen (18) months is required with Software Development & Application Security. (**) Complex is defined as a group of interacting, interrelated systems. To qualify, a project must have a minimum duration of four (4) months.	
M13.2	The Contractor must demonstrate that the proposed resource has a minimum of six (6) months' hands-on experience in the last six (6) years in researching, assessing, designing and testing secure integrated solutions (*) involving ***Protected data*** and ***emerging technologies***. (*) Includes functioning prototypes. Solutions must have been developed and deployed to at least a test stage involving production data. To qualify, a project must have a minimum duration of four (4) months.	
M13.3	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience researching, advising and guiding solution architects and developers on integrating and implementing security improvements within solutions. To qualify, a project must have a minimum duration of four (4) months.	

C.14 Information Technology Security R&D Specialist (SME), Level 3

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M14.1	The Contractor must demonstrate that the proposed resource has a minimum of seven (7) years' hands-on experience (*) in the last fifteen (15) years, planning, developing and implementing IT security architectures or IT security designs for complex (**) applications or information systems, involving the following areas: • Software Development & Application Security • Cloud infrastructure and/or platforms • Endpoint Security • Identity & Access Management • Communications and Network Security (*)The experience required is a combined total, however a minimum of three (3) years is required with Software Development & Application Security. (**) Complex is defined as a group of interacting, interrelated systems. To qualify, a project must have a minimum duration of four (4) months.	
M14.2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years' hands-on experience in the last six (6) years in researching, assessing, designing and testing secure integrated solutions (*) involving ***Protected data*** and ***emerging technologies***. (*) Includes functioning prototypes. Solutions must have been developed and deployed to at least a test stage involving production data. To qualify, a project must have a minimum duration of four (4) months.	
M14.3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years' experience researching, advising and guiding solution architects and developers on integrating and implementing security improvements within solutions.	

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 3 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	To qualify, a project must have a minimum duration of four (4) months.	

C.16 Privacy Impact Assessment Specialist, Level 2

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 2 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M15.1	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years' experience in the last ten (10) years performing privacy impact assessments (PIA). To qualify, a project must have a minimum duration of four (4) months.	
M15.2	The Contractor must demonstrate that the proposed resource has a minimum of eighteen (18) months' experience, in the last six (6) years performing all of the following tasks: • Performing privacy impact assessment (PIA) on IT infrastructure and systems for a Canadian Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a large (*) Canadian-based commercial client. • 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. • Application of policies and procedures regarding access, retention, storage, use, transfer and disposal of documentation related to personally identifiable information (PII). • Developing and conducting Privacy Impact Assessments in accordance with best practices. • 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 • Application of privacy legislation and regulations such as:	

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 2 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	o Freedom of Information and Privacy Protection Act (FIPPA) o Municipal Freedom of Information and Protection of Privacy Act o Personal Information Protection and Electronic Documents Act (PIPEDA) • Application of privacy and security concepts; user authentication processes along with identification, definition and assignment of security roles. (*) Large is defined as an organization with 500 employees or more. To qualify, a project must have a minimum duration of four (4) months.	

C.16 Privacy Impact Assessment Specialist, Level 3

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 3 Name of proposed Resource: _____		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
M16.1	The Contractor must demonstrate that the proposed resource has a minimum of seven (7) years' experience in the last twelve (12) years performing privacy impact assessments (PIA). To qualify, a project must have a minimum duration of four (4) months.	
M16.2	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience, in the last six (6) years prior to the TA issuance date, performing all of the following tasks: • Performing privacy impact assessment (PIA) on IT infrastructure and systems for a Canadian Government (Federal, Provincial, Territorial, Municipal, or Crown Corporation) client or a (*) large Canadian-based commercial client.	

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 3 **Name of proposed Resource: _____**		
Criteria	**Mandatory Requirement**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• 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. • Application of policies and procedures regarding access, retention, storage, use, transfer and disposal of documentation related to personally identifiable information (PII). • Developing and conducting PIA in accordance with best practices. • 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 • Application of privacy legislation and regulations such as: o Freedom of Information and Privacy Protection Act (FIPPA) o Municipal Freedom of Information and Protection of Privacy Act o Personal Information Protection and Electronic Documents Act (PIPEDA) • Application of privacy and security concepts; user authentication processes along with identification, definition and assignment of security roles. (*) Large is defined as an organization with 500 employees or more. To qualify, a project must have a minimum duration of four (4) months.	

2.0 RATED RESOURCE ASSESSMENT CRITERIA

TBIPS Stream 6: Cyber Protection Services

C.1 Strategic Information Technology Security Planning and Protection Consultant, Level 2

Resource Category: C1 Strategic Information Technology Security Planning and Protection Consultant – Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R1.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	15	No Degree/Diploma = 0 points Degree/Diploma = 15 points **Maximum 15 points**	
R1.2	The Contractor should demonstrate that the proposed resource holds one (1) or more of the following valid certifications: • Certified Cloud Security Professional • Certified Information System Security Professional (CISSP) • Certified ISO 27001 Lead Implementer • Certified Information Systems Auditor (CISA) • Certified Information Security Manager (CISM) • Certified in Risk and Information System Control (CRISC) • Cloud Security Alliance Cloud Security Knowledge (CCSK) • GIAC / Any Intermediate or Advanced Cyber Security certification • GIAC / Any Intermediate or Advanced Cyber Defense certification • Payment Card Industry – Qualified Security Assessor (PCI-QSA) • System Security Certified Practitioner (SSCP)	20	0 certifications = 0 points 1 certification = 10 points 2 or more certifications = 20 points **Maximum 20 points**	

Resource Category: C1 Strategic Information Technology Security Planning and Protection Consultant – Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Control Objectives for Information & related Technology (COBIT) • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+ • Sherwood Applied Business Security Architecture (SABSA)			
R1.3	The Contractor should demonstrate that the proposed resource holds one (1) or more of the following valid certifications: • Information Technology Infrastructure Library (ITIL) • Information Technology Service Management (ITSM). • Project Management	5	No certification = 0 points Certification = 5 points **Maximum 5 points**	
Maximum Available Points				40
Minimum Points Required (65%)				26
Contractor Score				

C.1 Strategic Information Technology Security Planning and Protection Consultant, Level 3

Resource Category: C1 Strategic Information Technology Security Planning and Protection Consultant – Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R2.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	

Resource Category: C1 Strategic Information Technology Security Planning and Protection Consultant – Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.			
R2.2	The Contractor should demonstrate the proposed resource holds: A Masters' degree in: Information Technology Security; Cybersecurity and Threat Intelligence; or similar obtained through a recognized Canadian university OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R2.3	The Contractor should demonstrate that the proposed resource holds one (1) or more of the following valid certifications: • Certified Cloud Security Professional • Certified Information System Security Professional (CISSP) • Certified ISO 27001 Lead Implementer • Certified Information Systems Auditor (CISA) • Certified Information Security Manager (CISM) • Certified in Risk and Information System Control (CRISC) • Cloud Security Alliance Cloud Security Knowledge (CCSK) • GIAC / Any Intermediate or Advanced Cyber Security certification • GIAC / Any Intermediate or Advanced Cyber Defense certification • Payment Card Industry – Qualified Security Assessor (PCI-QSA) • System Security Certified Practitioner (SSCP) • Control Objectives for Information & related Technology (COBIT) • CompTIA Security+ • CompTIA Network+	30	0 certifications = 0 points 1 certification = 10 points 2 certifications = 20 points 3 or more certifications = 30 points **Maximum 30 points**	

Resource Category: C1 Strategic Information Technology Security Planning and Protection Consultant – Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• CompTIA Cloud+ • CompTIA CySA+ • Sherwood Applied Business Security Architecture (SABSA)			
R2.4	The Contractor should demonstrate that the proposed resource holds one (1) or more of the following valid certifications: • Information Technology Infrastructure Library (ITIL) • Information Technology Service Management (ITSM). • Project Management	5	No certification = 0 points Certification = 5 points **Maximum 5 points**	
Maximum Available Points				55
Minimum Points Required (65%)				35
Contractor Score				

C.3 Information Technology Security TRA and C&A Analyst, Level 2

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R3.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment,*** if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R3.2	The Contractor should demonstrate that the proposed resource has hands-on	30	Points will be allocated once for	

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	experience within the last five (5) years completing the following deliverables: • (SoS) Statements of Sensitivity for IT systems processing Protected or Classified information using the CSEC Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1). • (TRA) IT Security Threat and Risk Assessments supporting IT systems processing Protected or Classified information using CSEC Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1). • (SA&A/C&A) Security Assessment and Authorization / Security and Accreditation packages for IT systems processing Protected or Classified information using IT SA&A methodology and terminology as defined in CSEC Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33). • (TSR-P) Technical Security Reviews* of Commercial-Off-the-Shelf (COTS) hardware or software product(s). *Each TSR-P can be defined as containing all of the following: - Product functional information; - Product technical information; - Security evaluation of the security features provided by the product; - Vulnerability assessment; and - Recommendations. • (IT-SIA) IT Security Impact Analysis* reports for IT solutions. *The IT Security Impact Analysis reports can be defined as containing all of the following: - Type of security deliverable(s) required; - Estimate of the level of effort required; and		each deliverable type satisfying the criteria: SoS = 5 points TRA = 5 points SA&A/C&A = 5 points TSR-P = 5 points IT-SIA = 5 points ITSA-Cloud = 5 points **Maximum 30 points**	

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	- Estimate of costs. • (ITSA-Cloud) IT Security assessments on IT solutions configured using an outsourced ***Cloud Computing*** model.			
R3.3	The Contractor should demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher	10	0 certifications = 0 points 1 certification = 5 points 2 or more certifications = 10 points **Maximum 10 points**	
R3.4	The Contractor should demonstrate that the proposed resource has experience in risk management activities for Cloud-based applications for government projects/initiatives involving any of the following: • Biometric identification	15	5 points per project **Maximum 15 points**	

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile or Multi-experience • ***Artificial Intelligence*** or ***Machine Learning*** • Robotic Process Automation Note: A qualifying project must have a minimum duration of four (4) months.			
Maximum Available Points				65
Minimum Points Required (65%)				42
Contractor Score				

C.3 Information Technology Security TRA and C&A Analyst, Level 3

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R4.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R4.2	The Contractor should demonstrate that the proposed resource has hands-on experience within the last five (5) years	30	Points will be allocated for two or more of each deliverable type	

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 3 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
	completing two or more of each of the following deliverables: • (SoS) Statements of Sensitivity for IT systems processing Protected or Classified information using the CSEC Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1). • (TRA) IT Security Threat and Risk Assessments supporting IT systems processing Protected or Classified information using CSEC Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1). • (SA&A/C&A) Security Assessment and Authorization / Security and Accreditation packages for IT systems processing Protected or Classified information using IT SA&A methodology and terminology as defined in CSEC Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33). • (TSR-P) A Technical Security Reviews* of Commercial-Off-the-Shelf (COTS) hardware or software product(s). *Each TSR-P can be defined as containing all of the following: - Product functional information; - Product technical information; - Security evaluation of the security features provided by the product; - Vulnerability assessment; and - Recommendations. • (IT-SIA)*IT Security Impact Analysis reports for IT solutions. *The IT Security Impact Analysis reports can be defined as containing all of the following: - Type of security deliverable(s) required; - Estimate of the level of effort required; and		satisfying the criteria, up to the maximum for that deliverable type: SoS = 5 points TRA = 5 points SA&A/C&A = 5 points TSR-P = 5 points IT-SIA = 5 points ITSA-Cloud = 5 points **Maximum 30 points**	

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	- Estimate of costs. • (ITSA-Cloud) An IT Security Assessments on IT solutions configured using an outsourced ***Cloud Computing*** model.			
R4.3	The Contractor should demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+CompTIA Mobile App Security+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher	15	0 certifications = 0 points 1 certification = 5 points 2 certifications = 10 points 3 or more certifications = 15 points **Maximum 15 points**	
R4.4	The Contractor should demonstrate that the proposed resource has experience in risk management activities for Cloud-based applications for government projects/initiatives involving any of the following: • Biometric identification	10	2 points per project **Maximum 10 points**	

Resource Category: C.3 Information Technology Security TRA and C&A Analyst, Level 3 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
	• Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile or Multi-experience • ***Artificial Intelligence*** or ***Machine Learning*** • Robotic Process Automation Note: A qualifying project must have a minimum duration of four (4) months.			
Maximum Available Points				65
Minimum Points Required (65%)				42
Contractor Score				

