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

VARIOUS LEVEL 3 RESOURCES FOR IT OPERATION SUPPORT

TABLE OF CONTENTS

PART 7 - RESULTING CONTRACT CLAUSES

LIST OF ANNEXES TO THE RESULTING CONTRACT:

LIST OF ATTACHMENTS TO PART 3 (BID PREPARATION INSTRUCTIONS):

LIST OF ATTACHMENTS TO PART 4
(EVALUATION PROCEDURES AND BASIS OF SELECTION):

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

VARIOUS LEVEL 3 RESOURCES FOR OPERATION SUPPORT

GENERAL INFORMATION

1.1 INTRODUCTION

The bid solicitation 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 Certifications: includes the certifications to be provided;

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

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

The Annexes include the Statement of Work, the Basis of Payment and the Security Requirements Checklist.

1.2 Summary

a) 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.

b) It is intended to award up to a maximum of four contract(s) each for an initial period of two years plus two one year irrevocable option allowing Canada to extend the term of the contract. For the life of the awarded contracts no single contract holder will be permitted to exceed $20M in awarded Task Authorizations..

c) 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.

d) 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.

e) The following Category of Personnel will be 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)
B.13	Operations Support Specialist	3	40
C.6	IT Security Engineer	3	15
C.7	IT Security Incident Management Specialist	3	15

NOTE : This solicitation is raised for Level 3 resources, however SSC may also require occasion Level 1 and Level 2 resources. In order to standardize any Resulting Contract(s), the firm per diem rate from the financial bid provided by Bidders for Level 3 resources will be used to determine the firm per diems for Level 1 and Level 2 resources as follows :

- ***Level 1 Firm Per Diem rate : 70% of Contractor's Level 3 rate***
- ***Level 2 Firm Per Diem rate : 80% of Contractor's Level 3 rate***

f) 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.

g) 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 COMMUNICATIONS NOTIFICATION

As a courtesy, the Government of Canada requests that successful Bidders notify the Contracting Authority in advance of their intention to make public an announcement related to the award of a contract.

1.4 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.

1.5 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.

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 (2014-09-14) 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

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.

2.3 Enquiries – Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than seven (7) 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.

2.4 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.

Note to Bidders: Bidders are requested to indicate the Canadian province or territory they wish to apply to any resulting contract in their Bid Submission Form

2.5 Improvement of Requirement during Solicitation Period

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

2.6 Volumetric Data

The Total Estimated # of Resources Required (per year) data has been provided to Bidders to assist them in preparing their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of number of resources per year will be consistent with this data. It is provided purely for information purposes.

PART 3- BID PREPARATION INSTRUCTIONS

3.1 BID PREPARATION INSTRUCTIONS

a) Canada requests that bidders provide their bid in separately bound sections as follows:

(i) Section I: Technical Bid (3 hard copies and 4 soft copies on CD's or DVD's)

(ii) Section II: Financial Bid (1 hard copy and 1 soft copy on CD and DVD)
(iii) Section III: Certifications (1 hard copy and 1 soft copy on CD and DVD)

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

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.

Multiple bids from the same Bidder (or a bid from a Bidder and another bid from any of its affiliates) are not permitted in response to this solicitation. Each Bidder must submit a single bid. For the purposes of this bid solicitation, individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture. If any Bidder submits more than one bid (or an affiliate also submits a bid), either on its own or as part of a joint venture, Canada will choose at its discretion which bid to consider.

a) **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:

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

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 2 to Part 3, 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 "Bidders Response" columns of Attachment 2 to Part 3, 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. A technically responsive bid is one that

complies with the mandatory requirements of this bid solicitation, meets all mandatory evaluation criteria and obtains the required pass mark.

(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 Appendix A. 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) **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.

NOTE : This solicitation is raised for Level 3 resources, however SSC may also require occasion Level 1 and Level 2 resources. In order to standardize any Resulting Contract(s), the firm per diem rate from the financial bid provided by Bidders for Level 3 resources will be used to determine the firm per diems for Level 1 and Level 2 resources as follows :

- ***Level 1 Firm Per Diem rate : 70% of Contractor's Level 3 rate***
- ***Level 2 Firm Per Diem rate : 80% of Contractor's Level 3 rate***

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

3.4 Section III: Certifications

Bidders must submit the certifications required under Part 5.

PART 4 EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 EVALUATION PROCEDURES

a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria. There are several steps in the evaluation process, which are described below. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

b) An evaluation team composed of representatives of 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.

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 2 to Part 3 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 2 to Part 3 of the RFP.

c) **Resource Evaluation:** Resources will only be assessed after contract award once specific requirements are are sought via the Task Solicitation process. After contract award, the Task Solicitation process, outlined in Part 7 (7.2.5) of the RFP, will be used for each requirement raised under the Contract. When a Task Solicitation (TS) form is issued, the Contractors will be requested to propose resource(s) to satisfy the specific requirement based on the TS form's Statement of Work. The proposed resource(s) will then be assessed against the mandatory and rated requirements identified in the solicitations evaluation.

