BID SOLICITATION
TASK-BASED INFORMATICS AND PROFESSIONAL SERVICES (TBIPS)
FOR
SHARED SERVICES CANADA

VARIOUS LEVEL 3 RESOURCES FOR CYBER AND IT SECURITY:

TABLE OF CONTENTS

List of Annexes to the Resulting Contract:

List of Attachments to the Request for Proposal:

List of Suppliers Invited to Bid on this Requirement:
ALL Qualified

BID SOLICITATION
TASK-BASED INFORMATICS AND PROFESSIONAL SERVICES (TBIPS)
FOR
SHARED SERVICES CANADA

VARIOUS LEVEL 3 RESOURCES FOR CYBER AND IT SECURITY:

PART 1 - GENERAL INFORMATION

1.1 INTRODUCTION

The document states terms and conditions that apply to bid solicitation #13-18801-0/A. 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 and states that the Bidder agrees to be bound by the clauses and conditions contained in all parts of 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 Security, Financial and Other Requirements: includes specific requirements that must be addressed by bidders; and

Part 6 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 and the Security Requirements Checklist.

1.2 SUMMARY

This bid solicitation is being issued to satisfy the requirement of Shared Services Canada (SSC) for Task-Based Informatics Professional Services (TBIPS) under the TBIPS Supply Arrangement (SA) method of supply. The resulting contract will be used by SSC, an organization with a mandate to provide shared services. The Contract will be used by SSC to provide shared services to its clients, which include SSC itself, those government institutions for whom SSC's services are mandatory at any point during the Contract period, and those other organizations for whom SSC's services are optional at any point in the Contract period and that choose to use those services from time to time. SSC may choose to use this Contract for some or all of its clients and may use alternative means to provide the same or similar services.

It is intended to result in the award of a maximum of **four** contract(s) for one year plus two one-year irrevocable option allowing Canada to extend the term of the contract.

There is a security requirement associated with this requirement. For additional information, see Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. Bidders should consult the "Security Requirements on PWGSC Bid Solicitations - Instructions for Bidders" document on the Departmental Standard Procurement Documents (http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html) website.

Only selected TBIPS SA Holders currently holding a TBIPS SA for Tier 2 in the National Capital Region under the EN578-055605/E series of Supply Arrangements (SAs) are invited to compete. The TBIPS Supply Arrangement EN578-055605/E 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.

The following Category of Personnel are required on an "as and when requested" basis in accordance with Annex "B" of the TBIPS SA:

TBIPS ID	CATEGORY OF PERSONNEL	LEVEL OF EXPERTISE	TOTAL ESTIMATED # OF RESOURCES REQUIRED (PER YEAR)
BUSINESS SYSTEMS CLASS			
B1	Business Analyst	3	10
CYBER PROTECTION SERVICES CLASS			
C1	IT Security Planning and Protection Specialist	3	8
C3	IT TRA & C&A Specialist	3	16
C7	IT Security Design Specialist	3	30
C11	IT Security VA Specialist	3	4
C16	IT Privacy Specialist	3	4

The Contractor must obtain from its employee(s) or subcontractor(s) the completed and signed non-disclosure agreement, and provide it to the Technical Authority before they are given access to information by or on behalf of Canada in connection with the Work.

On July 12, 2012, the Government of Canada invoked the National Security Exception under Canada's domestic and international trade agreements in respect of procurements related to email, networks and data centres for Shared Services Canada. As a result, this requirement is subject to the National Security Exception and, as a result, none of the trade agreements apply to this procurement.

1.3 DEBRIEFINGS

After contract award, bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 10 working days of receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

1.4 CONFLICT OF INTEREST – UNFAIR ADVANTAGE

In order to protect the integrity of the procurement process, bidders are advised that Canada may reject a bid in the following circumstances:

a. if the Bidder, any of its subcontractors, any of their respective employees or former employees was involved in any manner in the preparation of the bid solicitation or in any situation of conflict of interest or appearance of conflict of interest;

b. if the Bidder, any of its subcontractors, any of their respective employees or former employees had access to information related to the bid solicitation that was not available to other bidders and that would, in Canada's opinion, give or appear to give the Bidder an unfair advantage.

The experience acquired by a bidder who is providing or has provided the goods and services described in the bid solicitation (or similar goods or services) will not, in itself, be considered by Canada as conferring an unfair advantage or creating a conflict of interest. This bidder remains however subject to the criteria established above.

Where Canada intends to reject a bid under this section, the Contracting Authority will inform the Bidder and provide the Bidder an opportunity to make representations before making a final decision. Bidders who are in doubt about a particular situation should contact the Contracting Authority before bid closing. By submitting a bid, the Bidder represents that it does not consider itself to be in conflict of interest nor to have an unfair advantage. The Bidder acknowledges that it is within Canada's sole discretion to determine whether a conflict of interest, unfair advantage or an appearance of conflict of interest or unfair advantage exists.

PART 2 - BIDDER INSTRUCTIONS

2.1 STANDARD INSTRUCTIONS, CLAUSES AND CONDITIONS

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 (PWGSC).

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.

The 2003 (2014-03-01) 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.

Wherever the terms "Public Works and Government Services Canada" or "PWGSC" are used in the 2003, substitute "Shared Services Canada";

Subsection 5.4 of Standard Instructions - Goods or Services - Competitive Requirements 2003 is amended as follows:

Delete: sixty (60) days
Insert: 180 days

The text under subsections 4 and 5 of Section 01 – Code of Conduct and Certifications of 2003 referenced above is replaced by:

4. Bidders who are incorporated or who are a sole proprietorship, including those bidding as a joint venture, have already provided a list of names of all individuals who are directors of the Bidder, or the name of the owner, at the time of submitting an arrangement under the Request for Supply Arrangement (RFSA). These bidders must diligently maintain this list up-to-date by informing Canada in writing of any change occuring during the validity period of the bid as well as during the period of any contract arising from this bid solicitation.

5. Canada may, at any time, request that a Bidder provide properly completed and Signed Consent Forms *(Consent to a Criminal Record Verification form - PWGSC-TPSGC 229)* for any or all individuals aforementioned list within a specified time period. Failure to provide such Consent Forms within the time period provided will result in the bid being declared non-responsive.

2.2 SUBMISSION OF BIDS

Bids must be addressed to the Contracting Authority and the location indicated on page 1 of the RFP. A cancellation date stamp, a courier bill of lading or a date stamped label from a Delivery Company must indicate that the Bid was received on or before the closing date and time. Delivery Company means an incorporated courier company, Canada Post Corporation, or a national equivalent of a foreign country. The Contracting Authority will have the right to ask for information to verify that the Bid was received by the Delivery Company on or before the closing date and time. Failure to comply with this request will render the Bid non-responsive.

Postage meter imprints, whether imprinted by the Respondent or the Delivery Company are not acceptable as proof of timely mailing.

Due to the nature of the RFP, responses transmitted by facsimile or e-mail to Shared Services Canada will not be accepted.

Bidders are requested to send an e-mail notification to gary..r.cooper@ssc-spc.gc.ca

2.3 FORMER PUBLIC SERVANT

a. **Information Required**

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 with FPS, bidders must provide the information required below before contract award.

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:

an individual;

an individual who has incorporated;

a partnership made of former public servants; or

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 FPS in receipt of a pension, as applicable:

name of former public servant;

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 web sites 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:

name of former public servant;

conditions of the lump sum payment incentive;

date of termination of employment;

amount of lump sum payment;

rate of pay on which lump sum payment is based;

period of lump sum payment including start date, end date and number of weeks;

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.

2.4 ENQUIRIES – BID SOLICITATION

All enquiries must be submitted in writing to the Contracting Authority no later than fourteen (14) calendar days before the bid closing date. Enquiries received after that time may not be answered.

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 questions or may request that the Bidder do so, so that the proprietary nature of the question 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.

2.5 APPLICABLE LAWS

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

A bidder may, at its 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.

PART 3- BID PREPARATION INSTRUCTIONS

3.1 BID PREPARATION INSTRUCTIONS

a) Copies of Bid: Unless the RFP specifies otherwise, Canada requests that bidders provide their bid in separately bound sections as follows:

(i) Section I: Technical Bid (2 hard copies and 1 soft copy) – soft copy on USB Drive in MS Office Word Compatible Format.

(ii) Section II: Financial Bid (1 hard copy and 1 soft copy) – soft copy on USB Drive in MS Office Word Compatible Format.

(iii) Section III: Certifications (1 hard copy).

If there is a discrepancy between the wording of the soft copy and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy**.** Prices must appear in the financial bid only. Prices must not be indicated in any other section of the bid.

b) Format of Bid: Canada requests that bidders follow the format instructions described below in the preparation of their bid:

(iv) use 8.5 x 11 inch (216 mm x 279 mm) paper;

(v) use a numbering system that corresponds to the bid solicitation;

(vi) 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

(vii) include a table of contents.

c) **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. The Policy on Green Procurement which can be found at:http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html

To assist Canada in reaching its objectives, bidders are encouraged to:

(viii) use paper containing fibre certified as originating from a sustainably-managed forest and/or containing minimum 30% recycled content; and

(ix) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

d) **Submission of Only One Bid from a Bidding Group**:

i. The submission of more than one bid from members of the same bidding group is not permitted in response to this bid solicitation. If members of a bidding group participate in more than one bid, Canada will set aside all bids received from members of that bidding group.

ii. For the purposes of this article, "**bidding group**" means all entities (whether those entities include one or more natural persons, corporations, partnerships, limited liability partnerships, etc.) that are related to one another. Regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law, entities are considered "**related**" for the purposes of this bid solicitation 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.

b. **Joint Venture Experience**:
Except where expressly provided otherwise, at least one member of a joint venture Bidder must meet any given mandatory requirement of this bid solicitation. Joint venture members cannot pool their abilities to satisfy any single mandatory requirement of this bid solicitation. Wherever substantiation of a mandatory requirement is required, the Bidder is requested to indicate which joint venture member satisfies the requirement. 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 solicitation period.

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 services, 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 requirement, 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.

3.2 SECTION I: TECHNICAL BID

The technical bid consists of the following:

(i) Bid Submission Form: Bidders are requested to include the Bid Submission Form - Attachment 1 to Part 3 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, the Bidder's Procurement Business Number, the Bidder's status under the Federal Contractors Program for Employment Equity, 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: The technical bid must substantiate the compliance with the specific articles of Attachment 1 to Part 4, 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 meets the requirements and will carry out the required Work. Simply stating that the Bidder complies 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 "Reference to additional documentation within the bid" columns of Attachment 1 to Part 4, where bidders are requested to indicate where in their bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

(iii) Customer Reference Contact Information: The Bidder must provide customer references who must each confirm, the facts identified in the Bidder's bid. 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. Bidders are also requested to include the title of the contact person. If the named individual is unavailable when required during the evaluation period, the Bidder may provide the name and contact information of an alternate contact from the same customer.

3.3 SECTION II: FINANCIAL BID

a) Pricing: Bidders must submit their financial bid in accordance with Attachment 2 to Part 4. The total amount of Goods and Services Tax or Harmonized Sales Tax must be shown separately, if applicable. All prices must be firm prices.

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 2% 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) 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 years. 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.

d) Blank Prices: Bidders are requested to insert "$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, $0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is $0.00 will be declared non-responsive.

3.4 SECTION III: CERTIFICATIONS

Bidders must submit the certifications required under Part 5of this bid solicitation.

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 SSC will evaluate the bids on behalf of Canada. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

c) In addition to any other time periods established in the bid solicitation:

(i) **Requests for Clarifications**: If Canada seeks clarification or verification from the Bidder about its bid, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.

(ii) **Extension of Time**: If additional time is required by the Bidder, the Contracting Authority may grant an extension in his or her sole discretion.

d) For the resource proposed, the Bidder must include an up to date resume.

4.2 TECHNICAL EVALUATION

a) Mandatory Corporate Criteria: Each bid will be reviewed to determine whether it meets the mandatory requirement of the bid solicitation. All elements of the bid solicitation that are mandatory requirements are identified specifically with the words “must” or “mandatory”. Bids that do not comply with each and every mandatory requirement will be considered non-responsive and be disqualified. The mandatory evaluation criteria are described in Attachment 1 to Part 4 of the RFP.

b) Point-Rated Technical Criteria: 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. Bids that do not obtain the required global pass mark of 70% points for the point-rated technical criteria specified in this bid solicitation will be considered non-responsive and be disqualified. The rated evaluation criteria are described in Attachment 1 to Part 4 of the RFP.

c) Resource Evaluation

Resources will only be assessed after contract award once specific tasks are requested of the Contractor. After contract award, the Task Solicitation process, outlined in Part 6 of the RFP, will be used for each requirement raised under the Contract. When a Task Solicitation (TS) form is issued, the Contractor will be requested to propose resource(s) to satisfy the specific requirement based on the TS form’s Statement of The proposed resource(s) will then be assessed against the mandatory and rated requirements identified in the Contract’s Statement of Work.

d) Reference Checks: If reference checks are conducted by Canada, they will be conducted in writing by e-mail (unless the contact at the reference is only available by telephone). Canada will send all e-mail reference check requests to contacts supplied by all the Bidders on the same day. Canada will not award any points unless the response is received within 5 working days. 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. Points will only be allocated if the reference customer is an outside client of the Bidder itself and not that of an affiliate (for example, the outside client cannot be the

customer of an affiliate of the Bidder). Points will not be allocated if the outside client is itself an affiliate or other entity that does not deal at arm's length with the Bidder. Crown references will be accepted.

4.3 FINANCIAL EVALUATION

Financial Evaluation: The financial evaluation will be conducted using the firm per diem rates provided by the technically responsive bid(s) to calculate the Total Financial Score. "**ANNEX B" Basis of Payment**

(a) There are two financial evaluation methods possible for this requirement. Method 1 will be used if 3 or more bids are determined to be technically responsive (see Method 1 (b) below), and Method 2 will be used if fewer than 3 bids are determined to be technically responsive (see Method 2 (c) below).

(b) **Method 1:** The following financial evaluation method will be used if 3 or more bids are determined to be technically responsive:

(i) **STEP 1 - ESTABLISHING THE LOWER AND UPPER MEDIAN BANDS FOR EACH PERIOD AND EACH CATEGORY OF PERSONNEL**: The Contracting Authority will establish, for each period and each Category of Personnel, the median band limits based on the firm per diem rates proposed by the technically responsive bids. For each period and each Category of Personnel, the median will be calculated using the median function in Microsoft Excel and will represent a range that encompasses the lower median rate to a value of minus (-) 10% of the median, and an upper median rate to a value of plus (+) 25% of the median.

(ii) **STEP 2 - POINT ALLOCATION**: Points will be allocated for each period and each Category of Personnel as follows:

(A) If a firm per diem rate for any given period and Category of Personnel is either lower than the established lower median band limit or higher than the established upper median band limit for that period and Category of Personnel, the Bidder who proposed such rate will be allocated 0 points for that period and Category of Personnel.

(B) If a firm per diem rate for any given period and Category of Personnel is within the established upper and lower median band limits for that period and Category of Personnel, the Bidder who proposed such rate will obtain points for that period and Category of Personnel based on the following calculation, which will be rounded to two decimal places:

$$\frac{\text{Lowest proposed firm per diem rate within the median band limits}}{\text{Bidder's proposed firm per diem rate}} \times \text{Points Assigned (see Table 1)}$$

(C) If a firm per diem rate for any given period and Category of Personnel is within the established median band limits for that period and Category of Personnel and is the lowest proposed firm per diem rate, the Bidder who proposed such rate will be allocated the applicable points assigned at Table 1 for that period and Category of Personnel.

TABLE 1 - POINTS					
TBIPS ID	**RESOURCE CATEGORIES**	**INITIAL (1 YEAR) CONTRACT PERIOD**	**OPTION PERIOD 1**	**OPTION PERIOD 2**	**TOTAL POINTS**
BUSINESS SYSTEMS					
B1	Business Analyst - Level 3	100	100	100	300
CYBER PROTECTION SERVICES CLASS					
C1	IT Security Planning and Protection Specialist - Level 3	100	100	100	300
C3	IT TRA & C&A Specialist - Level 3	100	100	100	300
C7	IT Security Design Specialist - Level 3	100	100	100	300
C11	IT Security VA Specialist - Level 3	100	100	100	300
C16	IT Privacy Specialist-Level 3	100	100	100	300
	Total Points	600	600	600	1,800

(iii) **STEP 3 - TOTAL FINANCIAL SCORE**: Points allocated under STEP 2 for each period and Category of Personnel will be added together and rounded to two decimal places to produce the Total Financial Score.