C.7 Information Technology Security Design Specialist, Level 2

Resource Category: C.7 Information Technology Security Design Specialist, Level 2 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
R5.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R5.2	The Contractor should demonstrate that the proposed resource has hands-on experience (*) in the last seven (7) years designing, architecting or engineering IT	10	0 to <1 year = 0 points	

Resource Category: C.7 Information Technology Security Design Specialist, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	Security components and architectures while working with CSEC Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33) guidelines. (*) To qualify, at least one (1) year must have involved processing data at a security classification of Protected B or higher. To qualify, a project must have a minimum duration of four (4) months.		1 to <2 years = 2 points 2 to <3 years = 4 points 3 to <4 years = 6 points 4 to <5 years = 8 points 5+ years = 10 points **Maximum 10 points**	
R5.3	The Contractor should demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher	10	0 certifications = 0 points 1 certification = 5 points 2 or more certifications = 10 points **Maximum 10 points**	
R5.4	The Contractor should demonstrate that the proposed resource has hands-on	4	2 points per project	

Resource Category: C.7 Information Technology Security Design Specialist, Level 2 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
	experience in security design for Cloud-based applications for government projects/initiatives involving any of the following: • Biometric identification • Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile or Multi-experience • ***Artificial Intelligence*** or ***Machine Learning*** • Robotic Process Automation • Analytic Pipelines To qualify, a project must have a minimum duration of four (4) months.		**Maximum 4 points**	
Maximum Available Points				34
Minimum Points Required (65%)				22
Contractor Score				

C.7 Information Technology Security Design Specialist, Level 3

Resource Category: C.7 Information Technology Security Design Specialist, Level 3 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
R6.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	

Resource Category: C.7 Information Technology Security Design Specialist, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.			
R6.2	The Contractor should demonstrate the proposed resource holds: A Masters' degree in: Information Technology Security; Cybersecurity and Threat Intelligence; or similar obtained through a recognized Canadian university OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R6.3	The Contractor should demonstrate that the proposed resource has hands-on experience (*) in the last seven (7) years performing either of the following activities: • designing, architecting or engineering IT Security components and architectures for ***enterprise solutions***; OR • designing, architecting or engineering IT Security components and architectures involving ***emerging technologies***; while working with CSEC Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach (ITSG-33) guidelines. (*) To qualify, at least one (1) year must have involved processing data at a security classification of Protected B or higher. To qualify, a project must have a minimum duration of four (4) months.	10	0 to <1 year = 0 points 1 to <2 years = 2 points 2 to <3 years = 4 points 3 to <4 years = 6 points 4 to <5 years = 8 points 5+ years = 10 points **Maximum 10 points**	

Resource Category: C.7 Information Technology Security Design Specialist, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R6.4	The Contractor should demonstrate that the proposed resource holds two or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher	20	0-1 certifications = 0 points 2 certifications = 10 points 3 or more certifications = 20 points **Maximum 20 points**	
R6.5	The Contractor should demonstrate that the proposed resource has hands-on experience in security design for Cloud-based applications for government projects/initiatives involving any of the following: • Biometric identification • Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile or Multi-experience	10	2 points per project **Maximum 10 points**	

Resource Category: C.7 Information Technology Security Design Specialist, Level 3 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
	• ***Artificial Intelligence*** or Machine Learning • Robotic Process Automation • Analytic Pipelines To qualify, a project must have a minimum duration of four (4) months.			
Maximum Available Points				60
Minimum Points Required (65%)				42
Contractor Score				

C.8 Network Security Analyst, Level 2

Resource Category: C.8 Network Security Analyst, Level 2 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
R7.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R7.2	The Contractor must demonstrate that the proposed resource has one or more of the following certifications: • A current and valid Firewall Administrator certification from a ***Next Generation Firewall*** vendor (e.g. Cisco, Fortinet, Palo Alto, etc.). • AWS Certified Advanced Networking Specialty	10	0 certifications = 0 points 1 certification = 5 points 2 or more certifications = 10 points **Maximum 10 points**	

Resource Category: C.8 Network Security Analyst, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Microsoft Certified: Azure Administrator Associate AND Azure Enterprise-Class Networking Workshop elective (counts as 1 certification) • MCSE: Cloud Platforms and Infrastructure			
R7.3	The Contractor should demonstrate that the proposed resource has experience in network security for government projects/initiatives involving any of the following: • Biometric identification • Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile • ***Artificial Intelligence*** or ***Machine Learning*** • Robotic Process Automation • Analytic Pipelines Note: A qualifying project must have a minimum duration of four (4) months.	12	4 points per project **Maximum 12 points**	
Maximum Available Points				32
Minimum Points Required (65%)				20
Contractor Score				

C.8 Network Security Analyst, Level 3

Resource Category: C.8 Network Security Analyst, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R8.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R8.2	The Contractor must demonstrate that the proposed resource has one or more of the following certifications: • A current and valid Firewall Administrator certification from a ***Next Generation Firewall*** vendor (e.g. Cisco, Fortinet, Palo Alto, etc.). • AWS Certified Advanced Networking Specialty • Microsoft Certified: Azure Administrator Associate AND Azure Enterprise-Class Networking Workshop elective (counts as 1 certification) • MCSE: Cloud Platforms and Infrastructure	10	0 certifications = 0 points 1 certification = 5 points 2 or more certifications = 10 points **Maximum 10 points**	
R8.3	The Contractor should demonstrate that the proposed resource holds two or more certifications from the list below: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information	10	0-1 certifications = 0 points 2 or more certifications = 10 points **Maximum 10 points**	

Resource Category: C.8 Network Security Analyst, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Technology Infrastructure Library (ITIL) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Cloud+ • CompTIA Network+ • CompTIA Security+Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher			
R8.4	The Contractor should demonstrate that the proposed resource has experience in network security for government projects/initiatives involving any of the following: • Biometric identification • Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile • ***Artificial Intelligence*** or ***Machine Learning*** • Robotic Process Automation • Analytic Pipelines Note: A qualifying project must have a minimum duration of four (4) months.	10	2 points per project **Maximum 10 points**	
Maximum Available Points				40
Minimum Points Required (65%)				26
Contractor Score				

C.9 Information Technology Security Systems Operator, Level 2

Resource Category: C.9 Information Technology Security Systems Operator, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R9.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment,*** if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R9.2	The Contractor must demonstrate that the proposed resource has: A current and valid Firewall Administrator certification from a ***Next Generation Firewall*** vendor (e.g. Cisco, Fortinet, Palo Alto, etc.).	5	0 certifications = 0 points 1 certification = 5 points **Maximum 5 points**	
R9.3	The Contractor should demonstrate that the proposed resource holds two or more certifications from the list below: • AWS Certified Security Specialty • Microsoft Azure Security Technologies • MCSE: Cloud Platforms and Infrastructure • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Technology Infrastructure	10	0-1 certifications = 0 points 2 or more certifications = 10 points **Maximum 10 points**	

Resource Category: C.9 Information Technology Security Systems Operator, Level 2 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
	Library (ITIL) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Cloud+ • CompTIA Network+ • CompTIA Security+ • CompTIA Server+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher • Certified Windows Security Administrator • Certified UNIX Security Administrator • Certified Detection Analyst • Certified Incident Handler			
Maximum Available Points				25
Minimum Points Required (65%)				15
Contractor Score				

C.9 Information Technology Security Systems Operator, Level 3

Resource Category: C.9 Information Technology Security Systems Operator, Level 3 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
R10.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	

Resource Category: C.9 Information Technology Security Systems Operator, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.			
R10.2	The Contractor should demonstrate that the proposed resource has: A current and valid Firewall Administrator certification from a ***Next Generation Firewall*** vendor (e.g. Cisco, Fortinet, Palo Alto, etc.).	5	0 certifications = 0 points 1 certification = 5 points **Maximum 5 points**	
R10.3	The Contractor should demonstrate that the proposed resource holds two or more certifications from the list below: • AWS Certified Security Specialty • Microsoft Azure Security Technologies • MCSE: Cloud Platforms and Infrastructure • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Technology Infrastructure Library (ITIL) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Cloud+ • CompTIA Network+ • CompTIA Security+ • CompTIA Server+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification)	15	0-1 certifications = 0 points 2 certifications = 10 points 3 or more certifications = 15 points **Maximum 15 points**	

Resource Category: C.9 Information Technology Security Systems Operator, Level 3 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
	• SABSA Chartered Security Architect Foundation (SCF) or higher • Certified Windows Security Administrator • Certified UNIX Security Administrator • Certified Detection Analyst • Certified Incident Handler			
Maximum Available Points				30
Minimum Points Required (65%)				19
Contractor Score				

C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
R11.1	The Contractor should demonstrate that the proposed resource has hands-on experience testing web and/or mobile application security for the ***OWASP Top 10*** Most Critical Application Security Risks and providing assistance and guidance to developers to ensure a high level of application security.	20	0 to <1 year = 0 points 1 to <3 years = 10 points 3+ years = 20 points **Maximum 20 points**	
R11.2	The Contractor should demonstrate that the proposed resource has hands-on experience performing ***vulnerability scans*** and ***penetration testing*** for public ***Cloud-computing*** environments, services or solutions including all of the following activities: • Conducting thorough ***vulnerability scans*** and ***penetration testing*** to identify vulnerabilities that may leave the organization or data open to threats or theft; and	20	5 points per project **Maximum 20 points**	

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2 Name of Proposed Resource: _____				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Producing an actionable and prioritized list of deficiencies with explanations and technical recommendations			
R11.3	The Contractor should demonstrate that the proposed resource has hands-on experience in the last three years completing technical vulnerability analysis project(s) for Data Base Management Systems (DBMS).	5	5 points per project **Maximum 5 points**	
R11.4	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Computer Science or a related field in Information Technology, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
Maximum Available Points				55
Minimum Points Required (65%)				35
Contractor Score				

C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3 Name of Proposed Resource: _____				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R12.1	The Contractor should demonstrate that the proposed resource has hands-on experience testing web and/or mobile application security for the ***OWASP Top 10*** Most Critical Application Security Risks and providing assistance and guidance to developers to ensure a high level of application security.	20	0 to <3 years = 0 points 3 to <5 years = 10 points 5+ years = 20 points **Maximum 20 points**	

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R12.2	The Contractor should demonstrate that the proposed resource has hands-on experience within the last three years, assessing ***Cloud-computing*** IT architecture design against CSEC Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22) and CSEC Network Security Zoning (ITSG-38).	5	1 project = 1 point 2 projects = 2 points 3 projects = 3 points 4 or more projects = 5 points **Maximum 5 points**	
R12.3	The Contractor should demonstrate that the proposed resource has hands-on experience within the last three years completing technical vulnerability analysis project(s) for Data Base Management Systems (DBMS).	5	1 project = 1 point 2 projects = 3 points 3 or more projects = 5 points **Maximum 5 points**	
R12.4	The Contractor should demonstrate that the proposed resource possesses two or more current professional certification from any of the following: • AWS Certified Security Specialty • Microsoft Azure Security Technologies • MCSE: Cloud Platforms and Infrastructure • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • System Security Certified Practitioner (SSCP) d'ISC2 • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • CompTIA CySA+ • CompTIA PenTest+ • Certified Wireless Security Professional (CWSP) • GIAC any certification in Cloud Security	10	0-1 certification = 0 points 2 or more certifications = 10 points **Maximum 10 points**	

Resource Category: C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• GIAC any certification in Cyber Defense • GIAC any certification in Offensive Operations • GIAC Security Expert (GSE) Certification • Certified Windows Security Administrator • Certified UNIX Security Administrator • Certified Vulnerability Assessor (CVA) • EC Council Certified Ethical Hacker • SANS Mobile Device Security and Ethical Hacking			
R12.5	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Computer Science or a related field in Information Technology, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
Maximum Available Points				50
Minimum Points Required (65%)				32
Contractor Score				

C.14 Information Technology Security R&D Specialist (SME), Level 2

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R13.1	The Contractor should demonstrate that the proposed resource has:	10	No Degree/Diploma = 0 points	

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.		Degree/Diploma = 10 points **Maximum 10 points**	
R13.2	The Contractor should demonstrate the proposed resource holds: A Masters' degree in: Information Technology Security; Cybersecurity and Threat Intelligence; Software Engineering or similar obtained through a recognized Canadian university OR An equivalent ***Canadian academic credential assessment,*** if obtained outside Canada.	5	No Degree/Diploma = 0 points Degree/Diploma = 5 points **Maximum 5 points**	
R13.3	The Contractor should demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Systems Security Architecture Professional (ISSAP) • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+	10	0 certifications = 0 points 1 certification = 5 points 2 or more certifications = 10 points **Maximum 10 points**	