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.

e) **Joint Venture Experience**: In accordance with Attachment 2 to PART 3 herein, except where expressly provided otherwise, at least one member of a joint venture Bidder must meet any given mandatory and rated requirement of this solicitation. Joint venture members cannot pool their abilities to satisfy any single

mandatory and rated requirement of this solicitation. Wherever substantiation of a mandatory and rated 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 proposal will be evaluated should raise such questions through the Enquiries process as early as possible during the solicitation period.

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.

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 or in the case of a rated requirement no points would be allocated.

(a) There are two financial evaluation methods possible for this requirement. Method 1 will be used if 4 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 4 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 (+) 20% 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 (2 YEAR) CONTRACT PERIOD**	**OPTION PERIOD 1**	**OPTION PERIOD 2**	**TOTAL POINTS**
B.13	Operations Support Specialist	100	100	100	300
C.6	IT Security Engineer	100	100	100	300
C.7	IT Security Incident Management Specialist	100	100	100	300
	Total Points	300	300	300	900

(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.

(c) Method 2: The following financial evaluation method will be used if fewer than 4 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 / Bidder's proposed firm per diem rate x Points Assigned at Table 1 above

The Bidder with the lowest proposed firm 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.

4.4 Basis of Selection

a) The technically responsive bid(s) (maximum of 4) that obtain 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 _____ x **70** = Final Technical Score
Maximum Technical Points 280 pts.)

(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 x **30** = Final Financial Score
Maximum Financial Points (900 pts)

(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 (up to a maximum of 4) will become the top-ranked bidder.

PART 5- CERTIFICATIONS

Bidders must provide the required certifications to be awarded a contract. Canada will declare a bid non- responsive if the required certifications are not completed and submitted in accordance with the articles below.

Compliance with the certifications bidders provide to Canada is subject to verification by Canada during the bid evaluation period (before award of a contract) and after award of a contract. The Contracting Authority will have the right to ask for additional information to verify bidders' compliance with the certifications before award of a contract. The bid will be declared non-responsive if any certification made by the Bidder is untrue, whether made knowingly or unknowingly. Failure to comply with the certifications or to comply with the request of the Contracting Authority for additional information will also render the bid non-responsive.

5.1 Certifications Precedent to Contract Award

The certifications listed below should be completed and submitted with the bid, but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Contracting Authority will so inform the Bidder and provide the Bidder with a time frame within which to meet the requirement. Failure to comply with the request of the Contracting Authority and meet the requirement within that time period will render the bid non-responsive.

5.2 Federal Contractors Program for Employment Equity - Certification

(a) The Federal Contractors Program for Employment Equity (FCP) requires that some suppliers bidding for federal government contracts, valued at $200,000 or more (including all applicable taxes), make a formal commitment to implement employment equity. This is a condition precedent to contract award. If the Bidder is subject to the FCP, evidence of its commitment must be provided before the award of the Contract.

(b) Suppliers who have been declared ineligible contractors by Human Resources and Skills Development Canada (HRSDC) are no longer eligible to receive government contracts over the threshold for solicitation of bids as set out in the *Government Contract Regulations*. Suppliers may be declared ineligible contractors either as a result of a finding of non-compliance by HRSDC, or following their voluntary withdrawal from the FCP for a reason other than the reduction of their workforce to fewer than 100 employees. Any bids from ineligible contractors will be declared non-responsive.

(c) If the Bidder does not fall within the exceptions enumerated in (d)(i) or (ii) below, or does not have a valid certificate number confirming its adherence to the FCP, the Bidder must fax (819-953-8768) a copy of the signed form LAB 1168, Certificate of Commitment to Implement Employment Equity to the Labor Branch of HRSDC.

(d) Each bidder is requested to indicate in its bid whether it is:

(i) not subject to FCP, having a workforce of fewer than 100 permanent full or part-time employees in Canada;

(ii) not subject to FCP, being a regulated employer under the *Employment Equity Act*, S.C. 1995, c. 44;

(iii) subject to the requirements of FCP, because it has a workforce of 100 or more permanent full or part-time employees in Canada, but it has not previously obtained a certificate number from HRSD (because it has not bid before on requirements of $200,000 or more), in which case a duly signed certificate of commitment is required from the Bidder; or

(iv) subject to FCP-EE, and has a valid certification number (i.e., has not been declared an ineligible contractor by HRSDC).

(e) Further information on the FCP-EE is available on the following HRSDC Website:http://www.hrsdc.gc.ca/eng/labour/equality/employment_equity/index.shtml

5.3 Former Public Servant Certification

(a) Contracts with 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 spending public funds. In order to comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required below.