Bidders will find below an example of a financial evaluation using method 1. Please note this sample is not related to this RFP and is provided only as reference to financial evaluation methodology.

4.1 TABLE 2 - EXAMPLE OF A FINANCIAL EVALUATION USING METHOD 1

Resource Category	**Points Assigned**	**Bidder 1**		**Bidder 2**		**Bidder 3**	
		Contract Period	**Option Year 1**	**Contract Period**	**Option Year 1**	**Contract Period**	**Option Year 1**
IT Security Methodology, Policy and Procedures Analyst	**100** (50 pts. per period)	$400.00	$400.00	$420.00	$450.00	$450.00	$450.00
IT Security Engineer	**150** (75 pts. Per period)	$550.00	$550.00	$600.00	$650.00	$580.00	$600.00
IT Security Installation Specialist	**150** (75 pts. Per period)	$800.00	$800.00	$420.00	$450.00	$450.00	$450.00

IT Security Vulnerability Assessment (VA) Specialist	**150** (75 pts. Per period)	$975.00	$1000.00	$500.00	$550.00	$600.00	$635.00
IT Security Incident Management Specialist	300 (150 pts. per period)	$400.00	$400.00	$420.00	$450.00	$450.00	$450.00
Computer Forensics Specialist	150 (75 pts	$1200.00	$1300.00	$750.00	$775.00	$400.00	$450.00
TOTAL	1000						

STEP 1 - ESTABLISHING THE LOWER AND UPPER MEDIAN BANDS FOR EACH PERIOD AND EACH CATEGORY OF PERSONNEL

(Median 1)	For the **IT Security Methodology, Policy and Procedures Analyst** category, the initial contract period median would be $420.00. The lower median band limit would be $357.00 and higher median band limit would be $525.00. **NUMBERS ARE BASED ON A -15% and +25% MEDIAN for each category.**
(Median 2)	For the **IT Security Methodology, Policy and Procedures Analyst** category, the option year 1 median would be $450.00. The lower median band limit would be $382.50 and higher median band limit would be $562.50.
(Median 1)	For the **IT Security Engineer** category, the initial contract period median would be $580.00 The lower median band limit would be $493.00 and higher median band limit would be $725.00
(Median 2)	For the **IT Security Engineer** category, the option year 1 median would be $600.00. The lower median band limit would be $510.00 and higher median band limit would be $750.00.
(Median 1)	For the **IT Security Installation Specialist** category, the initial contract period median would be $450.00 The lower median band limit would be $382.50 and higher median band limit would be $562.50
(Median 2)	For the **IT Security Installation Specialist** category, the option year 1 median would be $450.00. The lower median band limit would be $382.50 and higher median band limit would be $562.50.
(Median 1)	For the **IT Security Vulnerability Assessment (VA) Specialist** category, the initial contract period median would be $600.00 The lower median band limit would be $510.00 and higher median band limit would be $750.00.
(Median 2)	For the **IT Security Vulnerability Assessment (VA) Specialist** category, the option year 1 median would be $635.00. The lower median band limit would be $539.75 and higher median band limit would be $793.75.
Median 1)	For the **IT Security Incident Management Specialist** category, the initial contract period median would be $420.00 The lower median band limit would be $357.00 and higher median band limit would be $525.00
(Median 2)	For the **IT Security Incident Management Specialist** category, the option year 1 median would be $450.00. The lower median band limit would be $382.50 and higher median band limit would be

	$562.50.
Median 1)	For the **Computer Forensic Specialist** category, the initial contract period median would be $750.00. The lower median band limit would be $637.50 and higher median band limit would be $937.50.
(Median 2)	For the **Computer Forensic Specialist** category, the option year 1 median would be $775.00. The lower median band limit would be $658.75 and higher median band limit would be $968.75.

STEP 2 – POINT ALLOCATION	
Bidder 1:	
IT Security Methodology, Policy and Procedures Analyst- Contract Period	= 50 points (lowest rate within the lower and upper median band limits)
IT Security Methodology, Policy and Procedures Analyst- Option Year 1	= 50 points (lowest rate within the lower and upper median band limits)
IT Security Engineer- Contract Period	= 75 points (lowest rate within the lower and upper median band limits)
IT Security Engineer- Option Year 1	= 75 points (lowest rate within the lower and upper median band limits)
IT Security Installation Specialist- Contract Period	= 0 (proposed rate is above the upper median band limit)
IT Security Installation Specialist- Option Year 1	= 0 (proposed rate is above the upper median band limit)
IT Security Vulnerability Assessment (VA) Specialist- Contract Period	= 0 (proposed rate is above the upper median band limit)
IT Security Vulnerability Assessment (VA) Specialist- Option Year 1	= 0 (proposed rate is above the upper median band limit)
IT Security Incident Management Specialist- Contract Period	=150 points (lowest rate within the lower and upper median band limits)
IT Security Incident Management Specialist- Option Year 1	=150 points (lowest rate within the lower and upper median band limits)
Computer Forensics Specialist- Contract Period	= 0 (proposed rate is above the upper median band limit)
Computer Forensics Specialist- Option Year 1	= 0 (proposed rate is above the upper median band limit)
Bidder 2:	
IT Security Methodology, Policy and Procedures Analyst- Contract Period	=47.62 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Methodology, Policy and Procedures Analyst- Option Year 1	=44.44 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Engineer- Contract Period	=68.8 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Engineer- Option Year 1	=63.5 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Installation Specialist- Contract Period	= 75 points (lowest rate within the lower and upper median band limits)
IT Security Installation Specialist- Option Year 1	= 75 points (lowest rate within the lower and upper median band limits)
IT Security Vulnerability Assessment (VA) Specialist- Contract Period	= 75 points (lowest rate within the lower and upper median band limits)
IT Security Vulnerability Assessment	= 75 points (lowest rate within the lower and upper median band limits)

(VA) Specialist- Option Year 1	
IT Security Incident Management Specialist- Contract Period	=142.86 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Incident Management Specialist- Option Year 1	=133.33 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Computer Forensics Specialist- Contract Period	= 75 points (lowest rate within the lower and upper median band limits)
Computer Forensics Specialist- Option Year 1	= 75 points (lowest rate within the lower and upper median band limits)
Bidder 3:	
IT Security Methodology, Policy and Procedures Analyst- Contract Period	=44.44 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Methodology, Policy and Procedures Analyst- Option Year 1	=44.44 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Engineer- Contract Period	=71.12 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Engineer- Option Year 1	=68.75 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Installation Specialist- Contract Period	=70 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Installation Specialist- Option Year 1	= 75 points (lowest rate within the lower and upper median band limits)
IT Security Vulnerability Assessment (VA) Specialist- Contract Period	=62.5 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Vulnerability Assessment (VA) Specialist- Option Year 1	=64.96 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Incident Management Specialist- Contract Period	=133.33 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
IT Security Incident Management Specialist- Option Year 1	=133.33 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Computer Forensics Specialist- Contract Period	= 0 (proposed rate is below the lower median band limit)
Computer Forensics Specialist- Option Year 1	= 0 (proposed rate is below the lower median band limit)
STEP 3 - TOTAL FINANCIAL SCORE	

Bidder 1

50+ 50+75+75+0+0+0+0+150+150+0+0= Total Financial Score of 550 points out of a possible 1000 points

Bidder 2

47.62+ 44.44+68.8+63.5+75+75+75+75+142.86+133.33+75+75 = Total Financial Score of 950.55 points out of a possible 1000 points

Bidder 3

44.44 + 44.44+71.12+68.75+70+75+62.5+64.96+133.33+133.33+0+0 = Total Financial Score of 767.87 points out of a possible 1000 points

(c) Method 2: The following financial evaluation method will be used if fewer than 3 bids are determined to be technically responsive:

(i) **STEP 1 - POINT ALLOCATION**: Points will be allocated to the Bidder, for each period and each Category of Personnel, using the following calculation which will be rounded to two decimal places:

Lowest proposed firm per diem rate x Points Assigned at Table 1 above
Bidder's proposed firm per diem rate

The Bidder with the lowest proposed RFP CEILING per diem rate will be allocated the applicable points assigned at Table 1 above.

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

(d) **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 Personnel that they later refuse to honors, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates for professional services bid, Canada may, but will have no obligation to, require price support for any rates proposed (either for all or for a specific Category of Resource). If Canada requests price support, it will be requested from all responsive Bidders proposing a rate that is at least 10% lower than the median rate bid by all responsive Bidders for the relevant Category or Categories of Personnel. Where Canada requests price support, the following information is required:

(i) an invoice (referencing a contract serial number) that shows that the Bidder has recently provided and invoiced another 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 Category of Personnel, where those services were provided in the National Capital Region for at least three months within the twelve months prior to the bid solicitation issuance date, and the fees charged were equal to or less than the rate offered to Canada;

(ii) in relation to the invoice in (i), a signed contract or a letter of reference signed by the Bidder's client that includes at least 70% of the tasks listed in this bid solicitation's Statement of Work for the Category of Personnel being examined for an unreasonably low rate;

(iii) in respect of each referenced contract, a resume for the resource that performed under that contract which shows that the resource would pass the Category of Personnel's mandatory criteria and achieve, if applicable, the required pass mark for the Category of Personnel's rated criteria; and

(iv) the name, telephone number and, if available, e-mail address of the invoiced client for each of the resources invoiced, so Canada can verify any facts presented for the affected Category or Categories of Personnel.

Once Canada requests substantiation of the rates bid for any Category of Personnel, it is the sole responsibility of the Bidder to submit information (as described above and as otherwise may be requested by Canada) 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. Where Canada determines that the information provided by the Bidder does not substantiate the unreasonably low rates, the bid will be considered non-responsive and will receive no further consideration. Only the Firm Per Diem Rates of technically responsive bids will be considered.

4.4 Basis of Selection

a) The technically responsive bid(s) that obtain one of the four the highest Total Bidder Scores will be recommended for award of a contract. The total possible Final Technical Score is **70** while the total possible Final Financial Score is **30**.

(i) **Calculation of Final Technical Score:** The Final Technical Score will be computed for each technically responsive bid by converting the Total Technical Score obtained for the point-rated technical criteria using the following formula, rounded to 2 decimal places:

Total Technical Score / Maximum Technical Points 300 pts.) x **70** = Final Technical Score

(ii) **Calculation of Final Financial Score:** The Final Financial Score will be computed for each technically responsive bid by converting the Total Financial Score obtained for the financial evaluation using the following formula rounded to 2 decimal places:

Total Financial Score / Maximum Financial Points (As per Table 4.1 above) x **30** = Final Financial Score

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

Final Technical Score + Final Financial Score = Total Bidder Score

b) 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.

c) In the event of identical Total Bidder Scores, then the bid with the highest Final Financial Score will become the top-ranked bidder.

d) The table below illustrates an example where all three bids are responsive and the selection of the contractor is determined by a 70/30 ratio of technical merit and price, respectively.

Basis of Selection - Highest Combined Rating Technical Merit (70%) and Price (30%)			
Bidder	**Bidder 1**	**Bidder 2**	**Bidder 3**
Overall Technical Score	250/300	275/300	225/300
Technical Merit Score	250/300 x 70 = 58.33	275/300 x 70 = 64.16	225/300 x 70 = 52.5
Pricing Score	1400/1600 x 30 = 26.25	1350/1600 x 30 = 25.31	1500/1600x30=28.12
Combined Rating	84.58	89.47	80.63
Overall Rating	2nd	1st	3rd

PART 5 - SECURITY REQUIREMENTS

5.1 MANDATORY AT CONTRACT AWARD - 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 requirement as indicated in Part 7 - Resulting Contract Clauses; and

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

1. Name of individual as it appears on security clearance application;
2. Level of security clearance obtained and expiry date; and
3. Security Screening Certificate and Briefing Form file number.

(b) Canada will not delay the award of any contract to allow bidders to obtain the required clearance.

(c) It is the responsibility of SA Holders to ensure that the information required concerning the security clearance is provided on time. SA Holders should indicate in their proposal if they meet all the security requirements and the status of their application for security clearance. SA Holders are advised to initiate the security clearance process as soon as possible with the Canadian Industrial Security Directorate (CISD) of Public Works and Government Services Canada (PWGSC) if they do not currently meet the security requirement specified herein. For any inquiries, SA Holders should contact CISD at 1-866-368-4646, or (613) 948-4176 in the National Capital Region. For personnel security clearance obtained under another entity or with a Federal Government Department other than PWGSC, SA Holders should contact the CISD security officer as soon as possible to be guided through the process of completing any paperwork required to request a transfer, or a duplicate of the security clearance or a new application for security clearance as appropriate.

(d) In the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

PART 6 - RESULTING CONTRACT CLAUSES

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

6.1 REQUIREMENT

_____ (the Contractor) agrees to supply to the Client the services described in the Contract, including Annex 'A' the Statement of Work, in accordance with and at the prices set out in the Contract. This includes providing professional services as requested by Canada.

(a) **Client(s):** includes any Government Department, Departmental Corporation or Agency, or other Crown entity described in the *Financial Administration Act* (as amended from time to time), and any other party for which the Department of Public Works and Government Services has been authorized to act from time to time under section 16 of the *Department of Public Works and Government Services Act*.

(b) **Reorganization of the 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.

(c) **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.

(d) **Location of Services:** Services must be delivered as requested to the locations specified in the Contract, which delivery locations must exclude any area subject to one of the Comprehensive Land Claim Agreements (CLCAs).

6.2 TASK SOLICITATION AND TASK AUTHORIZATION PROCEDURES

6.2.1 As and When Requested Task Authorizations : The Work to be performed under the Contract on an "as-and-when-requested basis" using a Task Solicitation process to issue 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.

6.2.2 Task Solicitation Work Distribution Process for TA Requirements: The Task Solicitations and the resulting Task Authorizations issued against the Contract define the performance required of a specified resource(s) to meet the requirement of a Shared Services Canada (SSC) client authorized to use the Contract.

Task Solicitations and Task Authorizations issued under the contract will be prepared by the SSC Contract Authority.

6.2.3 Authority to Raise Task Authorizations Under the Contract: Under the Contract, the Director of SSC Contracting Division delegates authority to issue Task Solicitations and Authorizations against the Contract. All delegated Technical Authorities shall follow all terms, conditions, and processes defined in the Contract. The Technical Authority listed in Article 6.6 of the Contract is required to ensure all delegated Technical Authorities follow the terms of the Contract.

6.2.4 Strike System for Work Distribution:

To ensure fairness, openness, and transparency to Contractors, the SSC Contract Authority reserves the right to apply strikes against a Contractor for actions deemed to be against the best interests of all Contractors and SSC. The actions for which strikes may be applied against a Contractor include, but are not limited to, the following actions:

a) Repeated failure to submit a proposal in response to a Task Solicitation within the time specified in the Task Solicitation;

b) Submission of inquiries regarding a Task Solicitation to someone other than the authorized SSC personnel identified in the Task Solicitation;

c) Proposal of resources who do not meet the requirements specified in the Task Solicitation;

d) Failure to secure in writing exclusive rights to the resource or resources submitted in a proposal for a specific Task Authorization;

e) Refusal by a Contractor to accept a Task Authorization for which it has submitted a proposal; and;

f) Any violation of terms and conditions outlined herein.

If a Contractor accumulates three (3) strikes against it within a year, the SSC Contract Authority reserves the right to take remedial action against the Contractor. Such remedial action could include suspension of the Contractor from use of the Contract, withdrawal of authorization to use the Contract from the Contractor, exclusion of the Supplier from any further Task Authorizations under the Contract, or other measures. The application of remedial actions is at the sole discretion of SSC.

Each action for which a strike is applied to a Contractor will be investigated by the SSC Contract Authority to confirm that the Contractor is in violation of the terms and conditions of the Contract. Withdrawal of authorization to use the Contract, for whatever reason, does not remove the right of the SSC Contract Authority or the designated user to pursue other measures that may be available.

6.2.5 Task Solicitation Process:

All work to be completed pursuant to this Contract will be authorized under the process detailed therein this article.