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher			
R13.4	The Contractor should demonstrate that the proposed resource has hands-on experience in security design for Cloud-based applications for projects/initiatives involving any of the following: • Biometric identification • Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile or Multi-experience • ***Artificial Intelligence*** or ***Machine Learning*** • Robotic Process Automation • Analytic pipelines To qualify, a project must have a minimum duration of four (4) months.	15	5 points per project **Maximum 15 points**	
Maximum Available Points				40
Minimum Points Required (65%)				26
Contractor Score				

C.14 Information Technology Security R&D Specialist (SME), Level 3

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R14.1	The Contractor should demonstrate that the proposed resource has: A university degree or post-secondary diploma in Information Technology, Computer Science or Electrical Engineering fields, obtained through a recognized Canadian university or college; OR An equivalent ***Canadian academic credential assessment,*** if obtained outside Canada.	10	No Degree/Diploma = 0 points Degree/Diploma = 10 points **Maximum 10 points**	
R14.2	The Contractor should demonstrate the proposed resource holds: A Masters' degree in: Information Technology Security; Cybersecurity and Threat Intelligence; Software Engineering or similar obtained through a recognized Canadian university OR An equivalent ***Canadian academic credential assessment,*** if obtained outside Canada.	5	No Degree/Diploma = 0 points Degree/Diploma = 5 points **Maximum 5 points**	
R14.3	The Contractor should demonstrate that the proposed resource holds one or more of the following valid certifications: • Certified Cloud Security Professional (CCSP) • Certified Information System Security Professional (CISSP) Certification • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Certified in Risk and Information Systems Control (CRISC) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP)	15	0 certifications = 0 points 1 certification = 5 points 2 certifications = 10 points 3 or more certifications = 15 points **Maximum 15 points**	

Resource Category: C.14 Information Technology Security R&D Specialist (SME), Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
	• Information Systems Security Architecture Professional (ISSAP) • CompTIA Security+ • CompTIA Network+ • CompTIA Cloud+ • Certified Wireless Security Professional (CWSP) • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher			
R14.4	The Contractor should demonstrate that the proposed resource has hands-on experience in security design for Cloud-based applications for projects/initiatives involving any of the following: • Biometric identification • Multi-factor authentication, secure enclave processing • ***Public Cloud*** Infrastructure-as-a-Service • Cloud-based Identity Access Management • Mobile or Multi-experience • ***Artificial Intelligence*** or ***Machine Learning*** • Robotic Process Automation • Analytic pipelines To qualify, a project must have a minimum duration of four (4) months.	10	2 points per project **Maximum 10 points**	
Maximum Available Points				40
Minimum Points Required (65%)				26
Contractor Score				

C.16 Privacy Impact Assessment Specialist, Level 2

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 2 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
R15.1	The Contractor should demonstrate that the proposed resource has: A university degree in any discipline obtained through a recognized Canadian university; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree = 0 points Degree = 10 points **Maximum 10 points**	
R15.2	The Contractor should demonstrate the proposed resource's experience in excess (*) of the minimum required under M15.1 for this resource category. (*) The additional years of experience is not required to fall within the past 10 years. To qualify, a project must have a minimum duration of four (4) months.	10	Total experience: 0 up to 4 years = 0 points 4+ years up to 5 years = 3 points 5+ years up to 6 years = 6 points 6+ years up to 7 years = 8 points More than 7 years = 10 points **Maximum 10 points**	
R15.3	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).	10	No certification = 0 point 1 Certification = 10 points **Maximum 10 points**	
R15.4	The Contractor should demonstrate that the proposed resource has a experience, within the last five (5) years prior to the TA issuance date with the identification of privacy risks associated with the use of	5	5 points per project **Maximum 5 points**	

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 2 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
	biometrics or other ***emerging technologies***. To qualify, a project must have a minimum duration of four (4) months.			
Maximum Available Points				35
Minimum Points Required (65%)				21
Contractor Score				

C.16 Privacy Impact Assessment Specialist, Level 3

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 3 Name of Proposed Resource: _____				
#	Point-Rated Requirement	Points Max	Point Grid	Demonstrated Experience Cross-reference to Proposal/Project# /Resume or CV
R16.1	The Contractor should demonstrate that the proposed resource has: A university degree in any discipline obtained through a recognized Canadian university; OR An equivalent ***Canadian academic credential assessment***, if obtained outside Canada.	10	No Degree = 0 points Degree = 10 points **Maximum 10 points**	
R16.2	The Contractor should demonstrate the proposed resource's experience in excess (*) of the minimum required under M1 for this resource category. (*) The additional years of experience is not required to fall within the past 12 years. To qualify, a project must have a minimum duration of four (4) months.	10	Total experience: 0 up to 7 years = 0 points 7+ years up to 8 years = 3 points 8+ years up to 9 years = 6 points 9+ years up to 10 years = 8 points	

Resource Category: C.16 Privacy Impact Assessment Specialist, Level 3 **Name of Proposed Resource: _____**				
#	**Point-Rated Requirement**	**Points Max**	**Point Grid**	**Demonstrated Experience** **Cross-reference to Proposal/Project# /Resume or CV**
			More than 10 years = 10 points **Maximum 10 points**	
R16.3	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).	10	No certification = 0 point 1 Certification = 10 points **Maximum 10 points**	
R16.4	The Contractor should demonstrate that the proposed resource holds a current and valid Certified Internal Auditor (CIA) or Certified Information Systems Auditor (CISA) certification.	10	0 certifications = 0 points 1 certification = 5 points 2 certifications = 10 points **Maximum 10 points**	
R16.5	The Contractor should demonstrate that the proposed resource has experience, within the last five (5) years with the identification of privacy risks associated with the use of biometrics or other ***emerging technologies***. To qualify, a project must have a minimum duration of four (4) months.	5	5 points per project **Maximum 5 points**	
Maximum Available Points				45
Minimum Points Required (65%)				27
Contractor Score				

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

4. CERTIFICATION OF LANGUAGE - [English or Bilingual or French]

The Contractor certifies that the proposed resource(s) in response to this draft Task Authorization is/are

[Option 1 - Unilingual English] 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.

[Option 2 - Bilingual] fluent in both official languages of Canada (French and English). The individual(s) proposed must be able to communicate orally and in writing in French and English without any assistance and with minimal errors.

[Option 3 - Unilingual French] fluent in French. The individual(s) proposed must be able to communicate orally and in writing in French without any assistance and with minimal errors.

_____ _____

Print name of authorized individual & sign above | Date

ANNEX B

BASIS OF PAYMENT

CONTRACT PERIOD 1 :

Initial Contract Period

(Date of Contract award for 1 year
(insert at contract award)

Resource Category	Level of Expertise	Firm Per Diem Rate
TBIPS Stream 6: Cyber Protection Services		
C.1 Strategic Information Technology Security Planning & Protection Consultant	2	
C.1 Strategic Information Technology Security Planning & Protection Consultant	3	
C.3 Information Technology Security TRA and C&A Analyst	2	
C.3 Information Technology Security TRA and C&A Analyst	3	
C.7 Information Technology Security Design Specialist	2	
C.7 Information Technology Security Design Specialist	3	
C.8 Network Security Analyst	2	
C.8 Network Security Analyst	3	
C.9 Information Technology Security Systems Operator	2	
C.9 Information Technology Security Systems Operator	3	
C.11 Information Technology Security Vulnerability Analysis Specialist	2	
C.11 Information Technology Security Vulnerability Analysis Specialist	3	
C.14 Information Technology Security Research and Development Specialist	2	
C.14 Information Technology Security Research and Development Specialist	3	
C.16 Privacy Impact Assessment Specialist	2	
C.16 Privacy Impact Assessment Specialist	3	

OPTION PERIODS:

Option Period 1

Starts after the initial 1 year period for 1 year

(_____ to _____)
(insert at contract award)

Resource Category	Level of Expertise	Firm Per Diem Rate
TBIPS Stream 6: Cyber Protection Services		
C.1 Strategic Information Technology Security Planning & Protection Consultant	2	
C.1 Strategic Information Technology Security Planning & Protection Consultant	3	
C.3 Information Technology Security TRA and C&A Analyst	2	
C.3 Information Technology Security TRA and C&A Analyst	3	
C.7 Information Technology Security Design Specialist	2	
C.7 Information Technology Security Design Specialist	3	
C.8 Network Security Analyst	2	
C.8 Network Security Analyst	3	
C.9 Information Technology Security Systems Operator	2	
C.9 Information Technology Security Systems Operator	3	
C.11 Information Technology Security Vulnerability Analysis Specialist	2	
C.11 Information Technology Security Vulnerability Analysis Specialist	3	
C.14 Information Technology Security Research and Development Specialist	2	
C.14 Information Technology Security Research and Development Specialist	3	
C.16 Privacy Impact Assessment Specialist	2	
C.16 Privacy Impact Assessment Specialist	3	

OPTION PERIODS:

Option Period 2

Starts after the option 1 period for 1 year

(_____ to _____)
(insert at contract award)

Resource Category	Level of Expertise	Firm Per Diem Rate
TBIPS Stream 6: Cyber Protection Services		
C.1 Strategic Information Technology Security Planning & Protection Consultant	2	
C.1 Strategic Information Technology Security Planning & Protection Consultant	3	
C.3 Information Technology Security TRA and C&A Analyst	2	
C.3 Information Technology Security TRA and C&A Analyst	3	
C.7 Information Technology Security Design Specialist	2	
C.7 Information Technology Security Design Specialist	3	
C.8 Network Security Analyst	2	
C.8 Network Security Analyst	3	
C.9 Information Technology Security Systems Operator	2	
C.9 Information Technology Security Systems Operator	3	
C.11 Information Technology Security Vulnerability Analysis Specialist	2	
C.11 Information Technology Security Vulnerability Analysis Specialist	3	
C.14 Information Technology Security Research and Development Specialist	2	
C.14 Information Technology Security Research and Development Specialist	3	
C.16 Privacy Impact Assessment Specialist	2	
C.16 Privacy Impact Assessment Specialist	3	

ANNEX C

SECURITY REQUIREMENTS CHECK LIST

Refer to SRCL/LVERS document in the Attachment section on Buy&sell.gc.ca

ANNEX C1
SECURITY CLASSIFICATION GUIDE

Services with various categories will be required.

Resource Category	Level of Resource	Minimum Security Clearance
C.1 Strategic Information Technology Security Planning & Protection Consultant	Level 2	Secret
C.1 Strategic Information Technology Security Planning & Protection Consultant	Level 3	Secret
C.3 Information Technology Security TRA and C&A Analyst	Level 2	Secret
C.3 Information Technology Security TRA and C&A Analyst	Level 3	Secret
C.7 Information Technology Security Design Specialist	Level 2	Secret
C.7 Information Technology Security Design Specialist	Level 3	Secret
C.8 Network Security Analyst	Level 2	Secret
C.8 Network Security Analyst	Level 3	Secret
C.9 Information Technology Security Systems Operator	Level 2	Secret
C.9 Information Technology Security Systems Operator	Level 3	Secret
C.11 Information Technology Security Vulnerability Analysis Specialist	Level 2	Secret
C.11 Information Technology Security Vulnerability Analysis Specialist	Level 3	Secret
C.14 Information Technology Security Research and Development Specialist	Level 2	Secret
C.14 Information Technology Security Research and Development Specialist	Level 3	Secret
C.16 Privacy Impact Assessment Specialist	Level 2	Secret
C.16 Privacy Impact Assessment Specialist	Level 3	Secret

All resources assigned to this Contract without exception must be cleared at a minimum to the SECRET Status Level.

ATTACHMENT 1.1

List of the substantive changes that were made in this RFP. Canada will not be held responsible for inadvertently omitting any changes.

Part #, Article and sub-article of the Present RFP	Substantive Changes
Security Requirement	Delete SRCL #23 Replace with SRCL #19
Annex A, Statement of Work Section 2	Canada Border Services Agency (CBSA) is seeking the services of an organization to provide professional IM/IT cyber security resources with particular expertise in compliance and security of the public cloud and emerging technologies as described further in this Statement of Work.
Annex A, Statement of Work Section 5 (a)	i. Assess the Security Operations Team(s), advise on the readiness of responsible areas to manage and fulfill their responsibilities; elaborate and develop specific management actions with respect to tools, training, personnel, collaboration and communication required. ii. Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings iii. Conduct Certification & Accreditation activities iv. Conduct technical security assessments against CBSA assets including: • Protected B/Medium Integrity/Medium Availability (PBMM) level and unclassified workloads • Dev/Test environments and data (data masking, obfuscation or encryption) • Solutions deployed as IaaS, PaaS and SaaS – inside and outside of Canada • Tailoring security control profiles • Reviewing and incorporating third party assessment evidence (CCCS, SOC, FedRAMP, ISO, etc..)
Annex A, Statement of Work Section 5 (c)	ii. Assist CBSA in the selection, deployment, integration, configuration and maintenance of best-in-class monitoring and other cyber security tools; Develop and integrate security processes into cloud service management; Establish strategic and operational security metrics; iii. Perform security systems monitoring and incident response; conduct incident investigations; prepare security briefings, reports and action plans.
Annex A, Statement of Work Section 5 (d)	d. Provide technical guidance, support, engineering and research in the design, development and securing of solutions based on emerging or evolving technologies (such as public-cloud networks, mobile applications, biometrics, robotic process automation, APIs, artificial intelligence/machine learning, and RFID):
Annex A, Statement of Work Section 5 (d)	iii. Review and advise on solution designs, development (including code review), configuration and operations; iv. Provide instructive analysis, advice, engineering and design support to CBSA on feasible methods to enable and facilitate the adoption and use of innovative technologies while strengthening their security posture and/or aiding to mitigate the threat exposure(s) such technologies present

<table>
<tr><th>Part #, Article and sub-article of the Present RFP</th><th>Substantive Changes</th></tr>
<tr><td></td><td>v. Provide updates as the technology security risks evolve
vi. Provide advice on how CBSA can assess and implement measures to constantly adjust to new technologies and development in the cyber security domain.</td></tr>
<tr><td>Annex A, Statement of Work Section 6</td><td>To address the work areas from Section 5, the Contractor must provide CBSA with IT Cyber security Professional Resources in the following, but not limited to, TBIPS categories on an ‘as and when’ requested basis as initiated through Task Authorizations (TAs).

<table><tr><th>Resource Categories</th><th>Levels</th></tr><tr><td>C.1 Strategic IT Security Planning & Protection Consultant</td><td>2, 3</td></tr><tr><td>C.3 Information Technology Security TRA and C&A Analyst</td><td>2, 3</td></tr><tr><td>C.7 Information Technology Security Design Specialist</td><td>2, 3</td></tr><tr><td>C.8 Network Security Analyst</td><td>2, 3</td></tr><tr><td>C.9 Information Technology Security Systems Operator</td><td>2, 3</td></tr><tr><td>C.11 Information Technology Security Vulnerability Analysis Specialist</td><td>2, 3</td></tr><tr><td>C.14 Information Technology Security Research and Development Specialist</td><td>2, 3</td></tr><tr><td>C.16 Privacy Impact Assessment Specialist</td><td>2, 3</td></tr></table></td></tr>
<tr><td>Annex A, Statement of Work Section 6</td><td>(Deleted)
Workstream 1
6.1 Business Analyst, Levels 2 and 3 (and related activities)
Workstream 2
6.4 C.6 Information Technology Security Engineer, Levels 2 and 3 (and related activities)</td></tr>
<tr><td>Annex A, Statement of Work Section 6</td><td>(The following were renumbered)
6.1 C.1 Strategic Information Technology Security Planning and Protection Consultant, Levels 2 & 3

6.2 C.3 Information Technology Security TRA and C&A Analyst, Levels 2 & 3

6.3 C.7 Information Technology Security Design Specialist, Levels 2 & 3
6.4 C.8 Network Security Analyst, Levels 2 & 3
6.5 C.9 Information Technology Security Systems Operator, Levels 2 & 3
6.6 C.11 Information Technology Security Vulnerability Analysis Specialist, Levels 2 & 3
6.7 C.14 Information Technology Security Research and Development Specialist, Levels 2 & 3
6.8 C.16 Privacy Impact Assessment Specialist, Levels 2 & 3
6.9 Common</td></tr>
<tr><td>Annex A, Statement of Work Section 6.8</td><td>(Added)
h. Conduct privacy analysis to identify privacy risks and provide evidence of compliance with the data privacy requirements of Canada’s international partners, where applicable.</td></tr>
<tr><td>Annex A, Statement of Work</td><td>(Deleted)
• Perform business function analysis and business impact assessments</td></tr>
</table>

Part #, Article and sub-article of the Present RFP	Substantive Changes
Section 6.9	
Annex A, Statement of Work Section 7	(Added) d. Quarterly Task Authorization Usage Report (Added) 21. Change Management documentation; 22. Configuration Management documentation; 46. Conversation notes
Annex A, Statement of Work Section 9	The Contractor personnel may be requested to work both onsite at CBSA premises in the NCR and/or remotely offsite at the Contractor's site. The location where services will be conducted, will be identified in each Task Authorization (TA). Certain services, (5) b) in particular, may partially be executed outside of the CBSA environments using the Supplier's equipment and/or CBSA equipment, however at no time is protected data to be stored externally to CBSA infrastructure. The remaining services and work will be conducted and integrated within CBSA environments using CBSA equipment.
Annex A, Statement of Work Section 14	(Added) All work must be conducted within Canada and all CBSA technology and information is to remain resident within Canada
Annex A1 Glossary	(Deleted definition) Managed IM/IT Security Services (MSS) / Managed IM/IT Security Services Provider (MSSP) (Added definition) Security Assessment Security Assessment & Authorization (SA&A) Review
Attachment 4.1 Mandatory Technical Criteria	(Added) Where a copy of Contract/Task Authorization documentation is required to provide verification of the details provided by the Bidder to demonstrate compliance with a criteria, the following is sufficient: 1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or 2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or 3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.

Part #, Article and sub-article of the Present RFP	Substantive Changes
Attachment 4.1 Mandatory Technical Criteria Section 1.0	(Deleted) CM1
Attachment 4.1 Mandatory Technical Criteria Section 1.0	(Renumbered CM2 to CM1, Revised Content) **Bidder's (*) billable ($) providing IM/IT *Cyber Security* Professional Services involving Public Cloud infrastructure~~.~~** The Bidder must provide a maximum of ten (10) reference contracts with a minimum cumulative billed value of $10,000,000.00 CDN (excluding taxes) for IM/IT ***Cyber Security*** Professional Services involving ***Public Cloud*** infrastructure in the last 5 years as of the publication date of this RFP performing or delivering either individually or collectively **ALL** of the following services: a) Performing technical ***Vulnerability Scans*** and ***Penetration testing*** against environments designed to meet any of the following security control profiles: a. Protected B Medium Integrity Medium Availability (PBMM) or higher b. FEDRAMP Moderate or High c. ISO 27001 and ISO 27017 d. NIST SP 800-53 Moderate or High b) Performing ***IT Enterprise Security Risk Assessments***, ***Security Audits***, or ***Security Assessment & Authorization Reviews*** c) Providing technical guidance, support, engineering and research in the development of ***secure*** solutions d) Security Operations: Performing information technology system monitoring, security incident handling, investigations and response To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CM1** • Projects do not have to contain all services, however all services must be demonstrated; • Each project must have been for ***Cyber Security*** professional services involving ***Public Cloud*** infrastructure and at least one identified service; • The Bidder must provide a copy of Contract/Task Authorization documentation to substantiate the details provided. **(*) In evaluating corporate experience for this criteria, Canada will consider the corporate experience referred to in:** **Part 3, Section 3.2** **Section I: Technical Bid** **Substantiation of Technical Compliance** **Paragraph C (page 14-15)**
Attachment 4.1 Mandatory Technical Criteria Section 1.0	(Renumbered CM3 to CM2, Revised Content) **Bidder's provision of concurrent IM/IT *Cyber Security* Professional Services**

<table>
<tr><th>Part #, Article and sub-article of the Present RFP</th><th>Substantive Changes</th></tr>
<tr><td></td><td>
The Bidder must have been awarded, within the past five (5) years as of the publication date of this RFP, one (1) contract supplying IM/IT Cyber Security professional services where:

• The Bidder provided a minimum of five (5) concurrent resources from any of the resource categories, or equivalent resource categories (*) under different titles, listed in the table below for six (6) consecutive months;
• Each of the resources must have provided IM/IT Cyber Security professional services for a minimum of 100 billable days during the six (6) consecutive month period.

<table>
<tr><th>Resource Category</th></tr>
<tr><td>C.1 Strategic Information Technology Security Planning and Protection Consultant</td></tr>
<tr><td>C.3 Information Technology Security TRA and C&A Analyst</td></tr>
<tr><td>C.7 Information Technology Security Design Specialist</td></tr>
<tr><td>C.8 Network Security Analyst</td></tr>
<tr><td>C.9 Information Technology Security Systems Operator</td></tr>
<tr><td>C.11 Information Technology Security Vulnerability Analysis Specialist</td></tr>
<tr><td>C.14 Information Technology Security Research & Development Specialist</td></tr>
<tr><td>C.16 Privacy Impact Assessment Specialist</td></tr>
</table>

(*) In the case a resource category title in the reference contract is not identical (**) to the resource category in the table above, the Bidder must provide substantiation that the work performed includes the associated tasks (***), excluding Common tasks itemized in Annex A - Statement of Work, for the listed resource category as outlined below:

C.1 Strategic Information Technology Security Planning and Protection Consultant (Section 6.1, 5 tasks including tasks e, and h)

C.3 Information Technology Security TRA and C&A Analyst (Section 6.2, 3 tasks including tasks d and f)

C.7 Information Technology Security Design Specialist (Section 6.3, 6 tasks including tasks e and i)

C.8 Network Security Analyst (Section 6.4, 5 tasks including tasks b and f)

C.9 IT Security Systems Operator (Section 6.5, 3 tasks including tasks c and d)

C.11 Information Technology Security Vulnerability Analysis Specialist (Section 6.6, 3 tasks including tasks a and b)

C.14 Information Technology Security Research & Development Specialist (Section 6.7, 3 tasks including a and c)

C.16 Privacy Impact Assessment Specialist (Section 6.8, 4 tasks including tasks b and f)

(**) Resource category titles will also be considered identical to those in the table above if they:
• Contain acronyms for the long form of a term used within the required resource categories (i.e. IT or IM/IT for Information Technology; VA for Vulnerability Analysis; R&D for Research & Development; PIA for Privacy Impact Assessment) and the remainder otherwise matches;
</td></tr>
</table>

Part #, Article and sub-article of the Present RFP	Substantive Changes
	• Contain long form terms for acronyms within the required resource categories (i.e. Threat & Risk Assessment for TRA; Certification & Accreditation for C&A) and the remainder otherwise matches; • Do not include the TBIPS Category # (i.e. C.1) but the remainder of the title matches identically or as per the considerations above. (***) For the purpose of demonstrating the equivalency of tasks for resources performing work for another country, where Canadian policies, guidelines, etc. are referenced in the Statement of Work tasks for a particular resource category, the Bidder may substitute the applicable country's policy, guideline, etc. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CM2** • The billable days must have been for the delivery of ***Cyber Security*** professional services; • The work billed for a given resource category must include the equivalent associated tasks for resource categories as outlined above. • The Bidder must provide a copy of Contract/Task Authorization documentation to substantiate the details provided.
Attachment 4.1 Mandatory Technical Criteria Section 1.0	(New CM3) The Bidder must demonstrate that they hold one of the following corporate partnerships: • AWS Consulting Partner • Microsoft Partner The Bidder must attach appropriate documentation from Microsoft or AWS demonstrating the described partnership level and current validity
Attachment 4.2 Point-Rated Technical Criteria	(Added) Where a copy of Contract/Task Authorization documentation is required to provide verification of the details provided by the Bidder to demonstrate compliance with a criteria, the following is sufficient: 1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or 2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or 3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.
Attachment 4.2 Point-Rated Technical Criteria Section 2.0	(Deleted) CR1 Renumbered CR2 to CR4 Renumbered CR3 to CR5 Renumbered CR4 to CR6