1.1 Stage 1—Preparation of Solicitation Document

To initiate the process, SSC's Cyber and IT Security Transformation manager authorized to use the Contract will identify the need for staff augmentation using the Contract. The delegated Technical Authority for the solicitation selects a category from the descriptions included in the Statement of Work, Annex A this Contract. The delegated Technical Authority develops a Statement of Work (SOW) to supplement the resource category description from the SOW as well as a corresponding resource evaluation grid. The delegated Technical Authority then submits these documents to the SSC Contract Authority who will review the documents and prepare a Task Solicitation form.

1.1.1 Contents of a Task Solicitation Form

The Task Solicitation form will provide relevant background information on the task. This includes project information for the requirement the task is being issued to address. The Task Solicitation form will describe the objective to be obtained by engaging a contract resource or resources for the requirement. It will also specify the location at

which the proposed resource will be required to provide services. The Task Solicitation form will typically contain the information described in the following subsections:

A. Objective

B. Background Information

C. Category and Level

The Task Solicitation form will identify the category, for which the proposed resource should be qualified to meet the requirement. The category, and level will reference Part 8, Annex A, Statement of Work.

D. Level of Effort

The Task Solicitation form will describe the level of work to be accomplished by the Task Authorization resource. The Task Solicitation form will specify the minimum number of resources the Contractor is to provide in its proposal. It will specify the tasks to be performed by the resource(s).

E. SSC Contract Authority

The Task Solicitation form will identify the SSC Contract Authority who is responsible for issuing the Task Solicitation and to whom all questions regarding the Task Solicitation should be addressed. It will provide contact information for the TA Technical Authority.

F. Solicitation Period

The Task Solicitation form will identify the solicitation period and the date by which Contractor must submit questions and concerns regarding the solicitation to the Contracting Authority. Contractors are typically required to respond to Task Solicitation within a minimum of five (5) business days, unless otherwise stipulated in the Task Solicitation form. The deadlines for submission of proposals and related questions will be explicitly stated in the Task Solicitation form. The questions submitted after the question period deadline will not be answered. All questions related to a Task Solicitation and SSC's answers will be made available to all Contractors participating in a Task Solicitation.

G. Security Requirement

The Task Solicitation form will specify the level of security clearance required by the Task Authorization resource.

H. Language Requirement

The Task Solicitation form will specify whether the requirement is for a resource to provide services in French, English, or both.

1.2 Stage 2—Distribution of the Task Solicitation

The Contract Authority will distribute; the Task Solicitation form, the category description, SOW and Evaluation Grid to all Contractors for solicitation competition.

1.3 Stage 3—Contractor Prepares and Submits Proposals

Contractor(s) receiving a Task Solicitation will prepare and submit a proposal in response to the Task Solicitation within the time specified in the solicitation. A Contractor is required to respond to a Task Solicitation within five (5) business days, unless otherwise stipulated in the solicitation. Failure by a Contractor to respond within the time specified in the Task Solicitation may result in a strike, as defined above in section 6.2.4, against the Contractor

1.3.1 Clarification of a Task Solicitation

Should a Contractor require clarification on any part of the Task Solicitation, it is the responsibility of the Contractor to contact the Contract Authority or delegated Technical Authority identified in the Task Solicitation to obtain clarification prior to the Contractor submitting their proposal. The Contractor must submit any questions regarding the Task Solicitation within the time specified in the solicitation and must direct them only to the authorized personnel as specified on the Task Solicitation.

All questions related to a Task Solicitation as well as SSC's answers, will be made available to all Contractors participating in a Task Solicitation**.** Failure by a Contractor to comply with this condition will result in disqualification of the Contractor's proposal and a strike against the Contractor.

1.3.2 Contents of a Proposal

As part of their proposal, Contractors must include the name and contact information for the Contractor's representative responsible for dealing with day-to-day performance issues. Failure to provide this information will render the Contractors' proposal non-compliant.

The Contractor must provide the résumé of the proposed resource as well as a completed Evaluation Grid. The evaluation grid will the comprised of the relevant mandatory and criteria detailed in Appendix A to Annex A.

The Contractor must propose resources who meet the requirements specified in the Task Solicitation. A Contractor's proposal of a resource that does not meet the requirements specified in the Task Solicitation will result in a strike against the Contractor.

If the Contractor mistakenly submits a resource who does not meet all of the requirements specified in the Task Solicitation, the Contractor must contact the Contract Authority directly within one working day to rectify the mistake. If the Contractor does not rectify the error, the submitted resource(s) will stand as the Contractor's proposal.

The Contractor must ensure that it has exclusive rights to the resource submitted in the Contractor's proposal for a specific TA and that the resource, if selected by SSC, will fulfill the engagement. Upon request by the SSC Project Authority, the Contractor must provide a signed copy of its exclusivity agreement with the proposed resource for a specific TA. A Contractor's failure to secure exclusive rights to the resource or resources submitted in the Contractor's proposal may result in a strike against a Contractor.

1.4 Stage 4 Evaluation of Proposals

1.4.1 Step 1 Proposals Forwarded to the Contract Authority

At the end of the proposal receipt period, when proposals from all Contractors have been received by SSC's Contract Authority, the résumés from the proposals are forwarded by the Contract Authority to the Technical Authority who initiated the requirement.

1.4.2 Step 2 Technical Authority Evaluates Proposals

The Technical Authority responsible for the requirement is wholly responsible for the evaluation of proposals and will document the evaluation. The Technical Authority first reviews the résumés for compliance with the requirements specified in the Task Solicitations; SOW and mandatory criteria,. The Technical Authority will rejects from further consideration any résumé the Technical Authority identifies as mandatory non-compliant.

Upon verification that Contractors proposed candidates meet the mandatory criteria, the Technical Authority will access and document using the same rating criteria evaluation tool to further evaluate and score all resources proposed by all Contractors.

The Technical Authority will identify the Contractor whose candidate receives the highest technical score

In the event of tie highest technical scores, at their sole discretion, the Technical Authority will have the option to request a candidate's interview. If the Technical Authority decides to interview proposed resources, a standardized template and set of questions for an interview Scorecard will be used. The Technical Authority will use the same interview Scorecard to interview all resources proposed by l Contractors. The Contractor is responsible for ensuring that a proposed resource is available for interview. If a resource fails to attend an interview, the Contractor that has submitted the resource will be found non-compliant.

After the technical evaluation has been completed, the Technical Authority submits the results to the Contract Authority.

If the Technical Authority elects to forgo an interview process for the tied high technical score candidates, the Contract Authority will award the Task Authorization to the Contractor who holds the lower firm per diem rate.

In the all cases other than a tie, the Contract Authority will award the Task Authorization to the Contractors receiving highest technical score.

1.4.3 Step 3 Technical Authority Documents Evaluation

The Technical Authority will document all decisions regarding the proposed resources and provide the Contract Authority all such supporting documentation. This documentation may include the following items:

- Identification of requirements for which a résumé is non-compliant;
- Evaluation of résumés using the common evaluation tool.

1.5 Stage 5—Task Authorization Award

All Contractors that have submitted proposals in response to a Task Solicitation will be notified of the results of the process.

The Task Authorization will incorporate the Task Solicitation documents and, by reference, terms and conditions of the Contract. The Task Authorization will authorize the Contractor to proceed based upon the agreed technical requirements and start and end dates.

The Contractor will not commence work until an approved Task Authorization has been received from the Contracting Authority. The Contractor acknowledges that any and all work performed in the absence of the aforementioned Task Authorization will be done at the Contractor's own risk, and SSC shall not be liable for payment thereafter, unless or until a Task Authorization is provided by the Contracting Authority.

1.6 Stage 6—Commencement of Work

The Contractor selected for a Task Authorization resulting from the Contract must commence work in accordance with a start date indicated in the Task Authorization.

1.6.1 Financial Limitations

The estimated total cost authorized for each Task Authorization will not be exceeded unless and until an increase is authorized by a formal Task Authorization amendment. No amendment of a Task Authorization will be binding upon the Contractor or SSC unless a formal Task Authorization amendment in writing has been issued by the Contracting Authority. Likewise, SSC will not be liable for any adjustment to the price of a Task Authorization on account of a change in the Task Authorization, unless the change is authorized in writing by the Contracting Authority.

1.6.2 Exercising an Option for Extension

A Task Authorization under the Contract can have options for extensions as required by the Technical Authority and specified in the Task Authorization. These options are exercised at SSC's sole discretion. When a Task Authorization is in the initial Task Authorization period or in any extension period, the Contractor is responsible for advising the Contract Authority and the Project Authority when there are 15 business days remaining in the Task Authorization.

Automatic extension of the Task Authorization is not authorized and SSC will not be responsible for any financial expenses incurred by the Contractor as a result of an extension not authorized by SSC. To exercise the option for an extension of the Task Authorization, the Project Authority must notify the Contract Authority that the option to extend the Task Authorization is to be exercised. When a Task Authorization is in its last extension, the Contractor is responsible for advising the Contract Authority and the SSC Project Authority when there are 20 business days remaining in the Task Authorization.

6.2.4 Period of Services of the Task Authorizations Awarded Under the Contract

Task Authorizations may be issued from the date that the Contract is signed until the expiry date of the Contract or any extension thereof. Each Task Authorization will indicate the period of services during which the specified work will be performed.

Furthermore, some Task Authorizations may contain a provision or provisions for option(s) that extend the initial period of service. Contractors will be notified in writing, at least ten (10) calendar days prior

to the expiration of the current period of service, of SSC's intention to exercise any option contained in a contract period-of-services article.

6.2.5 Termination of a Task Authorization

The Contract Authority may, at its sole discretion, terminate all or any part of a Task Authorization at any time upon three (3) calendar days written notice to the Contractor. In the event of such termination, the Contractor agrees that it shall be entitled to be compensated only for work performed and accepted up to the effective date of such termination

6.2.6 Task Authorization Limit and Authorities for Validly Issuing Task Authorizations:

To be validly issued, a TA must be signed by the 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.

6.2.7 Periodic Usage Reports:

i. The Contractor must compile and maintain records on its provision of services to the federal government under validly issued TAs issued under the Contract. The Contractor must provide this data to Canada in accordance with the reporting requirements detailed below. If any required information is not available, the Contractor must indicate the reason. If services are not provided during a given period, the Contractor must still provide a "NIL" report. The Contractor must submit the periodic usage reports on a quarterly 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. April 1 to June 30;
B. July 1 to September 30;
C. October 1 to December 31; and
D. January 1 to March 31.

The data must be submitted to the Contracting Authority no later than 30 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 the 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 TA (GST or HST extra);
E. the total amount (GST or HST extra) expended to date;
F. the start and completion date; and

G. the active status, 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 TAs (as amended):

A. the amount (GST or HST extra) specified in the contract (as last amended, if applicable) as Canada's total liability to the contractor for all validly issued TAs; and
B. the total amount, GST or HST extra, expended to date against all validly issued TA's.

6.2.8 Pre-Cleared Resources:

The Contractor must:

i. ensure that the specific individuals named in Annex E of this Contract or acceptable alternatives remain available in appropriate quantities for work under the Task Authorizations to be issued in accordance with this Contract, and must also ensure that these individuals maintain any professional qualifications and security levels associated with the corresponding resource categories of the bid solicitation for which they are available; and
ii. avoid delays associated with the Contract's security requirements by initiating the assessment and security clearance of additional resources by Canada within 15 business days of Contract award and on an ongoing basis during the Contract Period, in the quantities specified for each resource category in the Annex. Each such resource must meet the minimum qualifications applicable to the resource category for which they are available, as well as the security requirements identified in the Contract. If accepted by Canada, the Contract will be amended to list each such resource by name.

The resources identified in the Contract must be maintained and available in the quantities specified throughout the Contract Period. There is no limit to the number of resources that the Contractor may submit for consideration and assessment on an ongoing basis; however, the submission of alternatives does not relieve the Contractor from its obligation to provide, for a given task, specific individuals agreed to be provided to Canada in a validly issued TA or elsewhere as required by the terms of this Contract.

6.2.7 Consolidation of TAs 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 TAs for administrative purposes

.

6.2.9 Minimum Work Guarantee - All the Work - Task Authorizations

1. In this clause,

"Maximum Contract Value" means the amount specified in the "Limitation of Expenditure" clause set out in the Contract; and

"Minimum Contract Value" means 1% of the Maximum Contract Value.

2. 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 paragraph 3. 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.

3. In the event that Canada does not request work in the amount of the Minimum Contract Value during the period of the Contract, Canada must pay the Contractor the difference between the Minimum Contract Value and the total cost of the Work requested.

4. Canada will have no obligation to the Contractor under this clause if Canada terminates the Contract in whole or in part for default.

6.3 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:**

2035 (2014-03-01), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

The text under Subsection 04 of Section 41 – Code of Conduct and Certifications, of General Conditions 2035 referenced above is replaced by:

During the entire period of the Contract, the Contractor must diligently update, by written notice to the Contracting Authority, the list of names of all individuals who are directors of the Contractor whenever there is a change. As well, whenever requested by Canada, the Contractor must provide the corresponding Consent Forms.

6.4 SECURITY REQUIREMENT

The following Security Requirement (SRCL and related clauses), as set out under Annex "A" to the Supply Arrangement, applies to the Contract

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:

PWGSC FILE #	***Contractor Clearance***	***Personnel Security Screening***	***Contractor and its personnel***
EN578-055605-E	*FSC (Secret)*	*Secret*	*MUST NOT remove any protected/CLASSIFIED information*

(a) The Contractor must, at all times during the performance of the Contract, hold a valid Facility Security Clearance at the level of SECRET, issued by the Canadian and International Industrial Security Directorate (CIISD), Public Works and Government Services Canada (PWGSC).

(b) The Contractor personnel requiring access to PROTECTED/CLASSIFIED information, assets or sensitive work site(s) must EACH hold a valid personnel security screening at the level of SECRET, granted or approved by CIISD/PWGSC.

(c) The Contractor MUST NOT remove any PROTECTED/CLASSIFIED information from the identified work site(s), and the Contractor must ensure that its personnel are made aware of and comply with this restriction.

(d) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CIISD/PWGSC.

(e) The Contractor must comply with the provisions of the:

(i) Security Requirements Check List EN578-055605/E, described in Annex C

(ii) Industrial Security Manual (Latest Edition).

6.5 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 year(s) later; and

(ii) The period during which the Contract is extended, if Canada chooses to exercise its option set out in the Contract.

6.5.1 OPTION TO EXTEND THE CONTRACT

(i) The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to two additional one-year 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 at Annex B.

(ii) Canada may exercise this option at any time by sending a written notice to the Contractor. The option may only be exercised by the Contracting Authority, and will be evidenced, for administrative purposes only, through a contract amendment.

6.6 AUTHORITIES

(a) Contracting Authority

The Contracting Authority for the Contract is:

Gary Cooper
180 rue Kent St, 13-K088
P.O. Box/CP 9808 STN T CSC
Ottawa, ON K1G 4A8
Email: gary.cooper@ssc-spc.gc.ca
Tel. | Tél. : 613-218-9250

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** (*to be inserted 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.

(c) **Contractor's Representative** (*to be inserted at Contract award*)

The Contractor's Representative for the Contract is:

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
Facsimile: _____
E-mail address: _____

6.7 PAYMENT

(a) Basis of Payment

(i) **Professional Services provided with a Fixed Time Rate to a Maximum Price:** For professional services requested by Canada, Canada will pay the Contractor, in arrears, up to the Maximum Price, for actual time worked and any resulting deliverables in accordance with the firm all-inclusive per diem rates set out in Annex B of this contract, Basis of Payment, GST/HST extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.

(ii) **GST/HST**

(iii) **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.

(iv) **Professional Services Rates**: In Canada's experience, bidders 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. This denies Canada of the benefit of the awarded contract. If the Contractor refuses, or is unable, 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, Canada may impose sanctions or take other measures in accordance with the PWGSC Vendor Performance Policy (or equivalent) then in effect, which may include prohibiting the Contractor from bidding on future requirements that include any professional services, or rejecting the Contractor's other bids for professional services requirements on the basis that the Contractor's performance on this or other contracts is sufficiently poor to jeopardize the successful completion of other requirements.

(v) **Purpose of Estimates**: All estimated costs contained in the Contract are included solely for the administrative purposes of Canada and do not represent a commitment on the part of Canada to

purchase services in these amounts. Any commitment to purchase specific amounts or values of services is described elsewhere in the Contract.

(vi) Canada will not pay for any travel or living expenses associated with the performance of this contract.

(b) Limitation of Expenditure Canada 's total liability to the Contractor under the Contract must not exceed the amount set out on page one of the Contract, less any Applicable taxes. With respect to the amount set out on page one of the Contract, Customs duties are excluded and Goods and Services Tax or Harmonized Sales Tax is included, if applicable. Any commitments to purchase specific amounts or values of goods or services are described elsewhere in the Contract.

i. No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceed before obtaining the written approval of the Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum when:
   A. It is 75 percent committed, or
   B. 4 months before the Contract expiry date, or
   C. as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

whichever comes first.

ii. 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**

(i) **Monthly Payment**

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

(A) 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;

(B) all such documents have been verified by Canada;

(C) the Work performed has been accepted by Canada; and

(D) the time sheets for each resource showing the days and hours worked to support the charges claimed in the invoice have been submitted.

(ii) Once Canada has paid the maximum price, Canada will not be required to make any further payment, but the Contractor must complete all the work described in the Task Authorization/Contract, all of which is required to be performed for the maximum price. If the work described in the Task Authorization/Contract 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 price, Canada is only required to pay for the time spent performing the work related to that Task Authorization/Contract.

(d) **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 Contract must repay any overpayment, at Canada's request.

(e) **No Responsibility to Pay for Work not performed due to Closure of Government Office**

Where the Contractor, its employees, subcontractors, or agents are providing services on government premises under the Contract and those premises are inaccessible because of the evacuation or closure of government offices, and as a result no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if there had been no evacuation or closure.

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.

6.8 INVOICING INSTRUCTIONS

(a) The Contractor must submit invoices in accordance with the information required in the General Conditions. The Contractor's invoice must include a separate line item for each element in the Basis of Payment provision.

(b) By submitting invoices (other than for any items subject to an advance payment), 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.

(c) Canada will only be required to make payment following receipt of an invoice that satisfies the requirements of this Article.

(d) The Contractor will submit invoices on its own form, which will include:

(i) the date;

(ii) the Contractor name and address;

(iii) the Destination

(iv) Standing Offer/Supply Arrangement number;

(v) Contract serial number;

(vi) Financial codes, including GST or HST (as applicable) registration number;

(vii) Description of the Work

(viii) Category(ies) of Personnel and number of days worked;

(ix) Firm Per Diem Rate on which the total dollar amount of the invoice is based;

(x) the amount invoiced (exclusive of the Goods and Services Tax (GST) or Harmonized Sales Tax (HST) as appropriate) and the amount of GST or HST, as appropriate, shown separately;

(xi) Client Reference Number (CRN);

(xii) Business Number (BN); and

(xiii) Total value billed to date and the dollar amount remaining in the Contract to date.

(e) The Contractor will send the original and one copy of the invoice to the Technical Authority's paying office (SSC Finance) and one to the Contract Authority as follows:

The original and one copy of the invoice must be sent to the following location on a monthly basis:

Attn: SSC Accounts Payable
SSC Finance
700 Montreal Road, 8th Floor
Ottawa, Ontario K1A 0P7

A digital copy of the invoices must be sent to the Contracting Authority at the following location on a quarterly basis:

Attn: Gary Cooper
180 Kent Street 13th Floor
Ottawa, Ontario K1P 0B6

(f) The Technical Authority's paying office (SSC Account Payable) will send the invoices to the Technical Authority for approval and certification; the invoices will be returned to the paying office for all remaining certifications and payment action.

(g) Any invoices where items or group of items cannot be easily identified will be sent back to the Contractor for clarification with no interest or late payment charges applicable to Canada.

(h) If Canada disputes an invoice for any reason, Canada agrees to pay the Contractor the portion of the invoice that is not disputed provided that items not in dispute form separate line items of the invoice and are otherwise due and payable under the Contract.

(i) Notwithstanding the foregoing, the provisions of "Interest on Overdue Accounts", Section 16 of 2035 – General Conditions will not apply to any such invoices until such time that the dispute is resolved at which time the invoice will be deemed as "received" for the purpose of the "Method of Payment" clause of the Contract.

6.9 CERTIFICATIONS

Compliance with the certifications provided by the Contractor in its response to the RFP is a condition of the Contract and subject to verification by Canada during the entire Contract Period. If the Contractor does not comply with any certification or it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, under the default provision of the Contract, to terminate the Contract for default.

6.10 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 HRSDC-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 HRSDC will constitute the Contractor in default as per the terms of the Contract.

6.11 APPLICABLE LAWS

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in the province of Ontario or as indicated in the Bidder's Supply Arrangement.

6.12 PRIORITY OF DOCUMENTS

If there is a discrepancy between the wordings 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) General Conditions 2035 (2014-03-01);

(c) Annex A - Statement of Work;

(d) Annex B - Basis of Payment;

(e) Annex C - Security Requirements Check List;

(f) Supply Arrangement Number EN578-055605/xxx/EI (the "**Supply Arrangement"**) ***<To Be Inserted at Contract Award>***;

(g) the Contractor's bid dated _____, as amended _____, not including any software publisher license terms and conditions that may be included in the bid, not including any provisions in the bid with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of a web link) in the bid.

6.13 FOREIGN NATIONALS (CANADIAN CONTRACTOR)

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

6.14 INSURANCE REQUIREMENTS

The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

6.15 LIMITATION OF LIABILITY - INFORMATION MANAGEMENT/INFORMATION TECHNOLOGY

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 section, even if it has been made aware of the potential for those damages.

(a) **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 (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 relates 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 by Canada either in whole or in part for default, up to an aggregate maximum for this subparagraph (ii) of the greater of _0.75_ times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block 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 $2,000,000.00. In any case, the total liability of the Contractor under paragraph (e) will not exceed the total estimated cost (as defined above) for the Contract or $2,000,000.00, 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.

(b) **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, 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 paragraph (a), 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 paragraph 3.

6.16 JOINT VENTURE CONTRACTOR

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

(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.*

6.17 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, and 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 Section titled "Replacement of Specific Individuals" is deleted and the following applies instead:

Replacement of Specific Individuals

1. 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 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.

2. 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 for default under Section 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 propose a replacement to be rated by the Technical Authority. The replacement must have qualifications and experience that meet 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 subarticle (c).
3. Where an Excusable Delay applies, Canada may require (c) (ii) (B) above instead of terminating under the "Excusable Delay" Section. 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. The Contractor must not, in any event, allow performance of the Work by unauthorized replacement persons. The Contracting Authority may order that a 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 that a resource stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.
4. The obligations in this article apply despite any changes that Canada may have made to the Client's operating environment.

6.18 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.

6.19 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. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the. 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, 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.

6.20 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.

6.21 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 if an individual is not a permanent employee of the Contractor prior to the commencement of the meeting, to ensure that each meeting participant is aware of the fact that the individual is not a Contractor permanent employee;
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.

6.22 TRANSITION SERVICES AT END OF CONTRACT PERIOD

The Contractor agrees that, in the period leading up to the end of the Contract Period and for up to three months afterwards, it will make all reasonable efforts to assist Canada in the transition from the Contract to a new contract with another supplier. The Contractor agrees that there will be no additional charge for these services.

ANNEX A

STATEMENT OF WORK

1. Objectives

To acquire six (6) categories of Informatics professional services from the private sector by using the Task-Based Informatics Professional Services (TBIPS) supply arrangement on an as required basis.

2. Shared Services Canada (SSC) - Background

Shared Services Canada was created on August 4, 2011 to fundamentally transform how the Government manages its information technology (IT) infrastructure. SSC mandate is to consolidate and operate data center, network and email services with central agencies and SSC's Partners. The mandate for the provision of enterprise-wide IT-infrastructure services represents better value for money and a more reliable IT infrastructure to support modern government operations.

3. Cyber and IT Security Transformation Program (CITS)-Background

CITS Mandate: "Cyber and Information Technology Security Transformation is responsible for the development of plans and designs for GC IT infrastructure Cyber and IT security services and for GC Secret Infrastructure, within SSC mandate. This directorate will develop business cases for design-ready IT security and secret infrastructure services, and will develop and continuously improve strategic sourcing solutions, security controls and business architecture for the implementation and delivery of transformed services. This directorate fosters strategic relationships with central agencies and SSC's partners to develop policies, standards, technology guidance and on-going oversight for Cyber and IT security service management and delivery."

4. Scope of Work

Shared Services Canada (SSC), Cyber and IT Security Transformation division has a requirement for professional services on a "as and when required basis" for the services provided by IT Professionals in the IT Security domain, and to assist with the establishment of the Cyber and IT Security transformation program. CITS requires experienced, dynamic IT Security professional services with a secret clearance and expertise in various IM/IT technologies. Responsibilities will be initiated using a Task Authorization process.

The work performed under this contract will provide IT Security support and services in Unclassified, Classified and all Designated Domains for all Shared Services Canada Transformation Programs and Projects related to CITS sub-programs including:

4.1 Cyber Security sub-Program

- ***Scope:*** *... develops and continuously improves SSC's capacity to defend against emerging cyber threats through improved situational awareness, evaluation of risk likelihood and impact and the development of effective mitigation strategies. This includes developing cyber strategies, standards, guidelines, threat and impact assessments for SSC.*
- ***Functions:***
  - *Cyber Assessments and Situation Awareness*
  - *Supply Chain Integrity*

- *Strategic Planning and policy development in the cyber security domain*

4.2 IT Security Services sub-Program

- ***Scope:*** *... consolidation and standardization of the IT Security services identified below for unclassified, designated*, and secret infrastructures. This sub-program provides ongoing planning, monitoring, advice, and guidance regarding the design, implementation and operation of these services.*
- ***Functions:***
  - *Provide IT Security Advice and Guidance and develop security controls to the three SSC-mandated Transformation Programs (DCE, DCC, TTP, WTD), TBS Back-Office Application Consolidation initiatives, security tripartite partners (CSEC, TBS), partner projects and SSC Operations;*
  - *Develop strategic approaches and provide input to strategic plans in support of IT security strategies, sourcing strategies, and IT policies*
  - *Implement Identity, Credential and Access Management (ICAM) services*
  - *Transform Network Security services at the network level*
  - *Transform Device Security services for end user devices and for backend infrastructure devices*

4.3 Government of Canada Secure Infrastructure (GCSI) sub-Program

- ***Scope:*** *... design, development and implementation of GC secret level infrastructure for common and core services to support secret level processing requirements.*
- ***Functions:***
  - *Develop the GCSI Program*
  - *Define, plan, and coordinate GCSI program projects*

4.4 Enterprise Security Requirements Definition and Integration Services

- ***Scope:*** *... define security requirements in support of steady state SSC security services to transformation programs, partner projects, and other identified government initiatives.*
- ***Functions:***
  - *This service will provide the following core activities:*
  - *Definition of Security Profiles;*
  - *Definition of Security Controls;*
  - *Provision of Security Requirements Advice and Guidance; and,*
  - *Act as security requirements liaison with CSEC and TBS.*
  - *This service will provide the following program activity in support of transformation programs and partner projects:*
  - *Defining security requirements in support of procurement documents (e.g. RFP, contracts, SOWs, etc).*

5. Personnel Requirements

The Contractor must provide Informatics Professional Services in Six (6) different resource categories on an “as and when required” basis:

RESOURCE CATEGORY	LEVEL	TBIPS ID
IT Business Analyst	Level III	B1
IT Security Planning and Protection Specialist	Level III	C1
IT TRA & C&A Specialist	Level III	C3
IT Security Design Specialist	Level III	C7
IT Security VA Specialist	Level III	C11
IT Privacy Specialist	Level III	C16

These professional services are required in a large number of projects all related to the EA mandate identified above, or in general activities for related projects including: as Enterprise Architecture; Security Architecture, Evaluations or Certifications; and/or Project Management.

The level of effort and duration of projects may vary (e.g. from two weeks to two+ years). The Contractor personnel involved in both shorter and longer-term projects must be prepared to perform the same tasks repetitively. The Contractor personnel involved in longer duration projects may be required to participate in either all of the project, or only the part of the project pertaining to their area of expertise (possibly while working in a preformed project team).

The required services will be related to one or more of the activities listed below (Note: these activities are not inclusive of the entire spectrum of activities which may require the involvement of Contractor personnel):

5.1 Role Descriptions

The following provides a description of the proposed tasks and duties to be performed by each resource category.

5.1.1 B1 Business Analyst Level 3

The following responsibilities are associated with this “Statement of Work” (but are not limited to):

- Develop, review and manage business requirements
- Plan, coordinate, capture and follow up on meetings with SSC partner Departments and agencies for business requirements gathering along with their prioritization, associated business impact, costs/cost models and business dependencies.
- Perform analysis of the business requirements to identify and document SSC and partner roles and responsibilities
- Perform analysis of the business requirements to identify and document information, procedures and decision flows, and associated policies.
- Capture the current use cases associated with the business requirements
- Obtain and manage formal written SSC partner approvals of the business requirements specification document
- Establish acceptance test criteria with client.
- Support and use the selected departmental methodologies.
- Document, review with stakeholders and track actions and meetings decisions
- Identify and document current state business processes (business or operations)
- Provide guidance to technical architects and developers to meet the requirements
- Develop presentations for stakeholders or senior executives
- Perform business analysis of functional requirements to identify information, procedures and decision flows;
- Identify and evaluate existing procedures, methods, and items such as database content and structure
- Define and document interfaces of manual to automated operations within application subsystems, to external systems and between new and existing systems
- Working with various stakeholders and other sources to understand and identify all requirements information that is relevant to the project. Facilitates cross-functional meetings and exercises to verify current state, to capture requirements and to ensure Cyber project(s) alignment to existing transformation initiatives/ programs;

- Planning and implementing all requirements-related activities, including elicitation, validation, reporting status, resolving conflicts, and gaining approval.

- Develops and manages detailed business and functional requirements for Cyber project(s), by preparing use cases, data models, and capturing existing business rules from various forms of documentation such as process maps and interviews with subject matter experts. Organizing, structuring and understanding the elicited requirements; putting them into an appropriate form, and performing necessary verification and validation on them;
    - Managing the requirements themselves, including requirements change control and scope control.
- Assists in detailed design and development by maintaining "To-Be" process models, undertaking issues analysis and ensuring architecture and technical teams understand the underlying business objectives and functional capabilities required for project success;

The service required is to assist with the development and delivery of both an interim and longer-term Cyber Infrastructure Recall System by working among stakeholders and subject matter experts in gathering, analysing, modelling, communicating and validating requirements for architecture and design.

As time permits, the business analyst may be engaged in other work to support the Cyber Program.

In the course of this work, the Contractor may be required to provide Project Management assistance, with any or all of the tasks detailed below, to other professionals whose tasks fall within the Cyber Security program scope.