Part #, Article and sub-article of the Present RFP	Substantive Changes	
	(Deleted) CR5 (Added) CR7	
Attachment 4.2 Point-Rated Technical Criteria Section 2.0 CR1	The Bidder will be awarded up to 20 points for additional contracts meeting all the requirements of mandatory criteria CM2. A contract can be counted only once toward this criteria, and cannot be the same contract used to demonstrate compliance with mandatory criteria CM2. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR1**	10 points for each qualifying contract **Maximum: 20 points**
Attachment 4.2 Point-Rated Technical Criteria Section 2.0 CR2	The Bidder will be awarded up to 25 points for additional concurrent ***Cyber Security*** resources in excess of the five (5) resources under the same contract and during the same 6-consecutive month period used to demonstrate compliance with mandatory criteria CM2. To earn points, all qualifying conditions stated in CM2 must be met by these additional resources. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR2**	Number of resources working concurrently during the 6-month period 5 resources = 0 points 6 resources = 5 points 7 resources = 10 points 8 resources = 15 points 9 resources = 20 points 10 resources = 25 points **Maximum : 25 points**
Attachment 4.2 Point-Rated Technical Criteria Section 2.0 CR3	The Bidder will be awarded up to up to 15 points for the number of resource categories used by resources to demonstrate compliance with mandatory criteria CM2 and rated criteria CR1 and CR2. The resource categories must be from the list provided in CM2. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR3**	Number of resource categories used by resources to demonstrate compliance with CM2, CR1 and CR2: 1 category = 2 points 2 categories = 5 points 3 categories = 8 points 4 categories = 11 points 5 categories = 13 points 6+ categories = 15 points **Maximum 15 points**
Attachment 4.2 Point-Rated Technical Criteria Section 2.0 CR4	The Bidder will be awarded up to 10 points if the client of any of the qualifying contracts used to demonstrate compliance with Corporate Criteria CM1, CM2 or CR1 was the Government of Canada (*) (*) Government of Canada is defined as any Department, Agency or Crown Corporation of the Canadian Federal Government.	Government of Canada contract(s) used for CM1, CM2 or CR1 1-2 = 5 points 3+ = 10 points **Maximum: 10 points**

Part #, Article and sub-article of the Present RFP	Substantive Changes	
	A contract can be counted only once toward this criterion. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR4**	
Attachment 4.2 Point-Rated Technical Criteria Section 2.0 CR5	The Bidder (*) will be awarded up to 20 points if any of the ***Cyber Security*** services provided under qualifying contracts used to demonstrate compliance with Corporate Criteria CM1, CM2, or CR1 involved an ***emerging technology*** (*). Note: To be accepted, the emerging technology must be explicitly identified within the Contract/Task Authorization's Statement of Work. A contract can be counted only once toward this criteria. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR5** **(*) In evaluating corporate experience for this criteria, Canada will consider the corporate experience referred to in:** **Part 3, Section 3.2** **Section I: Technical Bid** **Substantiation of Technical Compliance** **Paragraph C (page 14-15)**	10 points for each contract used to demonstrate compliance with CM1, CM2 or CR1 involving an emerging technology as described in the criteria **Maximum: 20 points**
Attachment 4.2 Point-Rated Technical Criteria Section 2.0 CR6	The Bidder will be awarded additional points for demonstrating the following current and valid corporate partnerships or certification: • Microsoft Silver or Gold Partnership • AWS Partner Network Select, Advanced or Premier The Bidder must attach appropriate documentation demonstrating the described partnership level, or certification, and current validity.	Up to 5 points for each current and valid partnership as follows: • Microsoft Partner Silver or Gold (5 points) • AWS Partner Network, Select, Advanced or Premier (5 points): **Maximum: 10 points**
Attachment 4.2 Point-Rated Technical Criteria Section 2.0 CR7	<u>Talent Management Plan</u> The Bidder should describe the Talent Management Plan it proposes to implement in the resulting Contract. The Plan should describe how the Bidder will: a. Minimize and manage resource turnover; b. Maintain knowledge and expertise related to Canada Border Services Agency's requirements over the life of the resulting Contract both during	5 points for each of the points described below: No demonstration = 0 points 1. Includes processes the Bidder uses to keep its inventory of active resources up-to-date and how

Part #, Article and sub-article of the Present RFP	Substantive Changes	
	and in between Task Authorizations; c. Ensure that resources will stay current with technology changes during the life of the Contract; and d. Ensure that the Bidder is able to propose qualified resources to Canada Border Services Agency within five (5) days of receipt of a request; The Bidder's submission should be relevant to CBSA's requirement and should not exceed 2000 words.	intake and validation of new resources expertise is handled 2. Identifies individuals responsible for maintaining knowledge on CBSA's requirements, frequency of this maintenance, and how that knowledge is shared within the company 3. Describes how the Bidder maintains contact with the client regarding satisfaction with the outcomes or deliverables produced. 4. Describes how the Bidder maintains contact with the resources placed under the contract 5. Includes processes the Bidder uses to ensure they are able to provide alternative qualified individuals with specialized knowledge and expertise in a timely manner 6. Describes how the Bidder ensures resources skills and knowledge relative to the deliverables of the contract will remain current **Maximum: 30 points**
Attachment 4.2 Point-Rated Technical Criteria Section 2.0	Total Points Available 130 Minimum Points Required (~65%) 85	
Forms	Deletions and Additions to forms reflecting modifications made to Attachment 4.1.	
Appendix C to Annex A Section 1.0	(Deleted) Workstream 1 (Deleted) B.1 Business Analyst, Level 2 (Deleted) B.1 Business Analyst, Level 3 (Deleted) Workstream 2 (Heading)	

Part #, Article and sub-article of the Present RFP	Substantive Changes
Appendix C to Annex A Section 1.0 M1.2	Note: The experience required is a combined total, however a minimum of 1 year must be demonstrated for each activity.
Appendix C to Annex A Section 1.0 M2.2	Note: The experience required is a combined total, however a minimum of 1 year must be demonstrated for each activity.
Appendix C to Annex A Section 1.0 M4.1	Note: The experience required is a combined total, however a minimum of 6 months must be demonstrated for each area.
Appendix C to Annex A Section 1.0	(Deleted) C6.1 Information Technology Security Engineer, Level 2 (M5.1 to M5.4) (Deleted) C6.1 Information Technology Security Engineer, Level 3 (M6.1 to M6.4)) Renumbered remaining criteria for resources as follows: C.7 Information Technology Security Design Specialist, Level 2 (M5.x) C.7 Information Technology Security Design Specialist, Level 3 (M6.x) C.8 Network Security Analyst, Level 2 (M7.x) C.8 Network Security Analyst, Level 3 (M8.x) C.9 Information Technology Security Systems Operator, Level 2 (M9.x) C.9 Information Technology Security Systems Operator, Level 3 (M10.x) C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2 (M11.x) C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3 (M12.x) C.14 Information Technology Security R&D Specialist (SME), Level 2 (M13.x) C.14 Information Technology Security R&D Specialist (SME), Level 3 (M14.x) C.16 Privacy Impact Assessment Specialist, Level 2 (M15.x) C.16 Privacy Impact Assessment Specialist, Level 3 (M16.x)
Appendix C to Annex A Section 1.0 M5.1	Note: The experience required is a combined total, however a minimum of one (1) year is required with Software Development & Application Security.
Appendix C to Annex A Section 1.0 M6.1	Note: The experience required is a combined total, however a minimum of two (2) years is required with Software Development & Application Security.
Appendix C to Annex A Section 1.0	The Contractor must demonstrate that the Proposed Resource has eighteen (18) months hands-on experience in the last eight (8) years deploying and supporting network security on outsourced Public Cloud service provider infrastructure.

Part #, Article and sub-article of the Present RFP	Substantive Changes
M7.3	To qualify, a project must have a minimum duration of four (4) months.
Appendix C to Annex A Section 1.0 M8.1	The Contractor must demonstrate that the Proposed Resource has seven (7) years hands-on experience performing all of the following activities : • ***Configuring***[2]and supporting automated IT Security management software; • ***Configuring***[2]and supporting firewalls, routers and load balancers; • Designing and supporting network failover and recovery using infrastructure-as-code; • ***Configuring***[2]and supporting Elastic Computing; • ***Configuring***[2]and supporting Security Groups and Access Control Lists (ACLs) for incoming and outgoing packets; • Designing User Defined Routes (UDRs) to force tunneling; • ***Configuring***[2]and integrating network infrastructures using a hybrid cloud ***configuration***[1] Note: Projects do not require all activities however **all** activities must be demonstrated. To qualify, a project must have a minimum duration of four (4) months.
Appendix C to Annex A Section 1.0 M8.3	The Contractor must demonstrate that the Proposed Resource has three (3) years experience in the last eight (8) years designing, deploying and supporting network security on outsourced ***public cloud*** service provider infrastructure. To qualify, a project must have a minimum duration of four (4) months.
Appendix C to Annex A Section 1.0 M9.1	(*)The experience required is a combined total, however a minimum of eighteen (18) months is required for each.
Appendix C to Annex A Section 1.0 M10.1	(*)The experience required is a combined total, however a minimum of three (3) years is required for each.
Appendix C to Annex A Section 1.0 M13.1	(*)The experience required is a combined total, however a minimum of eighteen (18) months is required with Software Development & Application Security.
Appendix C to Annex A Section 1.0 M13.1	(*)The experience required is a combined total, however a minimum of three (3) years is required with Software Development & Application Security.
Appendix C to Annex A Section 2.0	(Deleted) Workstream 1 (Deleted) B.1 Business Analyst, Level 2 (Deleted) B.1 Business Analyst, Level 3

Part #, Article and sub-article of the Present RFP	Substantive Changes
	(Deleted) Workstream 2 (Heading)
Appendix C to Annex A Section 2.0	(Deleted) C6.1 Information Technology Security Engineer, Level 2 (R5.1 to R5.4) (Deleted) C6.1 Information Technology Security Engineer, Level 3 (R6.1 to R6.4)) Renumbered remaining criteria for resources as follows: C.7 Information Technology Security Design Specialist, Level 2 (R5.x) C.7 Information Technology Security Design Specialist, Level 3 (R6.x) C.8 Network Security Analyst, Level 2 (R7.x) C.8 Network Security Analyst, Level 3 (R8.x) C.9 Information Technology Security Systems Operator, Level 2 (R9.x) C.9 Information Technology Security Systems Operator, Level 3 (R10.x) C.11 Information Technology Security Vulnerability Analysis Specialist, Level 2 (R11.x) C.11 Information Technology Security Vulnerability Analysis Specialist, Level 3 (R12.x) C.14 Information Technology Security R&D Specialist (SME), Level 2 (R13.x) C.14 Information Technology Security R&D Specialist (SME), Level 3 (R14.x) C.16 Privacy Impact Assessment Specialist, Level 2 (R15.x) C.16 Privacy Impact Assessment Specialist, Level 3 (R16.x)

ATTACHMENT 3.1
BID SUBMISSION FORM

BID SUBMISSION FORM		
Bidder's full legal name		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Company Security Officer (CSO) contact information:	Name:	
	Title:	
	Address:	
	Telephone #:	
	Fax #:	
	Email:	
Bidder's Procurement Business Number (PBN) [see the Standard Instructions 2003] **[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*.**]**		
Jurisdiction of Contract: 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)		

Bidder's Proposed Site(s) or Premises Requiring Safeguard Measures. See Part 3 for instructions.	Address of proposed site or premise: _____ City: _____ Province: _____ Postal Code: _____ Country: _____
Former Public Servants 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"
Security Clearance Level of Bidder [include both the level and the date it was granted] **[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*.**]**	
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.	
Signature of Authorized Representative of Bidder	

ATTACHMENT 3.2

ELECTRONIC PAYMENT INSTRUMENTS

The Bidder accepts to be paid by any of the following Electronic Payment Instrument(s):

( ) VISA Acquisition Card;

( ) MasterCard Acquisition Card;

( ) Direct Deposit (Domestic and International);

( ) Electronic Data Interchange (EDI);

( ) Wire Transfer (International Only);

( ) Large Value Transfer System (LVTS) (Over $25M)

ATTACHMENT 4.1

MANDATORY TECHNICAL CRITERIA

NOTE TO BIDDERS: Where indicated by ***bold italics***, those terms are defined within the Glossary.

Where a copy of Contract/Task Authorization documentation is required to provide verification of the details provided by the Bidder to demonstrate compliance with a criteria, the following is sufficient:

1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or
2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or
3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.