General Program Support:

a) Developing business documents such as business cases and strategic investment proposals and ensuring alignment with the Directorate's business plan.

b) Analyzing and documenting new and existing business processes to support Cyber Program and project objective(s)

c) Assists the project managers in the preparation of project charters, statements of work, project plans and schedules; Assists project managers in performing processes that support the project management planning domains such as change control process, issue tracking, risk management and SSC gating processes

5.1.2 C1 IT Security Planning and Protection Specialist Level 3

The following responsibilities are associated with this "Statement of Work" (but are not limited to):

- Review, analyze, and/or apply the IT Security Policies, Procedures and Guidelines of International government, Federal, Provincial or Territorial government.
- Review, analyze, and apply the best practices, national or international computer law and ethics, IT Security architecture, and IT Security Risk Management Methodology
- Develop vision papers delineating the way ahead to ensure that IT Security and cyber protection are business enablers
- Conduct business function analysis and business impact assessments
- Brief senior managers
- Provide strategic assessments on technology trends and emerging technologies

- Provide IT Security strategic planning and advice.
- Conduct feasibility studies, technology assessments and cost-benefit analyses, and propose system implementation plans for IT Security
- Develop advanced R&D policy/strategy
- Collect, collate and prioritize client IT Security and Information Infrastructure Protection requirements
- Evaluate and assist in the selection of enterprise-wide technology tools
- Review and prioritize IT Security and Information Infrastructure Protection programs
- Develop strategic IT Security architecture vision, strategies and designs using the Business Transformation Enablement Program (BTEP) methodology and the Government Strategic Reference Model(GSRM)
- 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
- Develop and deliver training material relevant to the resource category
- Review and prioritize IT Security and Information Infrastructure Protection programs

5.1.3 C3 Security TRA and C&A Analyst Level 3

The following responsibilities are associated with this “Statement of Work” (but are not limited to):

- Following the GC Harmonized Threat & Risk Assessment (HTRA) Methodology, formulate and document Statements of Sensitivity, identify threat agents, threats and threat scenarios, perform threat assessment, determine risks, identify potential vulnerabilities and recommend safeguards and other risk mitigation strategies on the IT enterprise-wide infrastructure, systems, and services identified by the Technical Authority
- Formulate and document a draft and final Threat Assessment report
- Formulate and document a draft and final Threat Risk Assessment report
- Develop a report that synthesizes recommendations and risk mitigation strategies for senior management and other stakeholders, with supporting detailed technical documentation
- Work in partnership with all stakeholders to identify technical architecture, challenges, risks, and recommendations for various SSC projects related to the SSC’s Transformation Programs/Initiatives;
- Collaborate with all stakeholders on the evaluation of any relevant data from service providers, transformation teams, project management build teams and operational teams;
- Complete tasks as needed directly supporting the GC and SSC Cyber and IT Security Transformation Program as well as other CITS core transformation programs;
- Produce various security artifacts as needed;
- Participation in related IT Security meetings, discussions and presentations to stakeholders or senior management;
- Document, review and track actions and meetings decisions;
- Perform functional and options analysis in support of program delivery;
- Perform impact analysis with the perspective of an enterprise solution, evaluate and make recommendations;
- Create presentations and present to various stakeholders, and facilitate meetings and discussions.
- Review Statement of Sensitivity, Statement of Acceptable Risk documents
- Identify threat agents, threats and threat scenarios, determine risks, identify potential vulnerabilities and recommend appropriate safeguards and other risk mitigation

strategies on the IT infrastructure, systems, applications and services identified by the Technical Authority, while re-using existing relevant information as much as possible
- Verify that security safeguards for applications, systems, and infrastructures meet the applicable policies and standards
- Verify that security safeguards have been implemented correctly
- Assess and verify that residual risk indicated in risk assessments meet an acceptable level
- Review security assessment results to ensure that the system will operate at an acceptable level of risk and that it will comply with the departmental and system security policies and standards

- Support the Certification Authority in evaluating the certification evidence package;
- Responsible for producing a number of SSC CITS ITSPD template documents, such as: SA&A Reports, Briefing Notes ITSG-33 based security controls profiles, TRAs, as well as other types of security assessments
- Write Certification Report and Accreditation Letters based on status of the safeguards selected and implemented;
- Witness security tests where appropriate;
- Review and critique safeguard implementation plans;
- Audit results of security testing, security validation and security checklist compliance;
- Collaborate on the investigation of security requirements, attributes, and safeguards that further enhance the security profile of the system;
- Assist business partners in the development of security requirements (Statement of Sensitivity, Asset Categorization, Threat modelling, Business Needs for Security, Statement of Acceptable Risk, etc...);
- Assessment of Reference Architecture Documents, Technical Architecture Documents and Detailed Design Documents as they apply to security;
- Assessment of IT security controls (ITSG33 based) and safeguards;
- Assessment of mitigation strategies;
- Assessment of residual risk;
- As required, deliver IT Security training awareness sessions;
- Other ad hoc technical documents or reports as required by the Certification Authority.
- The SA&A evidence review includes producing a Shared Services Canada (SSC) Certification Report as well as the related evidence package. Documents to review to produce both the report and package include (but are not limited to) Privacy Assessment questionnaire, Statement of Sensitivity, Architecture Diagrams, Statement of Acceptable Risk, Security Testing and Evaluation plan, Vulnerability Assessment report, Safeguard Implementation Plan, Concept of Operations, Security Requirements Traceability Matrix
- Security Concept of Operations
- A high level overview of what security (from privacy, organizational, administrative, personnel, and technical, procedural and contingency management viewpoints) must be met in the final system's design solution.
- A contextual security view of the project functionality (logical diagrams, specific business level circumstances, conditions and concerns) that the system's security design will be expected to satisfy.
- Architecture Design
- Describes the conceptual design, logical design, network design and physical design from a security perspective.
- Threat and Risk Assessment comprised of:
- Statement of sensitivity;
- Threat assessment;
- Non-technical vulnerability assessment;

- Risk assessment;
- Recommendations for risk mitigation.
- Privacy Assessment (Questionnaire)
- Security Requirements Traceability Matrix
- Security Testing and Evaluation Plan
- A plan of what is going to be tested and evaluated, a procedure of how it is going to be tested and evaluated and the results of the testing and evaluation.
- Vulnerability Assessment (VA) / Penetration Testing
- Develop Vulnerability Assessment Plan
- In consultation with required parties, conduct (or observe in some cases) and document results of Vulnerability Assessment (VA) / Penetration Testing
- Safeguard Implementation Plan
- Identification of deficiencies found during formal security testing and evaluation activities and/or the final TRA with recommendations to address the deficiencies in the achievement of the required security.
- Provide evidence that services and /or applications and infrastructure meets the requirements that have been documented in the above mentioned deliverables, including:
- Verification that security safeguards meet the applicable policies and standards;
- Validation of security requirements by mapping system-specific security policy to functional security requirements, and mapping the security requirements through the various stages of design documents;
- Verification 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;
- Security testing and evaluation (ST&E) to determine if the technical safeguards are functioning correctly.
- Review and provide written feedback on the following types of deliverables:
    - Security Management Plan
    - Privacy Management Plan
    - Service Continuity Plan
    - Security Risk Assessment Reports
- Contractors' plans, documents and evidence of an ISO 27001 certified or equivalent Information Security Management System (ISMS)

5.1.4 C7 IT Security Design Specialist Level 3

The following responsibilities under this contract include the following, but not limited to:

- Work in partnership with all stakeholders to identify technical architecture, challenges, risks, and recommendations for various SSC projects related to the SSC's Transformation Programs/Initiatives;
- Collaborate with all stakeholders on the evaluation of any relevant data from service providers, transformation teams, project management build teams and operational teams;
- Complete tasks as needed directly supporting the GC and SSC Cyber and IT Security Transformation Program as well as other CITS core transformation programs;
- Conduct analysis of Current State Assessments in support of CITS core transformation programs;
- Produce various security artifacts as needed;
- Participation in related IT Security meetings, discussions and presentations to stakeholders or senior management;

- Document, review and track actions and meetings decisions;
- Perform functional and options analysis in support of program delivery;
- Perform impact analysis with the perspective of an enterprise solution, evaluate and make recommendations;
- Create presentations and present to various stakeholders, and facilitate meetings and discussions.
- Provide Security Training & Awareness.
- IT Security requirements support for core CITS Transformation Programs comprised of, but not limited to:

  a) Review business and IT Security requirements from various SSC programs and initiatives;
  b) Work in partnership with all stakeholders to develop security control profiles based on CSEC ITSG-33 and other related security standards, in support of various SSC projects related to SSC's Transformation Programs/Initiatives;
  c) Validate IT Security requirements by mapping business and/or security requirements through the various stages of the Information System Security Implementation Process (ISSIP);
  d) Analyze and evaluate client requirements and documentation;
  e) Plan, conceptualize, coordinate and document recommendations for solutions based on client requirements;
  f) Perform functional and options analysis in support of program delivery;
  g) Perform impact analysis with the perspective of an enterprise solution, evaluate and make recommendations;

- IT Security strategies, frameworks, models, methodologies, roadmaps, plans, heat maps, RACI matrices, policies and instruments in the areas of, but not limited to:

  a) Security Risk Management, including risk assessment methodologies;
  b) Security Assessment & Authorization (SA&A);
  c) Security Program Management and Governance, including organizational and/or functional design or review, and IS and/or ITS program-level compliance reporting;
  d) Review/analyze various SSC and/or TBS transformation initiative deliverables and ensure compliance, alignment, and conformity of deliverables with Government of Canada (e.g., TBS, CSEC, PS, SSC) IT Security strategies, principles, methodologies, frameworks, programs, policies and instruments (directives, standards, guidelines), and procedures
  e) Develop IT Security standards, procedures and guidelines pursuant to the requirements of Canada's National Security Policy, Treasury Board Secretariat's Policy on Government Security, and supporting operational standards (e.g., MITS), departmental/agency security policy, and other relevant standards, procedures and guidelines
  f) Develop IT Security policy in the areas of IT security and assurance, standard Certification & Accreditation frameworks for IT systems, information infrastructure protection, product evaluation, privacy, Business Continuity Planning, contingency planning and Disaster Response Planning, Research & Development
  g) IT Security Service Management;

- IT Security risk management comprised of, but not limited to:

  a) Review/analyze various SSC and/or TBS transformation initiative deliverables and ensure compliance, alignment, and conformity of deliverables with Government of Canada (e.g., TBS, CSEC, PS, SSC) IT Security strategies, principles, methodologies, frameworks, programs, policies and instruments (directives, standards, guidelines), and procedures;

b) Recommendations for IT Security risk mitigation and other related deliverables, as required.

Additional deliverables requirements for Cyber Security sub-Program (but are not limited to):

- Assist in completing all necessary documentation (such as Reports, Roadmaps, Presentation decks) on various current-state assessments (such as Communications Security (COMSEC), Local Information Protection Centre (LIPC);
- Document security related processes for transformation initiatives);
- Development of Request for proposals (RFP) documents to assist in the procurement process of security hardware/software to be used in the Shared Services Canada – Security Operations Centre (SSC-SOC).

Additional deliverables requirements for IT Security Services sub-Program (but are not limited to):

- Contribute to the development and/or create the following documentation in support of Device Security:
  a) Project Plan
  b) Project Charter
  c) Business Case
  d) Communications Plan
  e) Service Definition, Change Management Strategy/Plan and Implementation Strategy
  f) Procurement Strategy including: Request For Information (RFI), Request For Proposal (RFP), Statement of Work (SoW),
  g) Industry Day Information (i.e. Questions and Answers pertaining to Device Security, presentation)
  h) Security Assessment & Authorization Artifacts (Statement of Sensitivity, Concept of Operations, Threat Assessments).
- Develop and validate ITSG-33 security control profiles in support of various SSC back office projects related to the transformation of network perimeter security services;
- Create presentations and present to various stakeholders, and facilitate and record meetings and discussions as requested by the Technical Authority;
- Provide and document various security control profiles, reports, security analyses, work breakdown structures, schedules, and other related documents as requested by the Technical Authority.

Additional deliverables requirements for Enterprise Security Requirements Definition sub-Program (but are not limited to):

- Document requirements-gathering and security assurance input related to large scale Telecom and Converged Communications projects and possibly for other SSC Transformation Programs.
- Create and document service definitions for Telecom and Converged Communications-related projects, and possibly for other SSC Transformation Programs.
- Per ITSG-33 ISSIP security lifecycle process, determine and document related security controls based on GC, NIST and other guidance for input in to Enterprise architecture documents, RFP SOWs, and in order to fulfill the SA&A process. Input will be required commencing with the Concept phase and continuing through to the Installation phase.
- Perform and document Threat Assessments Reports.

5.1.5 C11 IT Security VA Specialist Level 3

The following responsibilities and scope of work under this contract include the following, but not limited to:

- Review, analyze, and/or apply:
  - Threat agents analysis tools and other emerging technologies including privacy enhancement, predictive analysis, VoIP, data visualization and fusion, wireless security devices, PBX and telephony firewall
  - War dialers, password crackers
  - Public Domain IT vulnerability advisory services
  - Network scanners and vulnerability analysis tools such as SATAN, ISS, Portscan & NMap
  - Networking Protocols (HTTP, FTP, Telnet)
  - Internet security protocols such as SSL, S-HTTP, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP, SNMP
  - Wireless Security
  - Intrusion detection systems, firewalls and content checkers
  - Host and network intrusion detection and prevention systems - Anti-virus management
- Identify threats to, and technical vulnerabilities of, networks
- Conduct on-site reviews and analysis of system security logs
- Collect, collate, analyze and disseminate public domain information related to networked computer threats and vulnerabilities, security incidents and incident responses
- Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings
- Completed tasks directly supporting the departmental IT Security and Cyber Protection Program
- Develop and deliver training material relevant to the resource category

5.1.6 C16 IT Security Specialist (Privacy) Level 3

The following responsibilities and scope of work under this contract include the following, but not limited to:

- The Privacy Specialist will analyze privacy concerns related to SSC Services, create and deliver privacy checklist documents for review and approval, perform Privacy Impact Assessments (PIAs) against SSC services and work on various documents in response to the Office of Privacy commissioner.
- The work performed needs to be done according to the following standards, policies documents and best practices:
  - Privacy Act and related provincial legislation;
  - Office of Privacy Commissioner Expectations on completing Privacy Impact Assessments (PIAs);
  - Latest TBS Directive on Privacy Impact Assessments (PIA) (Treasury Board Core Privacy Impact Assessment (PIA) template);
  - CSA's Model Code for the Protection of Personal Information (Q830);
  - Records Management.
- The resource is required to have extensive knowledge of the GC standards, policies and guidelines.
- The resource should be certified in the field of IT Privacy, preferably through an industry recognized certification body.
- Must analyses privacy concerns related to SSC services;
- Must create and deliver of privacy checklist document for review and approval;

- Must perform Privacy Impact Assessments (PIA) against SSC services while consulting with the Program area and Access to Information and Privacy (ATIP);
- Must create and update (as required) presentations, briefing notes, responses to letters from the Office of Privacy Commissioner OPC, related to Privacy Impact Assessments (PIA) performed or in progress.
- Must assist with and review Privacy Impact Assessment (PIA) related activities pursuant to the new TBS Directive on Privacy Impact Assessments, and related policies and instruments (standards, processes, guidelines, and procedures);
- Must assess privacy risks and propose mitigation mechanisms or strategies;
- Must review project documentation where available and/or applicable including demonstration(s), data flow diagrams and presentation materials;
- Must initiate and participate in discussions regarding privacy issues;
- Must meet with Office of Privacy Commissioner (OPC) to discuss elements of the Privacy Impact Assessment (PIA) and issue record of decision for each meeting. Follow-up on any action items identified;
- Must accept, review and respond to questions from departmental stakeholders prior to producing the final Privacy Impact Assessment (PIA) report(s);
- Must follow-up on further information requirements; discuss privacy and policy risks that may be identified during analysis;
- Must review project documentation related to IT issues, technologies and architecture influencing privacy risks;
- Must report on compliance with policies and related instruments (e.g., directives, standards, processes, guidelines, and procedures);
- Must produce final draft Privacy Impact Assessment (PIA) reports within a sufficient timeframe to allow ample opportunity to review findings with all stakeholders including ATIP;
- Must finalize Privacy Impact Assessments (PIAs)and briefing notes;

6.0 Deliverables

- The actual requirements for resources will be identified on an “as-and-when-requested” basis through an approval Task Authorization (TA).
- In addition to the services described in each resource category, while performing the Work each resource must provide to or a representative of a GC entity technical advice and the transfer of functional knowledge through the provision of written documents and individual and group training.
- The Contractor must provide the deliverables (in draft, final or both forms) to the Technical Authority or their representative as specified in each Task Authorization (TA). The scope and specific content of each deliverable will be submitted to the Technical Authority for review and to determine acceptance.
- The final copies of the deliverables must incorporate the comments received and changes requested by the Technical Authority or their representative and will be delivered on or before the end date specified in each TA.
- Each resource must submit a weekly status report to the Technical Authority conforming to the report format specified in each TA.
- The schedule, format and content of each deliverable shall be mutually agreed to by the Task Authorization (TA) and the Contractor in writing and will be based on the Task Authorization TA’s organizational standards (e.g. business requirement template to be used, standard architecture format for business views, etc.).
- Documentation deliverables shall be in hard copy format and electronic copy format using Microsoft (MS) Office suite of products, or agreed by the contractor and the Technical Authority in the event other format would be suitable.

- Progress (Status) Report. The Contractor shall prepare a written status and progress report on the work performed for the project, which is to be attached to the monthly timesheet claim. At a minimum, progress reports shall contain the following information:
    - All significant activities performed by the Contractor(s) during the period,
    - Status of all action/decision items, as well as a list of outstanding activities,
    - A description of any problems encountered which are likely to require the attention of the Technical Authority, and any recommendations relating to the conduct of the work.
    - Current milestones with planned dates, progress since last report, issues encountered, and next steps.
    - Hours expended by the contractor against the task during the reporting period.
    - Highlight the expectations/deliverables for the coming month, week, quarter.
- Progress report and timesheet must also be included when sending the invoice.

7. Format of Deliverables

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

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

Deliverables must be editable in Microsoft Office Suite (e.g., Word, Excel, PowerPoint and Visio) version 2007 or newer.