1.0 MANDATORY CORPORATE TECHNICAL CRITERIA

Criteria	Mandatory Requirement	Bidder's Response
CM1 (PB)	**Bidder's (*) billable ($) providing IM/IT *Cyber Security* Professional Services involving Public Cloud infrastructure.** The Bidder must provide a maximum of ten (10) reference contracts with a minimum cumulative billed value of $10,000,000.00 CDN (excluding taxes) for IM/IT ***Cyber Security*** Professional Services involving ***Public Cloud*** infrastructure in the last 5 years as of the publication date of this RFP performing or delivering either individually or collectively **ALL** of the following services: a) Performing technical ***Vulnerability Scans*** and ***Penetration testing*** against environments designed to meet any of the following security control profiles: a. Protected B Medium Integrity Medium Availability (PBMM) or higher b. FEDRAMP Moderate or High c. ISO 27001 and ISO 27017 d. NIST SP 800-53 Moderate or High b) Performing ***IT Enterprise Security Risk Assessments***, ***Security Audits***, or ***Security Assessment & Authorization Reviews*** c) Providing technical guidance, support, engineering and research in the development of ***secure*** solutions d) Security Operations: Performing information technology system monitoring, security incident handling, investigations and response To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CM1** • Projects do not have to contain all services, however all services must be demonstrated; • Each project must have been for ***Cyber Security*** professional services involving ***Public Cloud*** infrastructure and at least one	PA

<table>
<tr><th>Criteria</th><th>Mandatory Requirement</th><th>Bidder's Response</th></tr>
<tr><td></td><td>identified service;
• The Bidder must provide a copy of Contract/Task Authorization documentation to substantiate the details provided.

(*) In evaluating corporate experience for this criteria, Canada will consider the corporate experience referred to in:

Part 3, Section 3.2
Section I: Technical Bid
Substantiation of Technical Compliance
Paragraph C (page 14-15)</td><td></td></tr>
<tr><td>CM2</td><td>Bidder’s provision of concurrent IM/IT Cyber Security Professional Services

The Bidder must have been awarded, within the past five (5) years as of the publication date of this RFP, one (1) contract supplying IM/IT Cyber Security professional services where:

• The Bidder provided a minimum of five (5) concurrent resources from any of the resource categories, or equivalent resource categories (*) under different titles, listed in the table below for six (6) consecutive months;
• Each of the resources must have provided IM/IT Cyber Security professional services for a minimum of 90 billable days during the six (6) consecutive month period.

<table>
<tr><th>Resource Category</th></tr>
<tr><td>C.1 Strategic Information Technology Security Planning and Protection Consultant</td></tr>
<tr><td>C.3 Information Technology Security TRA and C&A Analyst</td></tr>
<tr><td>C.7 Information Technology Security Design Specialist</td></tr>
<tr><td>C.8 Network Security Analyst</td></tr>
<tr><td>C.9 Information Technology Security Systems Operator</td></tr>
<tr><td>C.11 Information Technology Security Vulnerability Analysis Specialist</td></tr>
<tr><td>C.14 Information Technology Security Research & Development Specialist</td></tr>
<tr><td>C.16 Privacy Impact Assessment Specialist</td></tr>
</table>

(*) In the case a resource category title in the reference contract is not identical (**) to the resource category in the table above, the Bidder must provide substantiation that the work performed includes the associated tasks (***), excluding Common tasks itemized in Annex A - Statement of Work, for the listed resource category as outlined below:

C.1 Strategic Information Technology Security Planning and Protection Consultant (Section 6.1, 5 tasks including tasks e, and h)

C.3 Information Technology Security TRA and C&A Analyst (Section 6.2, 3 tasks including tasks d and f)

C.7 Information Technology Security Design Specialist (Section 6.3, 6 tasks including tasks e and i)

C.8 Network Security Analyst (Section 6.4, 5 tasks including tasks b and f)

C.9 IT Security Systems Operator (Section 6.5, 3 tasks including tasks c and d)</td><td></td></tr>
</table>

Criteria	Mandatory Requirement	Bidder's Response
	C.11 Information Technology Security Vulnerability Analysis Specialist (Section 6.6, 3 tasks including tasks a and b) C.14 Information Technology Security Research & Development Specialist (Section 6.7, 3 tasks including a and c) C.16 Privacy Impact Assessment Specialist (Section 6.8, 4 tasks including tasks b and f) (**) Resource category titles will also be considered identical to those in the table above if they: • Contain acronyms for the long form of a term used within the required resource categories (i.e. IT or IM/IT for Information Technology; VA for Vulnerability Analysis; R&D for Research & Development; PIA for Privacy Impact Assessment) and the remainder otherwise matches; • Contain long form terms for acronyms within the required resource categories (i.e. Threat & Risk Assessment for TRA; Certification & Accreditation for C&A) and the remainder otherwise matches; • Do not include the TBIPS Category # (i.e. C.1) but the remainder of the title matches identically or as per the considerations above. (***) For the purpose of demonstrating the equivalency of tasks for resources performing work for another country, where Canadian policies, guidelines, etc. are referenced in the Statement of Work tasks for a particular resource category, the Bidder may substitute the applicable country's policy, guideline, etc. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CM2** • The billable days must have been for the delivery of ***Cyber Security*** professional services; • The work billed for a given resource category must include the equivalent associated tasks for resource categories as outlined above. • The Bidder must provide a copy of Contract/Task Authorization documentation to substantiate the details provided.	
CM3	The Bidder must demonstrate that they hold one of the following corporate partnerships: • AWS Consulting Partner • Microsoft Partner The Bidder must attach appropriate documentation from Microsoft or AWS demonstrating the described partnership level and current validity.	

ATTACHMENT 4.2

POINT-RATED TECHNICAL CRITERIA

NOTE TO BIDDERS: Where indicated by ***bold italics***, those terms are defined within the Glossary

Where a copy of Contract/Task Authorization documentation is required to provide verification of the details provided by the Bidder to demonstrate compliance with a criteria, the following is sufficient:

1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or
2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or
3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.

2.0 CORPORATE POINT-RATED TECHNICAL CRITERIA

CR#	Rated Technical Criteria	Points Allocation	Bidder's Response
CR1	The Bidder will be awarded up to 20 points for additional contracts meeting all the requirements of mandatory criteria CM2. A contract can be counted only once toward this criteria, and cannot be the same contract used to demonstrate compliance with mandatory criteria CM2. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR1**	10 points for each qualifying contract **Maximum: 20 points**	
CR2	The Bidder will be awarded up to 25 points for additional concurrent ***Cyber Security*** resources in excess of the five (5) resources under the same contract and during the same 6-consecutive month period used to demonstrate compliance with mandatory criteria CM2. To earn points, all qualifying conditions stated in CM2 must be met by these additional resources. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR2**	Number of resources working concurrently during the 6-month period 5 resources = 0 points 6 resources = 5 points 7 resources = 10 points 8 resources = 15 points 9 resources = 20 points 10 resources = 25 points **Maximum : 25 points**	

CR3	The Bidder will be awarded up to up to 15 points for the number of resource categories used by resources to demonstrate compliance with mandatory criteria CM2 and rated criteria CR1 and CR2. The resource categories must be from the list provided in CM2. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR3**	Number of resource categories used by resources to demonstrate compliance with CM2, CR1 and CR2: 1 category = 2 points 2 categories = 5 points 3 categories = 8 points 4 categories = 11 points 5 categories = 13 points 6+ categories = 15 points **Maximum 15 points**	
CR4	The Bidder will be awarded up to 10 points if the client of any of the qualifying contracts used to demonstrate compliance with Corporate Criteria CM1, CM2 or CR1 was the Government of Canada (*) (*) Government of Canada is defined as any Department, Agency or Crown Corporation of the Canadian Federal Government. A contract can be counted only once toward this criterion. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR4**	Government of Canada contract(s) used for CM1, CM2 or CR1 1-2 = 5 points 3+ = 10 points **Maximum: 10 points**	
CR5	The Bidder (*) will be awarded up to 20 points if any of the ***Cyber Security*** services provided under qualifying contracts used to demonstrate compliance with Corporate Criteria CM1, CM2, or CR1 involved an ***emerging technology*** (*). Note: To be accepted, the emerging technology must be explicitly identified within the Contract/Task Authorization's Statement of Work. A contract can be counted only once toward this criteria. To demonstrate compliance with this criterion, the Bidder must complete and submit **Form CR5** **(*) In evaluating corporate experience for this criteria, Canada will consider the**	10 points for each contract used to demonstrate compliance with CM1, CM2 or CR1 involving an emerging technology as described in the criteria **Maximum: 20 points**	

	corporate experience referred to in: **Part 3, Section 3.2** **Section I: Technical Bid** **Substantiation of Technical Compliance** **Paragraph C (page 14-15)**		
CR6	The Bidder will be awarded additional points for demonstrating the following current and valid corporate partnerships or certification: • Microsoft Silver or Gold Partnership • AWS Partner Network Select, Advanced or Premier The Bidder must attach appropriate documentation demonstrating the described partnership level, or certification, and current validity.	Up to 5 points for each current and valid partnership as follows: • Microsoft Partner Silver or Gold (5 points) • AWS Partner Network, Select, Advanced or Premier (5 points): **Maximum: 10 points**	
CR7	<u>Talent Management Plan</u> The Bidder should describe the Talent Management Plan it proposes to implement in the resulting Contract. The Plan should describe how the Bidder will: a) Minimize and manage resource turnover; b) Maintain knowledge and expertise related to Canada Border Services Agency's requirements over the life of the resulting Contract both during and in between Task Authorizations; c) Ensure that resources will stay current with technology changes during the life of the Contract; and d) Ensure that the Bidder is able to propose qualified resources to Canada Border Services Agency within five (5) days of receipt of a request; The Bidder's submission should be relevant to CBSA's requirement and should not exceed 2000 words.	5 points for each of the points described below: No demonstration = 0 points 1. Includes processes the Bidder uses to keep its inventory of active resources up-to-date and how intake and validation of new resources expertise is handled 2. Identifies individuals responsible for maintaining knowledge on CBSA's requirements, frequency of this maintenance, and how that knowledge is shared within the company 3. Describes how the Bidder maintains contact with the client regarding satisfaction with the outcomes or deliverables produced. 4. Describes how the Bidder maintains contact with the resources placed under the contract 5. Includes processes the Bidder uses to ensure they are able to provide alternative qualified individuals with specialized knowledge and expertise in a timely manner 6. Describes how the Bidder ensures resources skills and knowledge relative to the deliverables of the contract	

		will remain current **Maximum: 30 points**	
Total Points Available			**130**
Minimum Points Required (~65%)			**85**
Bidder score			

ATTACHMENT 4.3

BIDDER'S RESPONSE FORMS TO CORPORATE REQUIREMENTS

CORPORATE MANDATORY REQUIREMENT CM1

Bidder's (*) billable ($) providing IM/IT *Cyber Security* Professional Services involving Public Cloud infrastructure.

The Bidder must provide a maximum of ten (10) reference contracts with a minimum cumulative billed value of $10,000,000.00 CDN (excluding taxes) for IM/IT ***Cyber Security*** Professional Services involving ***Public Cloud*** infrastructure in the last 5 years as of the publication date of this RFP performing or delivering either individually or collectively **ALL** of the following services:

a) Performing technical ***Vulnerability Scans*** and ***Penetration testing*** against environments designed to meet any of the following security control profiles:
   a. Protected B Medium Integrity Medium Availability (PBMM) or higher
   b. FEDRAMP Moderate or High
   c. ISO 27001 and ISO 27017
   d. NIST SP 800-53 Moderate or High

b) Performing ***IT Enterprise Security Risk Assessments***, ***Security Audits***, or ***Security Assessment & Authorization Reviews***

c) Providing technical guidance, support, engineering and research in the development of ***secure*** solutions

d) Security Operations: Performing information technology system monitoring, security incident handling, investigations and response

- Projects do not have to contain all services, however all services must be demonstrated;
- Each project must have been for ***Cyber Security*** professional services involving ***Public Cloud*** infrastructure and at least one identified service;
- The Bidder must provide a copy of Contract/Task Authorization documentation to substantiate the details provided.

(*) In evaluating corporate experience for this criteria, Canada will consider the corporate experience referred to in:

Part 3, Section 3.2
Section I: Technical Bid
Substantiation of Technical Compliance
Paragraph C (page 14-15)

Copy and complete for each Reference Contract

CM1 FORM
A) Contract/Task Authorization (TA) Reference #: _____

B) Client Information (*) (*) The Contact Reference must be an individual who is or was at the time an employee of the client organization who can provide confirmation of all information	
Organization Name	
Contact Reference Name and Title	
Address	
Telephone	
E-mail	

C) Contract / Task Authorization Billed Value (*) (*) Billed value, excluding taxes, for ***Cyber Security*** professional services involving ***Public Cloud*** infrastructure and at least one identified service.	
Contract/TA Billed Value	

D) Project Description	
Project Name	
Project Description: As defined in the Contract/Task Authorization's Statement of Work	
Project Start and End dates If project is ongoing, the solicitation closing date will be used.	
Scope of Cyber Security services delivered: A description of the work undertaken and services delivered that includes how the work meets the criteria	
Identify which of the following services this project demonstrates: ***Public Cloud*** infrastructure and: a) Performing technical ***Vulnerability Scans*** and ***Penetration testing*** against environments designed to meet any of the following security control profiles: a. Protected B Medium Integrity Medium Availability (PBMM) or higher b. FEDRAMP Moderate or High c. ISO 27001 and ISO 27017 d. NIST SP 800-53 Moderate or High b) Performing ***IT Enterprise Security Risk Assessments***, ***Security Audits***, or ***Security Assessment & Authorization Reviews*** c) Providing technical guidance, support, engineering and research in the development of ***secure*** solutions d) Security Operations: Performing information technology system monitoring, security incident handling, investigations and response	

Supporting Documentation

Ensure to include a copy of the Contract/Task Authorization documentation to substantiate the details provided.

The following is sufficient:

1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or
2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or
3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.

CORPORATE MANDATORY REQUIREMENT CM2

Bidder's provision of concurrent IM/IT *Cyber Security* Professional Services

The Bidder must have been awarded, within the past five (5) years as of the publication date of this RFP, one (1) contract supplying IM/IT ***Cyber Security*** professional services where:

- The Bidder provided a minimum of five (5) concurrent resources from any of the resource categories, or equivalent resource categories (*) under different titles, listed in the table below for six (6) consecutive months;
- Each of the resources must have provided IM/IT ***Cyber Security*** professional services for a minimum of 90 billable days during the six (6) consecutive month period.

Resource Category
C.1 Strategic Information Technology Security Planning and Protection Consultant
C.3 Information Technology Security TRA and C&A Analyst
C.7 Information Technology Security Design Specialist
C.8 Network Security Analyst
C.9 Information Technology Security Systems Operator
C.11 Information Technology Security Vulnerability Analysis Specialist
C.14 Information Technology Security Research & Development Specialist
C.16 Privacy Impact Assessment Specialist

(*) In the case a resource category title in the reference contract is not identical (**) to the resource category in the table above, the Bidder must provide substantiation that the work performed includes the associated tasks (***), excluding Common tasks itemized in Annex A - Statement of Work, for the listed resource category as outlined below:

C.1 Strategic Information Technology Security Planning and Protection Consultant (Section 6.1, 5 tasks including tasks e, and h)

C.3 Information Technology Security TRA and C&A Analyst (Section 6.2, 3 tasks including tasks d and f)

C.7 Information Technology Security Design Specialist (Section 6.3, 6 tasks including tasks e and i)

C.8 Network Security Analyst (Section 6.4, 5 tasks including tasks b and f)

C.9 IT Security Systems Operator (Section 6.5, 3 tasks including tasks c and d)

C.11 Information Technology Security Vulnerability Analysis Specialist (Section 6.6, 3 tasks including tasks a and b)

C.14 Information Technology Security Research & Development Specialist (Section 6.7, 3 tasks including a and c)

C.16 Privacy Impact Assessment Specialist (Section 6.8, 4 tasks including tasks b and f)

(**) Resource category titles will also be considered identical to those in the table above if they:

- Contain acronyms for the long form of a term used within the required resource categories (i.e. IT or IM/IT for Information Technology; VA for Vulnerability Analysis; R&D for Research & Development; PIA for Privacy Impact Assessment) and the remainder otherwise matches;
- Contain long form terms for acronyms within the required resource categories (i.e. Threat & Risk Assessment for TRA; Certification & Accreditation for C&A) and the remainder otherwise matches;
- Do not include the TBIPS Category # (i.e. C.1) but the remainder of the title matches identically or as per the considerations above.

(***) For the purpose of demonstrating the equivalency of tasks for resources performing work for another country, where Canadian policies, guidelines, etc. are referenced in the Statement of Work tasks for a particular resource category, the Bidder may substitute the applicable country's policy, guideline, etc.

- The billable days must have been for the delivery of ***Cyber Security*** professional services;
- The work billed for a given resource category must include the equivalent associated tasks for resource categories as outlined above.
- The Bidder must provide a copy of Contract/Task Authorization documentation to substantiate the details provided.

CM2 Form (3 Parts):

PART 1
A) Contract Reference #: _____

B) Client Information (*) (*) The Contact Reference must be an individual who is or was at the time an employee of the client organization who can provide confirmation of all information	
Organization Name	
Contact Reference Name and Title	
Address	
Telephone	
E-mail	

C) Contract Information	
Start Date	
Completion Date	

D) Is/was this a TBIPS Contract? Yes ____ No _____

E) Project Description	
Project Name	
Project Description: As defined in the Contract/Task Authorization's Statement of Work	
Project Start and End dates If project is ongoing, the solicitation closing date will be used.	
Scope of ***Cyber Security*** services delivered A description of the work undertaken and services delivered that includes how the work meets the criteria	

Complete Resources Detail:

PART 2
Contract Reference #: _____

F) 6-Consecutive Month Period to be evaluated	
Start Date	
End Date	

G) Section 1: Resource Information	
Resource #1:	Name
Task Authorization #:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #2:	**Name**
Task Authorization #:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #3:	**Name**
Task Authorization #:	
Resource Category title as worded in Reference Contract:	

Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #4:	**Name**
Task Authorization #:	
Name of Resource:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #5:	**Name**
Task Authorization #:	
Name of Resource:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	

For any of the resources included in Part 2 (G), if their resource category titles within the reference contract are not identical to those listed in the criteria, complete Part 3 to establish resource category equivalency as outlined in Criteria CM2.

Activity/Task Mapping

Select and complete the appropriate section for the resource category(ies) to be mapped.

PART 3
Contract Reference #: _____

Task Authorization(s) Reference #: _____

Resource: _____

C.1 Strategic Information Technology Security Planning and Protection Consultant	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.1: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(e) Conduct feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security	
(h) Review and prioritize IT Security and Information Infrastructure Protection programs	
AND The Bidder must provide substantiation that the work performed includes 3 additional associated tasks listed in Annex A Statement of Work, Section 6.1: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.3 Information Technology Security TRA and C&A Analyst	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.2: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(d) Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings	
(f) Conduct Accreditation activities such as: Review of the certification results in the design review documentation by the Accreditation 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).	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.2: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____ **Resource**: _____	
C.7 Information Technology Security Design Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.3: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(e) 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, API security, incident management, identity management).	
(i) Provide security architecture design and engineering support.	
AND The Bidder must provide substantiation that the work performed includes 4 additional associated tasks listed in Annex A Statement of Work, Section 6.3: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.8 Network Security Analyst	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.4: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(b) Analyze security data and provide advisories and reports	
(f) Identify and analyze technical threats to, and vulnerabilities of, networks	
AND The Bidder must provide substantiation that the work performed includes 3 additional associated tasks listed in Annex A Statement of Work, Section 6.4: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.9 Information Technology Security Systems Operator	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.5: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(c) Configure IT Security management	

(d) Configure intrusion detection systems, firewalls and content checkers, extracting and analyzing reports and logs, and responding to security incidents	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.5: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.11 Information Technology Security Vulnerability Analysis Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.6: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(a) 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 TLS, HTTPS, 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	
(b) Identify threats to, and technical vulnerabilities of, networks	

AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.6: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.14 Information Technology Security Research and Development Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.7: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(a) Review, analyze, and/or apply: • Universities and industrial IT Security R and D capabilities • Directory Standards such as X.400, X.500, and SMTP • Networking Protocols such as HTTP, FTP, Telnet • Internet security protocols such as TLS, HTTPS, S-MIME, IPSec, SSH • Wireless Security, Bluetooth standards • TCP/IP, UDP, DNS, SMTP, SNMP standards and protocols • Intrusion detection systems, firewalls and content checkers; • Cryptographic Algorithms • Security best practices	
(c) Design and develop prototypes, proof-of-concept models and trials including security functionality and emerging technologies	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.7: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.16 Privacy Impact Assessment Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.8: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(b) 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	
(f) Develop recommendations as to possible privacy risk mitigation strategies	
AND The Bidder must provide substantiation that the work performed includes 2 additional associated tasks listed in Annex A Statement of Work, Section 6.8: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Supporting Documentation

Ensure to include a copy of the Contract/Task Authorization documentation to substantiate the details provided

The following is sufficient:

1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or
2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or
3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.

CORPORATE RATED REQUIREMENT CR1

The Bidder will be awarded up to 20 points for additional contracts meeting all the requirements of mandatory criteria CM2.

A contract can be counted only once toward this criteria, and cannot be the same contract used to demonstrate compliance with mandatory criteria CM2.

10 points for each qualifying contract

Maximum: 20 points

CR1 Form

Copy and complete Parts 1, 2 and 3 (if applicable) for each additional qualifying Reference Contract

PART 1
A) Contract/Task Authorization Reference #: _____

B) Client Information (*) (*) The Contact Reference must be an individual who is or was at the time an employee of the client organization who can provide confirmation of all information	
Organization Name	
Contact Reference Name and Title	
Address	
Telephone	
E-mail	

C) Contract / Task Authorization Information	
Start Date	
Completion Date	

D) Is/was this a TBIPS Contract? Yes ____ No _____

E) Project Description	
Project Name	

Project Description: As defined in the Contract/Task Authorization's Statement of Work	
Project Start and End dates If project is ongoing, the solicitation closing date will be used.	
Scope of ***Cyber Security*** services delivered A description of the work undertaken and services delivered that includes how the work meets the criteria	

Complete Resources Detail:

PART 2
Contract Reference #: _____

F) 6-Consecutive Month Period to be evaluated	
Start Date	
End Date	

G) Section 1: Resource Information	
Resource #1:	Name
Task Authorization #:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #2:	Name
Task Authorization #:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	

No. of billable days within subject period (minimum 90 days)	
Resource #3:	Name
Task Authorization #:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #4:	Name
Task Authorization #:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #5:	Name
Task Authorization #:	
Resource Category title as worded in Reference Contract:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	

For any of the resources included in Part 2 (G), if their resource category titles within the reference contract are not identical to those listed in Criteria CM2, complete Part 3 to establish resource category equivalency as outlined in Criteria CM2.

Activity/Task Mapping

Select and complete the appropriate section for the resource category(ies) to be mapped.

PART 3
Contract Reference #: _____

Task Authorization Reference #: _____ **Resource(s)**: _____	
C.1 Strategic Information Technology Security Planning and Protection Consultant	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.1: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(e) Conduct feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security	
(h) Review and prioritize IT Security and Information Infrastructure Protection programs	
AND The Bidder must provide substantiation that the work performed includes 3 additional associated tasks listed in Annex A Statement of Work, Section 6.1: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____ **Resource(s)**: _____	
C.3 Information Technology Security TRA and C&A Analyst	
Equivalent Resource Category as worded in Reference Contract to be mapped	

The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.2: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(d) Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings	
(f) Conduct Accreditation activities such as: Review of the certification results in the design review documentation by the Accreditation 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).	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.2: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource(s): _____

C.7 Information Technology Security Design Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.3: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(e) 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, API security, incident management, identity management).	
(i) Provide security architecture design and engineering support.	

AND The Bidder must provide substantiation that the work performed includes 4 additional associated tasks listed in Annex A Statement of Work, Section 6.3: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.8 Network Security Analyst	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.4: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(b) Analyze security data and provide advisories and reports	
(f) Identify and analyze technical threats to, and vulnerabilities of, networks	
AND The Bidder must provide substantiation that the work performed includes 3 additional associated tasks listed in Annex A Statement of Work, Section 6.4: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____ **Resource**: _____	
C.9 Information Technology Security Systems Operator	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.5: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(c) Configure IT Security management	
(d) Configure intrusion detection systems, firewalls and content checkers, extracting and analyzing reports and logs, and responding to security incidents	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.5: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____ **Resource**: _____	
C.11 Information Technology Security Vulnerability Analysis Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	

The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.6: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(a) 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 TLS, HTTPS, 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	
(b) Identify threats to, and technical vulnerabilities of, networks	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.6: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource(s): _____

C.14 Information Technology Security Research and Development Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	

The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.7: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(a) Review, analyze, and/or apply: • Universities and industrial IT Security R and D capabilities • Directory Standards such as X.400, X.500, and SMTP • Networking Protocols such as HTTP, FTP, Telnet • Internet security protocols such as TLS, HTTPS, S-MIME, IPSec, SSH • Wireless Security, Bluetooth standards • TCP/IP, UDP, DNS, SMTP, SNMP standards and protocols • Intrusion detection systems, firewalls and content checkers; • Cryptographic Algorithms • Security best practices	
(c) Design and develop prototypes, proof-of-concept models and trials including security functionality and emerging technologies	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.7: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource(s): _____

C.16 Privacy Impact Assessment Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	

The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.8: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(b) 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	
(f) Develop recommendations as to possible privacy risk mitigation strategies	
AND The Bidder must provide substantiation that the work performed includes 2 additional associated tasks listed in Annex A Statement of Work, Section 6.8: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Supporting Documentation

Ensure to include a copy of the Contract/Task Authorization documentation to substantiate the details provided

The following is sufficient:

1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or
2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or
3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.