8. Regular Meetings

The Contractor's Project Authority must meet with the Technical Authority or their representative on a priority basis or as requested to discuss any issues associated with the provision of the required Informatics Professional Services. These meetings will be at no additional cost.

9. Service Levels

9.1 Normal Working Hours

Normal working hours will be no earlier than 7:00 am to no later than 6:00 pm EST Monday through Friday (with the exception of statutory holidays as defined by the province of work). The Contractor will be expected to work 7.5 hours/day within normal working hours, unless arrangements are made ahead of time with the Technical Authority. The Technical Authority will authorize additional hours of work in advance at the same rate as normal office hours. The Contractor will normally work during regular business hours, on site, unless otherwise agreed upon by the Contractor and the Technical Authority. For the duration of the contract all personnel must be available to work outside normal office hours as required.

9.2 Work location

The contractor's work will be performed on-site at Shared Services Canada or off-site (at the discretion of the Technical Authority/Manager). Shared Services Canada is located within the National Capital Region and access to IT systems and infrastructure will be made available as required. Over the duration of the Contract, the main location of

business of SSC's various locations or Branches may change but will remain in the National Capital Region (NCR), and no costs will be paid by SSC to the Contractor to compensate for any costs associated with such transition. The contractor is required to attend meetings at Shared Services Canada and at Key GC Stakeholders, but no significant travel will be required. All expenses for travel within the NCR are to be paid by the Contractor.

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

9.3 Travel Requirement

There is no travel requirement expected to conduct the Statement of Work. However, if travel is deemed necessary, Travel and Living expenses will only apply when the Contractor is requested to work outside the National Capital Region. If required, the Project Authority must authorize travel in advance, in writing.

Invoices for Travel and Living costs are to be supported by documentation (receipts) and will be reimbursed in accordance with the Treasury Board Policy and Guidelines on Travel in effect at the time of travel at actual cost with no allowance for mark-up or profit. Charges for air travel shall not exceed that for economy travel.

9.4 Reporting Relationship

The resource will functionally report to the Technical Authority/Manager.

10. Security Requirement

The resource must be cleared to a minimum of Secret throughout the course of the contract. Bidder must specify security clearance file number and expiration date.

11. Non-Disclosure

All work carried out by the contractor with respect to this Statement of Work will remain the property of the Crown. All reports, documentation, and extensions thereto shall remain the property of the Crown and the contractor shall not divulge, disseminate or reproduce such reports and/or documentation to any other person without the prior written permission of the Crown.

12. Proprietary Information

All information and documents made available to the contractor during the course of this project are deemed proprietary, and shall be returned to the Crown upon completion of the tasks specified in this Statement of Work or upon termination of the contract.

13. Interpretation

In the case of disputes regarding interpretation of statement of this Statement of Work or any of the terminology contained herein, the ruling of the Technical Authority shall prevail.

Appendix A to Annex A

Mandatory and Rated Requirements for the Task Solicitation Process

1.0 General Information

1.1 All work to be completed pursuant to this Contract will be authorized under the process detailed in Contract article 6.2.

1.2 In accordance with Task Solicitation of the Contract, the Contractor will be asked to submit resumes for each of the resources they propose to work on a Task Authorization (TA) requested by Canada.

1.3 The resource will be evaluated by the Technical Authority against the mandatory and rated requirements contained in the task authorization.

1.4 To be awarded an approved Task Authorization, the proposed Contractor resource must meet all of the mandatory requirements, and receive the highest score on the rated requirements.

2.0 Mandatory Requirements

3.1 The following are the mandatory requirements which will be used to evaluate each proposed resource in the relevant resource category of the TA:

3.1.1 Business Analyst Level III

Criteria	Mandatory Requirement	Demonstrated Experience	Project #
M1	A minimum of a three year college diploma(computer science or other IT related field; **OR** a university degree at the Bachelor level in Information Technology (computer science or engineering) or other IT related field; **OR** A minimum of **fifteen years** (in the last 20 years) in designing and/or implementing data center and/or telecommunication and/or network security solutions.		
M2	The Bidder must clearly substantiate that the proposed resource(s) have at minimum of ten(10) years' experience working as a Business Analyst performing 70% of tasks similar to those specified in the SOW.		
M3	Must hold a minimum of a valid Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

3.1.2 IT Strategic Security Planning & Protection Specialist Level III

Criteria	Mandatory Requirement	Demonstrated Experience	Project #
M1	A minimum of a three year college diploma(computer science or other IT related field; **OR** a university degree at the Bachelor level in Information Technology (computer science or engineering) or other IT related field; **OR** A minimum of **fifteen years** (in the last 20 years) in designing and/or implementing data center and/or telecommunication and/or network		

	security solutions.		
M2	The Bidder must clearly substantiate that the proposed resource(s) have at minimum of ten(10) years' experience working as a Security Planning & Protection Specialist performing 70% of tasks similar to those specified in the SOW.		
M3	Must hold a valid Security Clearance issued by PWGSC CISD at Top Secret and provide both file number and expiry date.		

3.1.3 IT Security Design Specialist Level III

Criteria	**Mandatory Requirement**	**Demonstrated Experience**	**Project #**
M1	A minimum of a three year college diploma(computer science or other IT related field; **OR** a university degree at the Bachelor level in Information Technology (computer science or engineering) or other IT related field; **OR** A minimum of **fifteen years** (in the last 20 years) in designing and/or implementing data center and/or telecommunication and/or network security solutions.		
M2	The Bidder must clearly substantiate that the proposed resource(s) have at minimum of ten(10) years' experience working as a Security Design Specialist performing 70% of tasks similar to those specified in the attached SOW.		
M3	Must clearly demonstrate experience for three (3) projects in the last 4 years developing documents including but not limited to: IT Security product and/or service descriptions, presentations, strategies and roadmaps. *To meet this requirement, the substantiated experience must include acquired experience focused on IT Security service delivery that needs to meet Communication Security Establishment Canada directives and guideline publications.* *A minimum of 4 months experience per project is required in any given area claimed for the experience to be considered.*		
M4	Must hold a minimum of a valid Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

3.1.4 IT Security VA Specialist Level III

Criteria	***Mandatory Requirement***	***Demonstrated Experience***	***Project #***

M1	A minimum of a three year college diploma(computer science or other IT related field; **OR** a university degree at the Bachelor level in Information Technology (computer science or engineering) or other IT related field; **OR** A minimum of **fifteen years** (in the last 20 years) in designing and/or implementing data center and/or telecommunication and/or network security solutions.		
M2	The Bidder must clearly substantiate that the proposed resource(s) have at minimum of ten(10) years' experience working as a Security VA Specialist performing 70% of tasks similar to those specified in the attached SOW. Experience must include at least five(5) Projects within the past three (3) years *A minimum of 4 months experience per project is required in any given area claimed for the experience to be considered.*		
M3	Must hold a minimum of a valid Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

3.1.5 IT TRA and C&A Specialist Level III

Criteria	**Mandatory Requirement**	**Demonstrated Experience**	**Project #**
M1	A minimum of a three year college diploma(computer science or other IT related field; **OR** a university degree at the Bachelor level in Information Technology (computer science or engineering) or other IT related field; **OR** A minimum of **fifteen years** (in the last 20 years) in designing and/or implementing data center and/or telecommunication and/or network security solutions.		
M2	The Bidder must clearly substantiate that the proposed resource(s) has experience as an TRA & C&A/SA&A Specialist for at least two (2) years within the past five (5) years undertaking at least 70% of SOW tasks, developing interpreting and applying IT C&A/SA&A methodology, policies instruments within a large organization. *To substantiate this mandatory requirement, the resource must include experience acquired and focused on an IT Security contract.*		
M3	The Bidder must clearly substantiate that the proposed resource(s) show they have experience using the following: • ITSG-33, NIST SP800-53, ISO/IEC 27001, or COBIT for risk management and security controls • Harmonized TRA Methodology (HTRA) • ITSG-22 and/or ITSG-38 for security zones • Policy on Government Security (PGS) / GSP, • The Management of Information Technology Security (MITS) Standard. *Experience must include at least five(5) Projects within the past three (3) years* *A minimum of 4 months experience per project is required in any given area claimed for the experience to be considered.*		
M4	Must hold a minimum of a valid Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

3.1.6 IT Privacy Specialist Level III

Criteria	Mandatory Requirement	Demonstrated Experience	Project #
M1	A minimum of a three year college diploma(computer science or other IT related field; **OR** a university degree at the Bachelor level in Information Technology (computer science or engineering) or other IT related field; **OR** A minimum of **fifteen years** (in the last 20 years) in designing and/or implementing data center and/or telecommunication and/or network security solutions.		
M2	The Bidder must clearly substantiate that the proposed resource(s) have at minimum of ten(10) years' experience working as a Privacy Specialist performing 70% of tasks similar to those specified in the attached SOW.		
M3	The Bidder must clearly substantiate that the proposed resource(s) show they have experience with the following: • Writing of Privacy Impact Assessments (PIAs) for IT Systems using the TBS PIA template or similar template. • Knowledge of the *Privacy Act* and the *Access to Information Act* • Knowledge of TBS Directive on Privacy Impact Assessment • Experience in engaging the Office of the Privacy Commissioner of Canada (OPC) on submitted PIAs and follow-up of OPC recommendations. • Experience writing briefing notes and executive summaries for PIAs on complex IT Systems. • Experience assessing level of residual privacy risk in IT Systems and suggesting mitigation measures. • Knowledge of current trends and issues in privacy such as: surveillance, data sovereignty, data matching, contracting to the private sector, enhanced identification methods and computer aided monitoring with audit trails. • Familiarity with departmental reporting obligations such as Personal Information Banks (PIBs) *Experience must include at least five(5) Projects within the past three (3) years* *A minimum of 4 months experience per project is required in any given area claimed for the experience to be considered.*		
M4	Must hold a minimum of a valid Top-Secret Security Clearance issued by PWGSC-CISD and provide both file number and expiry date.		

3.0 Point-Rated Requirements

3.1 The following examples are some, but not an exclusive list, of, the point-rated requirements which will be used to create evaluation grids for each proposed resource in the relevant resource category of the Task Solicitation process:

3.1.1 Business Analyst Level III

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	Must clearly demonstrate that the proposed resource has recent knowledge and experience in gathering, prioritizing, analyzing, and consolidating business requirements via interacting with the end users of one/multiple services and various project/program stakeholders	**10**	RATED POINT SCORE: • Less than 24 months = 0 points • 24 to 36 months = 4 points • 36 to 48 months = 6 points • 48 to 72 months = 8 points • 72 months and above = 10 points
R.2	Must clearly demonstrate that the proposed resource has recent work experience in identifying and documenting use cases associated with the business requirements.	**10**	RATED POINT SCORE: • Less than 24 months = 0 points • 24 to 36 months = 4 points • 36 to 48 months = 6 points • 48 to 72 months = 8 points • 72 months and above = 10 points
R.3	Must clearly demonstrate the proposed resource has recent knowledge and experience in identifying and documenting current state processes (business or operations).	**5**	RATED POINT SCORE: • Less than 24 months = 0 points • 24 to 36 months = 2 points • 36 to 48 months = 4 points • 48 months and above = 5 points
R.4	Must clearly demonstrate the proposed resource has recent work experience in developing financial analysis to support business cases and other management decisions.	**5**	RATED POINT SCORE: • Less than 24 months = 0 points • 24 to 36 months = 2 points • 36 to 48 months = 4 points • 48 months and above = 5 points
R.5	Must clearly demonstrate the proposed resource has recent work experience in (either developing business requirements or implementing) IT systems providing office automation applications, email, desktop, and network infrastructure services to users distributed across multiple sites.	**5**	RATED POINT SCORE: • Less than 24 months = 0 points • 24 to 36 months = 2 points • 36 to 48 months = 4 points • 48 months and above = 5 points
R.6	Must clearly demonstrate the proposed resource has recent work experience in (either developing business requirements or implementing) Secret Level-II and above IT systems providing office automation applications, email, desktop, and network infrastructure services to users distributed across multiple sites	**10**	RATED POINT SCORE: • Less than 12 months = 0 points • 12 to 24 months = 4 points • 24 to 36 months = 6 points • 36 to 48 months = 8 points • 48 months and above = 10 points
R.7	Must clearly demonstrate the proposed resource has work experience in developing presentations for stakeholders or senior executives.	**5**	RATED POINT SCORE: • Less than 24 months = 0 points • 24 to 48 months = 4 points • 48 months and above = 5 points

3.1.2 Strategic IT Security Planning and Protection Specialist Level III

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R. 1	Must clearly demonstrate the proposed resource has experience, within the last seven years, developing **security program-level strategy and/or operating models** for an enterprise wide or public sector organization with at least 3,000 employees. *Resource's project contribution is to have been Enterprise Wide[1], having had an impact over the majority of the organization* [1] Enterprise Wide: involving every Business Line or Sector within organization.	**20**	< 1 yr = 0 pts ≥ 1 yr < 3 yrs = 10 pts ≥ 3 yrs < 5 yrs = 15 pts ≥ 5 yrs = 20 pts
R.2	Must clearly demonstrate the proposed resource has experience, within the last seven years, developing **security roadmaps** for an enterprise wide or public sector organization with at least 3,000 employees. *Resource's project contribution is to have been Enterprise Wide[1], having had an impact over the majority of the organization* [1] Enterprise Wide: involving every Business Line or Sector within organization.	**20**	< 1 yr = 0 pts ≥ 1 yr < 3 yrs = 10 pts ≥ 3 yrs < 5 yrs = 15 pts ≥ 5 yrs = 20 pts
R.3	Must clearly demonstrate the proposed resource has experience, within the last seven years, conducting **security programmatic reviews/assessments** and providing recommended management action plan (MAP) remedial activities for an enterprise wide or public sector organization with at least 3,000 employees. *Resource's project contribution is to have been Enterprise Wide[1], having had an impact over the majority of the organization* [1] Enterprise Wide: involving every Business Line or Sector within organization.	**20**	< 1 yr = 0 pts ≥ 1 yr < 3 yrs = 10 pts ≥ 3 yrs < 5 yrs = 15 pts ≥ 5 yrs = 20 pts
R.4	Must clearly demonstrate the proposed resource has experience, within the last seven years, conducting **security organizational/functional reviews** for an enterprise wide or public sector organization with at least 3,000 employees. *Resource's project contribution is to have been Enterprise Wide[1], having had an impact over the majority of the organization* [1] Enterprise Wide: involving every Business Line or Sector within organization.	**20**	< 1 yr = 0 pts ≥ 1 yr < 3 yrs = 10 pts ≥ 3 yrs < 5 yrs = 15 pts ≥ 5 yrs = 20 pts
R.5	Must clearly demonstrate the proposed resource has experience, within the last seven years, developing **security**	**20**	< 1 yr = 0 pts ≥ 1 yr < 3 yrs = 10 pts ≥ 3 yrs < 5 yrs = 15 pts ≥ 5 yrs = 20 pts

	performance measurement frameworks for an enterprise wide or public sector organization with at least 3,000 employees. *Resource's project contribution is to have been Enterprise Wide[1], having had an impact over the majority of the organization* [1] Enterprise Wide: involving every Business Line or Sector within organization.		
R.6	Must clearly demonstrate the proposed resource has experience, within the last seven years, developing **rationalized security controls and compliance reporting frameworks** against myriad security requirements for an enterprise wide or public sector organization with at least 3,000 employees. *Resource's project contribution is to have been Enterprise Wide[1], having had an impact over the majority of the organization* [1] Enterprise Wide: involving every Business Line or Sector within organization.	**20**	< 1 yr = 0 pts ≥ 1 yr < 3 yrs = 10 pts ≥ 3 yrs < 5 yrs = 15 pts ≥ 5 yrs = 20 pts
R.7	The proposed resources hold current and valid certifications through industry recognized certification bodies in the one of the fields: CISSP - Certified Information Systems Security Professional CISM - Certified Information Security Manager CRISC - Certified in Risk and Information Systems Control SSCP - Systems Security Certified Professional CAP - Certification and Accreditation Professional CISA - Certified Information System Auditor SABSA - Sherwood Applied Business Security Architecture SCF - Sherwood Chartered Foundation SCP - Chartered Foundation Certificate (information security) SCM - Sherwood Chartered Master Open CA - Open Group Certified Architect Open CITS - Open Group Certified IT Specialist TOGAF - The Open Group Architecture Framework ABCP - Associate Business Continuity Professional CBCP - Certified Business Continuity Professional MBCP- Master Business Continuity Professional	**12**	2 points per certificates(maximum 6)

	CBCA - Certified Business Continuity Auditor CBCLA - Certified Business Continuity Lead Auditor APSCP - Associate Public Sector Continuity Professional CPSCP - Certified Public Sector Continuity Professional The Bidder must provide proof of certifications for the proposed resources.		
R8	The proposed resource holds a valid certification in Project Management by an organization with publically available training and certification. Example certifications are as follows: PMP - Project Management Professional Prince2 - (**Pr**ojects **In C**ontrolled **E**nvironments) Project Management Methodology The Bidder must provide proof of certifications for the proposed resources	**3**	

3.1.3 IT Security Design Specialist Level III

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	The proposed resource will receive points for each of the following certifications, to a maximum of 30 points: • Certified Information Systems Security Professional (CISSP) • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Information Security Management (ISO/IEC) • Certified in Risk and Information Systems Control (CRISC) • Information Technology Infrastructure Library (ITIL) • Certified Cyber Forensics Professional (CCFP) • Systems Security Certified Professional (SSCP) • Information Systems Security Architecture Professional (ISSAP) • The proposed resource is certified in Project Management by an organization with publically available training and certification. Some (not all) examples include: PMP, Prince2	**30**	5 points for each certification provided.

	• CAP (Certification and Accreditation Professional), • SSCP (Systems Security Certified Practitioner), • GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher • Microsoft Certified Architect (MCA) • Systems Security Certified Practitioner (SSCP) • Sherwood Applied Business Security Architecture (SABSA) • Certificate of Cloud Security Knowledge (CCSK) *Proof of certification must be provided.*		
R.2	Must clearly demonstrate recent (within last 5 years) minimum of 4 consecutive months experience per project in the last 4 years direct experience in the assessment or writing of formal Security Assessment (ITSG-33 based) or Certification reports. *To meet this rated requirement, the demonstrated experience must include acquired experience focused on IT Security service delivery that needs to meet Communication Security Establishment Canada directives and guideline publications.*	**20**	Up to a maximum of 5 projects totaling no more than 20 points: 4 points per project for Canadian federal government experience; 3 points per project for Canadian, provincial or municipal government experience; and 2 points per project for private sector experience.
R.3	Must clearly demonstrate the proposed resource recent (within last 5 years) minimum of 6 months project experience direct working knowledge of the GC standards, policies and guidelines and the principles of security and privacy by design. *To meet this rated requirement, the demonstrated experience must include acquired experience focused on IT Security service delivery that needs to meet Communication Security Establishment Canada directives and guideline publications.*	**20**	1 point for each policy, standard or guideline listed. **10 additional points** for demonstrating a working understanding of the security and privacy by design principle.
R.4	Recent (within last 5 years) direct experience developing the following documents: • Statement of Sensitivity, • Asset Categorization, • Threat modeling, • Business Needs for Security, • Statement of Acceptable Risk	**20**	2 point for each document demonstrated by project
R.5	Validation of the following: • IT security controls (ITSG33 based) and applicable safeguards; • Assessment of mitigation strategies;	**10**	1 point for each demonstrated document.

	• Assessment of residual risk.		
R6	Must clearly demonstrate the proposed resource must have at least two (2) years within the last five (5) years working as a TRA Analyst with experience developing and updating TRAs for IT Systems* other than in house developed software solutions. Clearly demonstrate the proposed resource have recent knowledge and experience in authoring a minimum of 2 TRAs for IT Systems using the Harmonized Threat and Risk Assessment (HTRA) methodology	**25**	5 points for each TRA (max 3) clearly identified. 10 additional points for demonstrating authoring two (2) TRA's using Harmonized Threat and Risk Assessment (HTRA) methodology
R7	Must clearly demonstrate the proposed resource has experience applying GC IT Security policies	**10**	Points will be awarded for experience demonstrated in the following manner: 120 to 132 months = 2 points >132 to 144 months = 4 points >144 to 156 months = 6 points >156 to 168 months = 8 points >168 months = 10 points
R.8	Must clearly demonstrate the proposed resource has experience performing the following IT Security tasks: • Analysis of IT Security tools and techniques • Analysis of security data and provision of advisories and reports • Preparation of technical reports such as requirement analysis, options analysis, technical architecture documents, mathematical risk modeling • Security architecture design and engineering support	**10**	Points will be awarded for experience demonstrated in the following manner: 24 to 30 months = 2 points >30 to 36 months = 4 points >36 to 42 months = 6 points >32 to 48 months = 8 points >48 months = 10 points
R.9	Must clearly demonstrate a minimum of 4 consecutive experience per project within the last 4 years, preparing briefings for, and making presentations to team leads/managers, equivalent to the Canadian Government EX1 level and above *Equivalent to the Canadian Government EX1 level is defined as a GC CS5 and above and multi-project Director in the private sector.* *To meet this rated requirement, the demonstrated experience must include acquired experience focused on IT Security service delivery that needs to meet Communication Security Establishment Canada directives and guideline publications.*	**20**	Up to a maximum of 5 projects totaling no more than 20 points, 4 points per project.

R.10	Must clearly demonstrate the proposed resource within the past five years, in the following areas: • X.500 Directory Standards; • LDAP; • MS operating systems; • Unix operating systems; • Linux operating systems; • z/OS operating systems; • Networking Protocols (HTTP, FTP, Telnet); • Internet security protocols (SSL, S-HTTP, S-MIME, IPSec, SSH); • Wireless Security; • TCP/IP, UDP, DNS, SMTP; • Intrusion detection systems and firewalls; and • Approved GoC Cryptographic Algorithms. *Evaluation will consider specific experience for each of the above in terms of work performed and months of experience gained in the past five years*.	**10**	One point per list item and experience up to a maximum of 10 points
R11	Must clearly demonstrate the proposed resource has project experience applying IT Security policies A minimum of 4 consecutive months experience per project is required in any given area claimed for the experience to be considered	**20**	RATED POINT SCORE: Up to a maximum of 5 projects totaling no more than 20 points: • 4 points per project for Canadian federal government experience; • 3 points per project for Canadian, provincial or • municipal government experience; and • 2 points per project for private sector experience.

3.1.4 IT Security VA Specialist Level III

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	The proposed resources hold current and valid certifications through industry recognized certification bodies such as: • CISA - Certified Information System Auditor • C|PEH - Certified Professional Ethical Hacker • CRISC - Certified in Risk and Information Systems Control • GCIA - Certified Intrusion Analyst • GCIH - Certified Incident Handler • GPEN – Certified Penetration Tester • GWAPT - Web Application Penetration Tester • GXPN – Certified Exploit Researcher and Advanced Penetration Tester • OWASP – Open Web Application Security Project • Other recognized Vulnerability Management certification. The Bidder must provide proof of certifications for the proposed resources.	**30**	5 points for each certification provided.
R.2	Must clearly demonstrate recent (within last 2 years) minimum of 2 consecutive months experience per project direct experience conducting end-to-end Technical Vulnerability assessments. End-to-End consists of: A. Establish a vulnerability assessment plan. B. Run a VA scan. C. Collect, draft, and submit the VA findings report to the various stakeholders. (i.e. System administrator, SA&A) D. Meet with various stakeholders and provide guidance on how to proceed. E. Provide final recommendation reports.	**20**	**4 points** per project If project is consecutive 6 months+: **10 points**

R.3	Must clearly demonstrate experience in the last 10 years in: A. Identifying security vulnerabilities. B. Providing guidance or recommendation for revisions and adjustments of security posture of systems or services. C. Active participation in improving security processes and security controls.	**30**	Maximum of 5 projects. Maximum 6 points per project. 2 points for each A., B., C. for a possibility of 6 points per project.
R.4	Must clearly demonstrate recent (within last 5 years) exposure and/or participation to server hardening processes.	**10**	10 points for 5yrs+ 5 points for 3yrs+ 2 points for 1yr+
R.5	Must demonstrate extensive (5 years+) experience in Vulnerability Assessment reporting	**10**	10 points for 10yrs+ 7 points for 7yrs+ 5 points for 5yrs+
R.6	Must indicate conducting research or audits for the purpose of gathering evidence for Vulnerability Assessment of systems. Interviews/Audits may be a combination of physical review, documented review as well as interviews with personnel who participated in the establishment of the systems security postures.	**10**	10 points for 10yrs+ 7 points for 7yrs+ 5 points for 5yrs+ 1 point per year under 5 yrs

3.1.5 IT TRA and C&A Specialist Level III

Criteria	Point-Rated Criteria	Max Points	Evaluation Criteria
R.1	The proposed resource will receive points for each of the following certifications, to a maximum of 30 points: • Certified Information Systems Security Professional • Certified Information Security Manager (CISM) • Certified Information Systems Auditor (CISA) • Information Security Management (ISO/IEC) • Certified in Risk and Information Systems Control (CRISC) • Information Technology Infrastructure Library (ITIL) • Systems Security Certified Professional (SSCP) • Information Systems Security Architecture Professional (ISSAP) • CAP (Certification and Accreditation Professional), • SSCP (Systems Security Certified Practitioner),	**30**	10 points for CISSP (ISC2) 5 points for each certification provided.

	• GIAC (Global Information Assurance Certification) • SABSA Chartered Security Architect Foundation (SCF) or higher • Systems Security Certified Practitioner (SSCP) • Security Architecture (SABSA) • • Privacy Certifications • Certified Information Privacy Professional/Information Technology (CIPP/IT) • Certified Information Privacy Professional/Canada (CIPP/C) • Other recognized privacy certification. *Proof of certification must be provided.*		
R.2	Must clearly demonstrate recent (within last 5 years) minimum of 4 consecutive months experience per project in the last 4 years direct experience in the assessment of evidence and writing of formal Security Assessment reports(ITSG-33 based). *To meet this rated requirement, the demonstrated experience must include acquired experience focused on IT Security service delivery that needs to meet Communication Security Establishment Canada directives and guideline publications.*	**20**	Up to a maximum of 5 projects totaling no more than 20 points: 4 points per project for Canadian federal government experience; 3 points per project for Canadian Territorial , provincial or municipal government experience; and 2 points per project for private sector experience.
R.3	Must clearly demonstrate the proposed resource recently (within last 5 years) has a minimum of 6 months project experience direct working knowledge of the GC standards, policies and guidelines and the principles of security and privacy by design. *To meet this rated requirement, the demonstrated experience must include acquired experience focused on IT Security service delivery that needs to meet Communication Security Establishment Canada directives and guideline publications.*	**20**	1 point for each project where policies, standards or guidelines were used. Please provide a detatailed liste and how the policy was used. **10 additional points** for demonstrating a working understanding of the security and privacy by design principle.
R.4	Recent (within last 5 years) direct experience reviewing the following documents: • Statement of Sensitivity, • Statement of acceptable risk • Asset Categorization, • Threat modeling, • Business Needs for Security, • Statement of Acceptable Risk	**20**	2 point for each document demonstrated by project
R.5	Development of the following: • IT security controls (ITSG33 based) and applicable safeguards;(based on business requirements)	**10**	1 point for each demonstrated document.

	• Assessment of mitigation strategies; • Identification of residual risk.		
R.6	Must clearly demonstrate the proposed resource must have at least two (2) years within the last five (5) years working as a TRA Analyst with experience developing and updating TRAs for IT SSC mandated services.(infrastructure, OS, etc..) Clearly demonstrate the proposed resource have recent knowledge and experience in authoring a minimum of 2 TRAs for IT Systems using the Harmonized Threat and Risk Assessment (HTRA) methodology	**25**	5 points for each TRA (max 3) clearly identified. 10 additional points for demonstrating authoring two (2) TRA's using Harmonized Threat and Risk Assessment (HTRA) methodology
R.7	Must clearly demonstrate the proposed resource has experience understanding and applying GC IT Security policies	**10**	Points will be awarded for experience demonstrated in the following manner: 120 to 132 months = 2 points >132 to 144 months = 4 points >144 to 156 months = 6 points >156 to 168 months = 8 points >168 months = 10 points
R.8	Must clearly demonstrate the proposed resource has experience performing the following IT Security tasks: • review of Business requirements • development of security controls profile based on business requirements using CSE ITSG-33. • Preparation of security assessment reports. • Security architecture design and engineering support	**10**	Points will be awarded for experience demonstrated in the following manner: 24 to 30 months = 2 points >30 to 36 months = 4 points >36 to 42 months = 6 points >32 to 48 months = 8 points >48 months = 10 points

Annex 'B'

BASIS OF PAYMENT

1. Professional Services

The Contractor will be paid in accordance with the Contract and the following Basis of Payment for Work performed pursuant to this Contract.

For the provision of Informatics Professional Services as described in Annex A - Statement of Work, the Contractor shall be paid the all inclusive firm daily rate(s) below in the performance of this Contract, HST extra.

FOR THE INITIAL CONTRACT PERIOD (1 YEAR)	
Category of Personnel	**Firm Per Diem Rate**
Business System Class	
Business Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

FOR THE OPTION YEAR 1 (1 YEAR)	
Category of Personnel	**Firm Per Diem Rate**
Business System Class	
Business Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

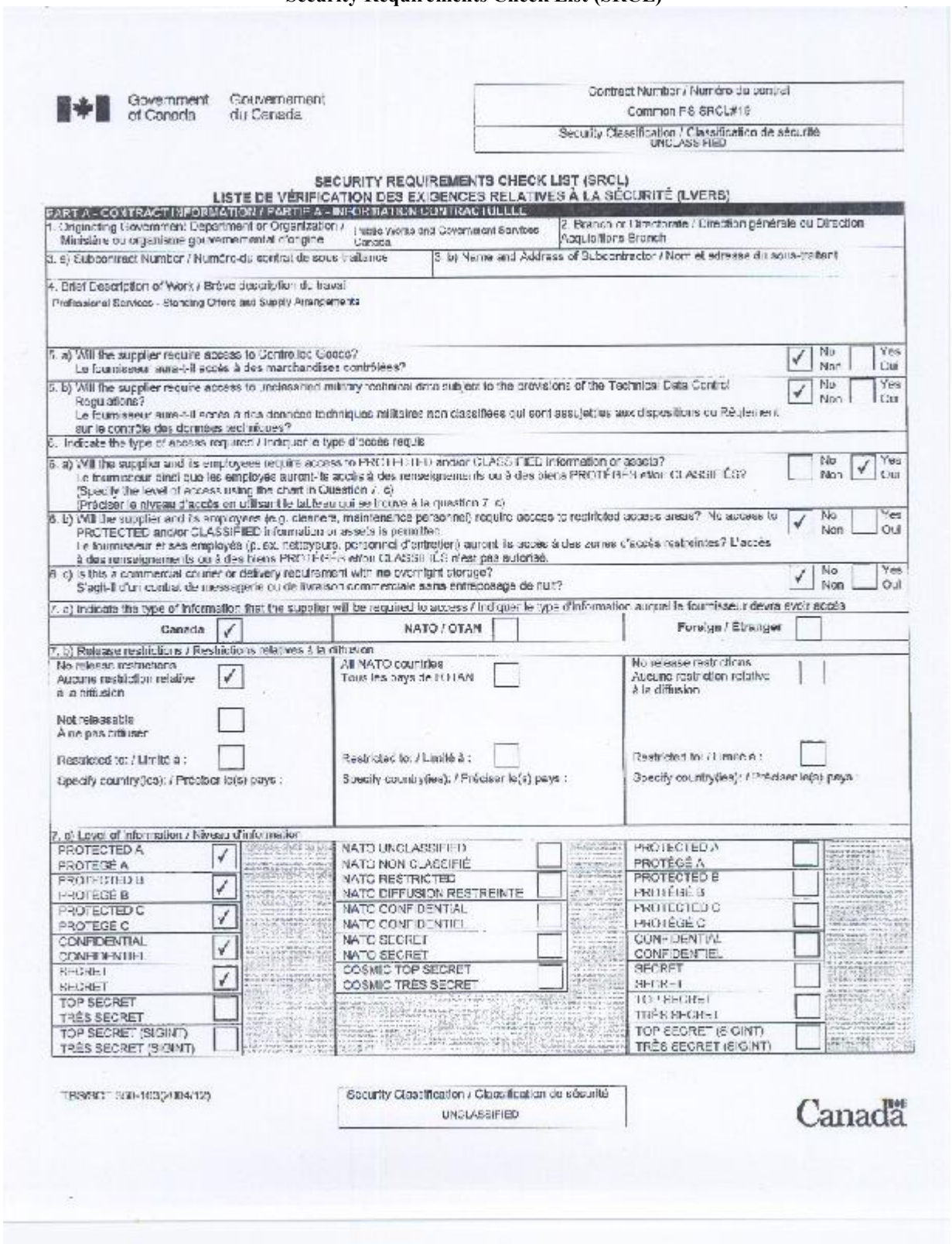
FOR THE OPTION YEAR 2 (1 YEAR)	
Category of Personnel	**Firm Per Diem Rate**
Business System Class	
Business Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

2.0 Taxes

(a) All prices and amounts of money in the contract are exclusive of Harmonized Sales Tax (HST), unless otherwise indicated. The HST is extra to the price herein and will be paid by Canada.