CORPORATE RATED REQUIREMENT CR2

The Bidder will be awarded up to 25 points for additional concurrent ***Cyber Security*** resources in excess of the five (5) resources under the same contract and during the same 6-consecutive month period used to demonstrate compliance with mandatory criteria CM2.

To earn points, all qualifying conditions stated in CM2 must be met by these additional resources.

Number of resources working concurrently during the 6-month period

5 resources = 0 points
6 resources = 5 points
7 resources = 10 points
8 resources = 15 points
9 resources = 20 points
10 resources = 25 points

Maximum : 25 points

CR2 Form (3 Parts):

PART 1
A) Contract Reference used to demonstrate compliance with Mandatory Criteria CM2#: _____

B) Project Description	
Project Name	
Project Description: As defined in the Contract/Task Authorization's Statement of Work	
Project Start and End dates If project is ongoing, the solicitation closing date will be used.	
Scope of ***Cyber Security*** services delivered A description of the work undertaken and services delivered that includes how the work meets the criteria	

Complete Resources Detail:

PART 2

C) 6-Consecutive Month Period used to demonstrate compliance with Mandatory Criteria CM2	
Start Date	

End Date	

D) Section 1: Additional Resources Information	
Resource #6:	Name
Task Authorization #:	
Resource Category title as worded in Reference Contract/TA:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #7:	**Name**
Task Authorization #:	
Resource Category title as worded in Reference Contract/TA:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #8:	**Name**
Task Authorization #:	
Resource Category title as worded in Reference Contract/TA:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #9:	**Name**
Task Authorization #:	
Name of Resource:	
Resource Category title as worded in Reference Contract/TA:	

Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	
Resource #10:	**Name**
Task Authorization #:	
Name of Resource:	
Resource Category title as worded in Reference Contract/TA:	
Resource Category title as worded in Criteria CM2 (if not identical to resource category title as worded in the reference contract, complete an activity task mapping in Part 3 for the appropriate resource category and include with your submission).	
No. of billable days within subject period (minimum 90 days)	

For any of the resources included in Part 2 (D), if their resource category titles within the reference contract are not identical to those listed in the criteria, complete Part 3 to establish resource category equivalency as outlined in Criteria CM2.

Activity/Task Mapping

Select and complete the appropriate section for the resource category(ies) to be mapped.

PART 3
Contract Reference #: _____ **Resource(s)**: _____

Task Authorization Reference #: _____ **Resource**: _____	
C.1 Strategic Information Technology Security Planning and Protection Consultant	
Equivalent Resource Category as worded in Reference Contract to be mapped	

The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.1: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(e) Conduct feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security	
(h) Review and prioritize IT Security and Information Infrastructure Protection programs	
AND The Bidder must provide substantiation that the work performed includes 3 additional associated tasks listed in Annex A Statement of Work, Section 6.1: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.3 Information Technology Security TRA and C&A Analyst	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.2: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(d) Develop reports such as: Data security analysis, Concepts of operation, Statements of Sensitivity (SoSs), Threat assessments, Privacy Impact Assessments (PIAs), Non-technical Vulnerability Assessments, Risk assessments, IT Security threat, vulnerability and/or risk briefings	

(f) Conduct Accreditation activities such as: Review of the certification results in the design review documentation by the Accreditation 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).	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.2: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.7 Information Technology Security Design Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.3: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(e) 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, API security, incident management, identity management).	
(i) Provide security architecture design and engineering support.	
AND The Bidder must provide substantiation that the work performed includes 4 additional associated tasks listed in Annex A Statement of Work, Section 6.3: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____ **Resource**: _____	
C.8 Network Security Analyst	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.4: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(b) Analyze security data and provide advisories and reports	
(f) Identify and analyze technical threats to, and vulnerabilities of, networks	
AND The Bidder must provide substantiation that the work performed includes 3 additional associated tasks listed in Annex A Statement of Work, Section 6.4: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____ **Resource: _____**	
C.9 Information Technology Security Systems Operator	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.5: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(c) Configure IT Security management	

(d) Configure intrusion detection systems, firewalls and content checkers, extracting and analyzing reports and logs, and responding to security incidents	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.5: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource: _____

C.11 Information Technology Security Vulnerability Analysis Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.6: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task as described in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(a) 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 TLS, HTTPS, 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	
(b) Identify threats to, and technical vulnerabilities of, networks	

AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.6: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____

Resource(s): _____

C.14 Information Technology Security Research and Development Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.7: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(a) Review, analyze, and/or apply: • Universities and industrial IT Security R and D capabilities • Directory Standards such as X.400, X.500, and SMTP • Networking Protocols such as HTTP, FTP, Telnet • Internet security protocols such as TLS, HTTPS, S-MIME, IPSec, SSH • Wireless Security, Bluetooth standards • TCP/IP, UDP, DNS, SMTP, SNMP standards and protocols • Intrusion detection systems, firewalls and content checkers; • Cryptographic Algorithms • Security best practices	
(c) Design and develop prototypes, proof-of-concept models and trials including security functionality and emerging technologies	
AND The Bidder must provide substantiation that the work performed includes 1 additional associated task listed in Annex A Statement of Work, Section 6.7: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Task Authorization Reference #: _____ **Resource(s)**: _____	
C.16 Privacy Impact Assessment Specialist	
Equivalent Resource Category as worded in Reference Contract to be mapped	
The Bidder must provide substantiation that the work performed includes the following associated tasks listed in Annex A Statement of Work, Section 6.8: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	
Activity/Task in Annex A: Statement of Work for the Resource Category in Criteria CM2	**Task performed under the reference contract, including substantiation**
(b) 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	
(f) Develop recommendations as to possible privacy risk mitigation strategies	
AND The Bidder must provide substantiation that the work performed includes 2 additional associated tasks listed in Annex A Statement of Work, Section 6.8: **The substantiation must not simply be a repetition of the tasks, but must explain responsibilities and demonstrate how the Bidder carried out the work while performing the tasks.**	

Supporting Documentation

Ensure to include a copy of any additional Contract/Task Authorization documentation to substantiate the details provided above.

The following is sufficient:

1. Contract including Statement of Work, excluding Annexes, attachments, forms and other appendices that are not necessary to substantiate the information provided; or
2. Contract including Statement of Work as #1 above, with confidential details redacted, so long as adequate detail remains to substantiate the information required to demonstrate compliance with the criteria; or
3. Client signature, electronic or wet, (at Director level or above) including name, title and contact information on the associated Form validating all the information provided within the form. Details included must fully substantiate the criteria.

CORPORATE RATED REQUIREMENT CR3

The Bidder will be awarded up to up to 15 points for the number of resource categories used by resources to demonstrate compliance with mandatory criteria CM2 and rated criteria CR1 and CR2.

The resource categories must be from the list provided in CM2.

Number of resource categories used by resources to demonstrate compliance with CM2, CR1 and CR2:

1 category = 2 points
2 categories = 5 points
3 categories = 8 points
4 categories = 11 points
5 categories = 13 points
6+ categories = 15 points

Maximum 15 points

Form CR3:

Resource Category	Reference Contract/TA#	Criteria X-Reference
C.1 Strategic Information Technology Security Planning and Protection Consultant		
C.3 Information Technology Security TRA and C&A Analyst		
C.7 Information Technology Security Design Specialist		
C.8 Network Security Analyst		
C.9 Information Technology Security Systems Operator		
C.11 Information Technology Security Vulnerability Analysis Specialist		
C.14 Information Technology Security Research & Development Specialist		
C.16 Privacy Impact Assessment Specialist		
# Resource Categories Used		

CORPORATE RATED REQUIREMENT CR4

The Bidder will be awarded up to 10 points if the client of any of the qualifying contracts used to demonstrate compliance with Corporate Criteria CM1, CM2 or CR1 was the Government of Canada (*).

(*) Government of Canada is defined as any Department, Agency or Crown Corporation of the Canadian Federal Government.

A contract can be counted only once toward this criterion.

Government of Canada contract(s) used for CM1, CM2 or CR1:
1-2 = 5 points
3+ = 10 points

Maximum 10 points

Form CR4:

	Contract Reference # used in CM1, CM2 or CR1	**Government of Canada Client Organization**
1		
2		
3		
4		
5		
6		

CORPORATE RATED REQUIREMENT CR5

The Bidder (*) will be awarded up to 20 points if any of the ***Cyber Security*** services provided under qualifying contracts used to demonstrate compliance with Corporate Criteria CM1, CM2 or CR1 involved an ***emerging technology***.

Note: To be accepted, the emerging technology must be explicitly identified within the Contract/Task Authorization's Statement of Work.

A contract can be counted only once toward this criteria.

10 points for each contract used to demonstrate compliance with CM1, CM2 or CR1 involving an emerging technology as described in the criteria.

Maximum: 20 points

(*) In evaluating corporate experience for this criteria, Canada will consider the corporate experience referred to in:

Part 3, Section 3.2
Section I: Technical Bid
Substantiation of Technical Compliance
Paragraph C (page 14-15)

Form CR5:

Contract Reference # used in CM1, CM2 or CR1	
Explanation why this Contract meets the criteria:	

Contract Reference # used in CM1, CM2 or CR1	
Explanation why this Contract meets the criteria:	

ATTACHMENT 4.4

PRICING SCHEDULE

The Bidder must complete this pricing schedule and include it in its financial bid.

The volumetric data included in this pricing schedule are provided for bid evaluated price determination purposes only. They are not to be considered as a contractual guarantee. Their inclusion in this pricing schedule does not represent a commitment by Canada that Canada's future usage of the services described in the bid solicitation will be consistent with this data.

PRICING SCHEDULE TABLE

		Initial Contract Period (1) (Date of Contract award for 1 year)			**Contract Period (2) Option 1 : Starts after Period 1 for 1 year**			**Contract Period (3) Option 2 : Starts after Period 2 for 1 year**		
		A	**B**	**C = A * B**	**D**	**E**	**F = D * E**	**G**	**H**	**I = G * H**
Resouce Category	**Level**	**Estimated number of days**	**firm per-diem rate *(bidder to insert)***	**Total Cost Contract Period (1)**	**Estimated number of days**	**firm per-diem rate *(bidder to insert)***	**Total Cost Contract Period (2)**	**Estimated number of days**	**firm per-diem rate *(bidder to insert)***	**Total Cost Contract Period (3)**
C.1 Strategic Information Technology Security Planning & Protection Consultant	2	240			240			60		
C.1 Strategic Information Technology Security Planning & Protection Consultant	3	240			240			60		
C.3 Information Technology Security TRA and C&A Analyst	2	240			240			108		
C.3 Information Technology Security TRA and C&A Analyst	3	360			360			108		
C.7 Information Technology Security Design Specialist	2	480			480			240		
C.7 Information Technology Security Design Specialist	3	480			480			240		
C.8 Network Security Analyst	2	480			240			240		
C.8 Network Security Analyst	3	240			240			240		
C.9 Information Technology Security Systems Operator	2	480			480			480		
C.9 Information Technology Security Systems Operator	3	240			240			240		
C.11 Information Technology Security Vulnerability Analysis Specialist	2	240			240			120		
C.11 Information Technology Security Vulnerability Analysis Specialist	3	240			240			120		
C.14 Information Technology Security R&D Specialist (SME)	2	720			720			720		
C.14 Information Technology Security R&D Specialist (SME)	3	720			720			720		
C.16 Privacy Impact Assessment Specialist	2	120			120			60		
C.16 Privacy Impact Assessment Specialist	3	120			120			60		
TOTAL COST FOR INFORMATION PURPOSES ONLY See Part 4, section 4.3 a)		**TOTAL COST Contract Period (1)**			**TOTAL COST Contract Period (2)**			**TOTAL COST Contract Period (3)**		
		TOTAL COST = Contract Period (1) + Contract Period (2) + Contract Period (3)								

ATTACHMENT 5.1

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY - CERTIFICATION

Remark to Contracting Authority: *Insert the following certification for requirements issued on behalf of a Department or Agency subject to the FCP, estimated at $1,000,000* ***and above****, Applicable Taxes included: (consult Annex 5.1 of the Supply Manual)(See also Part 5 – Certifications and Additional Information and Part 7 - Resulting Contract Clauses)*

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).