(b) The estimated HST of **$*<To Be Inserted at Contract Award>*** is included in the total estimated cost shown on page 1 of this Contract. The estimated HST to the extent applicable will be incorporated into all invoices and progress claims and shown as a separate item on invoices and progress claims. All items that are zero-rated, exempt, or to which the HST does not apply, are to be identified as such on all invoices. The Contractor agrees to remit to Canada Revenue Agency (CRA) any amounts of HST paid or due.

Annex C
Security Requirements Check List (SRCL)



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Common PS SRCL#16
Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Public Works and Government Services Canada
2. Branch or Directorate / Direction générale ou Direction: Acquisitions Branch
3. a) Subcontract Number / Numéro du contrat de sous-traitance
3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
4. Brief Description of Work / Brève description du travail: Professional Services - Standing Offers and Supply Arrangements
5. a) Will the supplier require access to Controlled Goods? / Le fournisseur aura-t-il accès à des marchandises contrôlées? — No / Non ☑ — Yes / Oui ☐
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? / Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? — No / Non ☑ — Yes / Oui ☐
6. Indicate the type of access required / Indiquer le type d'accès requis
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? / Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) / (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)) — No / Non ☐ — Yes / Oui ☑
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. / Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. — No / Non ☑ — Yes / Oui ☐
6. c) Is this a commercial courier or delivery requirement with no overnight storage? / S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? — No / Non ☑ — Yes / Oui ☐
7. c) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information			
PROTECTED A / PROTÉGÉ A	☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	☐
PROTECTED B / PROTÉGÉ B	☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	☐
PROTECTED C / PROTÉGÉ C	☑	NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐
CONFIDENTIAL / CONFIDENTIEL	☑	NATO SECRET / NATO SECRET	☐
SECRET / SECRET	☑	COSMIC TOP SECRET / COSMIC TRÈS SECRET	☐
TOP SECRET / TRÈS SECRET	☐		
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	☐		

PROTECTED A / PROTÉGÉ A	☐
PROTECTED B / PROTÉGÉ B	☐
PROTECTED C / PROTÉGÉ C	☐
CONFIDENTIAL / CONFIDENTIEL	☐
SECRET / SECRET	☐
TOP SECRET / TRÈS SECRET	☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)	☐

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
UNCLASSIFIED

Canada

ATTACHMENT 1 TO PART 4
Evaluation Criteria

1. Evaluation Disclaimer

The mandatory criteria will be evaluated on a "Met/Not Met" (i.e. compliant/non-compliant) basis. Proposals **must** demonstrate compliance with all of the following Mandatory requirements and must provide the necessary documentation to support a determination of compliance. Proposals that fail to meet any mandatory requirements will be deemed non-compliant and will be given no further consideration.

The Contracting Authority reserves the right to request reference(s)* from any of the SA Holder's listed projects to verify and validate the information stated in the proposal. If the reference is unable to verify or validate the information stated in the proposal, the bid will be deemed non-compliant.

2. Customer Reference Contact Information

The Bidder must provide customer references for point rated requirements R2 and R3 who must each confirm, the facts identified in the Bidder's bid. 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. Bidders are also requested to include the title of the contact person. If the named individual is unavailable when required during the evaluation period, the Bidder may provide the name and contact information of an alternate contact from the same customer.

Canada is not obliged to, but may in its discretion contact the Primary reference and, where applicable, the Backup reference, in order to validate the information submitted for point rated requirements R2 and R3. Canada may conduct any Project Reference validation check in writing by e-mail. Canada will email (cc) the Respondent's contact when an e-mail is sent out for Project Reference validation checks.

If Canada chooses to contact one or more references to validate information provided by a Bidder, Canada must receive the reference's response within 5 Federal Government Working Days (FGWDs) from the date of the request. If Canada does not receive confirmation (within 5 FGWDs) from either the Primary or Backup reference that the information in their bid is accurate (or that any inaccuracies are not material to whether or not the project meets the mandatory requirements), that Bidders Project Reference will not be considered in the evaluation. Canada may also contact a Primary or Backup reference for clarification purposes, either by email or by telephone.

If during a bid validation by Canada it becomes apparent that the address, telephone number, or email address for any of the references is incorrect or missing, the Bidder will be permitted to provide the correct address, telephone number, or email address within 1 FGWD of a request. If the named individual for the Primary reference is unavailable because they are on leave, or no longer working for that organization, Canada will contact the Backup reference from the same customer organization.

The Bidder will not be permitted to submit an alternate customer organization or project as a reference for the RFP after the bid closing date.

3. Mandatory Criteria

<table>
<tr><th colspan="5">Corporate Mandatory Requirement</th></tr>
<tr><th>Criteria</th><th>Mandatory Requirement</th><th colspan="3">Bidders Response</th></tr>
<tr><th></th><th></th><th>Met</th><th>Not Met</th><th>Reference to Additional Documentation within the Bid</th></tr>
<tr><td>M1</td><td>The Bidder must have demonstrated contract experience in supplying all of the following resource categories, for the required Mandatory Billable Days per category.

<table>
<tr><th>Category of Personnel</th><th>Mandatory Minimum Number of Billable Days</th></tr>
<tr><td>Business Analyst</td><td>1600</td></tr>
<tr><td>IT Strategic Security Planning and Protection Specialist</td><td>1000</td></tr>
<tr><td>IT TRA & C&A Specialist</td><td>1800</td></tr>
<tr><td>IT Security Design Specialist</td><td>2000</td></tr>
<tr><td>IT Security VA Specialist</td><td>600</td></tr>
<tr><td>IT Privacy Specialist</td><td>600</td></tr>
</table>

Bidders must complete Appendix A, B and C to Part 4.

The services provided must have been provided under a maximum of five contracts. It is not necessary for each contract to demonstrate all categories of personnel. Referenced contracts must have an excess (“Billed”) value in excess of $1M.

The experience must occur within the past five years prior to the RFP closing date. The experience may occur at any time during the five year period, so long as the-total number of Billable Days when added together meets the Minimum Billable Days requirement.

The work delivered by the Category of Personnel must include at least 70% of the associated tasks listed in the Statement of Work of this bid solicitation for that Category of Personnel.</td><td></td><td></td><td></td></tr>
</table>

This page has been left intentionally blank.

4. Point-Rated Technical Criteria

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
R1	The Bidder should demonstrate its billable days experience in excess to the minimum billable days under M1. The Bidder's demonstrated "Total Billable Days" provided in response to M1 will be used to evaluate this criterion. **Example Evaluation Scenario:** The Bidder will be awarded points for billable days in excess of the	**100**		

	Billable DAYS			
	(A)	(B)	(C)	(D)
CATEGORY OF PERSONNEL	TOTAL BILL DAY PROVIDED BY BIDDER	MINIMUM DAYS REQUIRED UNDER M1	BIDDER EXCESS	BIDDERS % INCREASE TO A MAXIMUM 100 PTS
Business Analyst	2175	1600	575	35.94
IT Strategic Security Planning and Protection Specialist	1225	1000	225	22.5
IT TRA & C&A Specialist	4000	1800	2200	100.00
IT Security Design Specialist	3000	2200	800	36.36
IT Security VA Specialist	850	600	250	41.67
IT Privacy Specialist	800	600	200	33.33
BIDDER SCORE = SUM (D) / # of CATEGORIES				
Sum (D) / 6 = 44.97				

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
	minimums identified under M1 as demonstrated in the example evaluation scenario provided below. In this example the Bidder would score 44.97 points out of a possible 100 points. Bidders must complete Appendix A, B and C to Part 4			
R2	SSC believes that the most significant risk associated with this contract is that the Contractor will be unable to provide the required number of qualified resources, in the required categories/level, within the timeframe specified in the Task Solicitation process. Vendors should demonstrate their ability to supply, manage and retain large groups of resources in support of a single client/project within the region of delivery. Bidders should supply a single client contract with a contact reference within the past 12 to 24 months encompassing a minimum of 10 resources in the NCR in support of a single client project for a minimum six consecutive months To be considered, reference project information must include: • Client Organization Name • Client Contact name and Title • Client Contact Phone # • Client Contact Email Address • Project start and end dates (yy/mo) • Total number of PS resources provided within a fixed 6 months period within the last 12 months	**50**	• **10 points**- A team of 10 resources were provided to a single client in the NCR; • **25 points**- A team of 15 resources were provided to a single client in the NCR; • **35 points**- A team of 25 resources were provided to a single client in the NCR; • **50 points**- A team of 30, or more, resources were provided to a single client in the NCR.	
R3	The Bidder should describe its proposed Risk Mitigation strategy, including the approach and or measures it proposes to undertake, to ensure its ability to propose fully qualified resources to Shared Services	**150**	*The extent to which the proposed risk mitigation strategy is fully and clearly*	

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
	Canada (SSC) within 5 days of receipt of a TA Request. The Bidder's mitigation strategy should include current corporate processes, as well as specific measures it proposes to implement to manage the resulting contract. In addition, the Bidder must provide a single Reference Project where it has successfully used a similar/same approach to ensure the timely provision of qualified resources to the client. To be considered, the reference project information must include: • Client Organization Name • Client Contact Name and Title • Client Contact Phone Number • Client Contact Email Address • Project start and end dates (yy/mo) • A description of the approach and/or measures implemented to ensure the timely provision of qualified resources to the client		*described:* • **30 points:** The risk mitigation strategy is described; • **75 points:** The risk mitigation strategy is reasonably described with a good level of detail of existing corporate processes, • **100 points:** The risk mitigation strategy is thoroughly described, including complete details of existing supporting corporate processes and specific measures to be implemented. *Relevance of the proposed risk mitigation strategy to ensure the timely provision of qualified resources:* • **15 points**: Response proposes a risk mitigation strategy (i.e. methods and/or activities) that demonstrates a minimal understanding of the stated risk;	

Corporate Rated Requirements				
			Bidder's Response	
#	Rated Evaluation Criteria	Points Max	Demonstrated Experience	Reference to Extra Documentation Within The Bid
			• **25 points:** Response proposes a risk mitigation strategy (i.e. methods and/or activities) which demonstrates some understanding of the stated risk; • **35 points:** Response proposes a risk mitigation strategy (i.e. methods and/or activities) which demonstrates a good understanding of the stated risk; • **50 points:** Response proposes a risk mitigation strategy (i.e. methods and/or activities) which demonstrates a clear and profound understanding of the stated risk.	
	Maximum Points Available:	300		
	Minimum Score Required:	210		
	Bidder's Score:			

ATTACHMENT 2 TO PART 4
FINANCIAL EVALUATION OF PROPOSAL
(PRICING TABLE)

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

As a minimum, the Bidder must respond to this pricing schedule by inserting in its financial bid for each of the periods specified below its quoted firm all inclusive per diem rate (in CAD $) for each of the resource categories identified. Bidders must propose the same per diem rate for both resources.

FOR THE INITIAL CONTRACT PERIOD (1 YEAR)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Business System Class	
System Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

FOR THE OPTION YEAR 1 (1 YEAR)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Business System Class	
System Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

FOR THE OPTION YEAR 2 (1 YEAR)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Business System Class	
System Analyst - Level 3	
Cyber Protection Services Class	
IT Security Planning and Protection Specialist - Level 3	
IT TRA & C&A Specialist - Level 3	
IT Security Design Specialist - Level 3	
IT Security VA Specialist - Level 3	
IT Privacy Specialist - Level 3	

Taxes

(c) All prices and amounts of money in the contract are exclusive of Harmonized Sales Tax (HST), unless otherwise indicated. The HST is extra to the price herein and will be paid by Canada.

(d) The estimated HST of **$*<To Be Inserted at Contract Award>*** is included in the total estimated cost shown on page 1 of this Contract. The estimated HST to the extent applicable will be incorporated into all invoices and progress claims and shown as a separate item on invoices and progress claims. All items that are zero-rated, exempt, or to which the HST does not apply, are to be identified as such on all invoices. The Contractor agrees to remit to Canada Revenue Agency (CRA) any amounts of HST paid or due.

Attachment 1 to Part 3: Bid Submission Form

BID SUBMISSION FORM		
Bidder's full legal name **[*Note to Bidders: Bidders who are part of a corporate group should take care to identify the correct corporation as the Bidder*.]**		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	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 in Canada the bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Number of FTEs [Bidders are requested to indicate, the total number of full-time-equivalent positions that would be created and maintained by the bidder if it were awarded the Contract. This information is for information purposes only and will not be evaluated.]		
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 products 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		

APPENDIX A TO ATTACHMENT 1 TO PART 4

RFP BILLABLE DAYS RESPONSE TABLE

Bidder's Name:_____

Billing Period (24 consecutive months) between ___/___/___ to ___/___/___
(dd/mm/yy) (dd/mm/yy)

By providing a response, the bidder certifies that billable days provided occurred during the billing period indicated above for all of the resource categories listed.

RESOURCE CATEGORY	NUMBER OF BILLABLE DAYS					
	Cross Reference to Contract Reference # _____	Cross Reference to Contract Reference # _____	Cross Reference to Contract Reference # _____	Cross Reference to Contract Reference # _____	Cross Reference to Contract Reference # _____	Total

APPENDIX B TO ATTACHMENT 1 TO PART 4

RESOURCE PROJECT REFERENCE FORM

CONTRACT REFERENCE #: _____	
Bidder Name:	
CUSTOMER REFERENCE CONTACT INFORMATION	
Name of Organization:	Contact Name:
E-mail address:	Telephone number:
CONTRACT DETAILS	
Contract Title and description:	
Contract Start Date (mm/yy):	Contract End Date (mm/yy):
Total Billable Value (in dollars):	
RESOURCE DETAILS	
Category of Personnel and Level	**Tasks performed under the contract with a cross reference to each specific SOW associated task**

Annex D

TASK AUTHORIZATION (TA) AND ACCEPTANCE FORM

TASK AUTHORIZATION (TA) FORM					
CONTRACTOR		CONTRACT NUMBER:	EN869-101336/		
COMMITMENT #		FINANCIAL CODING:			
TASK NUMBER (AMENDMENT):		ISSUE DATE:	RESPONSE REQUIRED BY:		
1. STATEMENT OF WORK (WORK ACTIVITIES AND DELIVERABLES): SEE ATTACHED FOR STATEMENT OF WORK AND CERTIFICATIONS REQUIRED.					
2. PERIOD OF SERVICES:	FROM (DATE):	TO (DATE):			
3. WORK LOCATION:					
4. TRAVEL REQUIREMENTS:					
5. LANGUAGE REQUIREMENTS:					
6. OTHER CONDITIONS/CONSTRAINTS:					
7. LEVEL OF SECURITY CLEARANCE REQUIRED FOR THE CONTRACTOR' PERSONNEL:					
RESOURCE CATEGORY	NAME OF PROPOSED RESOURCE	PWGSC SECURITY FILE NUMBER	PER DIEM RATE	ESTIMATED # OF DAYS	TOTAL COST
				ESTIMATED COST	
				GST	
				TOTAL LABOUR COST	
				ESTIMATED TRAVEL COST (IN ACCORDANCE WITH TBS GUIDELINES)	
				TOTAL ESTIMATED COST	
8. SIGNING AUTHORITIES:					
Name, Title and Signature of Individual Authorized to Sign on Behalf of Contractor	Contractor (signature)	Date:			
Name, Title and Signature of Individual Authorized to Sign on Behalf of SSC (Technical Authority)	SSC Technical Authority (signature)	Date:			
Name, Title and Signature of Individual Authorized to Sign on Behalf of SSC Procurement	SSC Contracting Authority (signature)	Date:			
You are requested to sell to her Majesty The Queen in Right of Canada, in accordance with the terms and conditions set out herein, referred to herein, or attached hereto, the services listed herein and in any attached sheets at the price set out thereof.					