(b) For the purposes of this clause,

(i) "**former public servant**" means a 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 and includes:

(A) an individual;

(B) an individual who has incorporated;

(C) a partnership made of former public servants; or

(D) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

(i) "**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 Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

(ii) "**pension**" means, in the context of the fee abatement formula, 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 *Canadian Pension Plan Act*, R.S., 1985, c. C-8.

(c) If the Bidder is an FPS in receipt of a pension as defined above, the Bidder must provide the following information:

(i) name of former public servant;

(ii) date of termination of employment or retirement from the Public Service.

(d) If the Bidder is an FPS who received a lump sum payment pursuant to the terms of a work force reduction program, the Bidder must provide the following information:

(i) name of former public servant;

(ii) conditions of the lump sum payment incentive;

(iii) date of termination of employment;

(iv) amount of lump sum payment;

(v) rate of pay on which lump sum payment is based;

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

(vii) number and amount (professional fees) of other contracts subject to the restrictions of a work force reduction program.

(e) For all contracts awarded during the lump sum payment period, the total amount of fee that may be paid to a FPS who received a lump sum payment is $5,000, including the Goods and Services Tax or Harmonized Sales Tax.

(f) By submitting a bid, the Bidder certifies that the information submitted by the Bidder in response to the above requirements is accurate and complete.

5.4 Code of Conduct and Certification

By submitting a bid, the Bidder certifies, for himself and his affiliates, to be in compliance with the Code of Conduct and Certifications clause of the Standard instructions. The related documentation hereinafter mentioned will help Canada in confirming that the certifications are true. By submitting a bid, the Bidder certifies that it is aware, and that its affiliates are aware, that Canada may request additional information, certifications, consent forms and other evidentiary elements proving identity or eligibility. Canada may also verify the information provided by the Bidder, including the information relating to the acts or convictions specified herein, through independent research, use of any government resources or by contacting third parties. Canada will declare non-responsive any bid in respect of which the information requested is missing or inaccurate, or in respect of which the information contained in the certifications is found to be untrue, in any respect, by Canada. The Bidder and any of the Bidder's affiliates, will also be required to remain free and clear of any acts or convictions specified herein during the period of any contract arising from this bid solicitation.

Bidders who are incorporated, including those bidding as a joint venture, must provide with their bid a complete list of names of all individuals who are currently directors of the Bidder (See Annex D). Bidders bidding as sole proprietorship, including those bidding as a joint venture, must provide the name of the owner with their bid. Bidders bidding as societies, firms, partnerships or associations of persons do not need to provide lists of names. If the required names have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply will render the bid non-responsive. Providing the required names is a mandatory requirement for contract award.

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) (http://www.tpsgc-pwgsc.gc.ca/app-acq/forms/229-eng.html) for any or all individuals aforementioned within the time specified. Failure to provide such Consent Forms within the time period provided will result in the bid being declared non-responsive.

PART 6 SECURITY REQUIREMENTS

6.1 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.

6.2 Financial Capability

(a) SACC Manual clause A9033T (2011-05-16) Financial Capability; except that subsection 3 is deleted and replaced with the following: “If the Bidder is a subsidiary of another company, then any financial information required by the Contracting Authority in 1(a) to (f) must be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the Bidder; however, if the Bidder is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary; the financial information of the parent company must be provided. If Canada determines that the Bidder is not financially capable but the parent company is, or if Canada is unable to perform a separate assessment of the Bidder’s financial capability because its financial information has been combined with its parent’s, Canada may, in its sole discretion, award the contract to the Bidder on the condition that the parent company grant a performance guarantee to Canada.”

(b) In the case of a joint venture bidder, each member of the joint venture must meet the financial capability requirements.

Part 7 - RESULTING CONTRACT CLAUSES

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

7.1 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).

7.2 TASK SOLICITATION AND TASK AUTHORIZATION PROCEDURES

7.2.1 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.

7.2.2 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 for resource requirements will be distributed to all contract holders with responding submissions being evaluated against respective solicitations mandatories and point rated criteria in order to determine a "Best Fit" resource. For the life of the awarded contracts no single contract holder will be permitted to exceed $20M in awarded Task Authorizations.

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

7.2.3 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 7.6 of the Contract is required to ensure all delegated Technical Authorities follow the terms of the Contract.

7.2.4 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 respond to solicitations without communicating in writing such decisions to Contract Authority;

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.

7.2.5 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, a SSC's 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 resource category from the descriptions included in the Statement of Work, Annex B this Contract. Based on the SOW resource category requirement, the technical authority will develop a corresponding resource evaluation grid establishing specific initiative resource skills and experience sought. 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.

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. Contractors interested in responding to a Task Solicitation are required to do so within five (5) business days, unless otherwise stipulated in the solicitation. While it is encouraged that all contractor's respond to solicitations they will not be penalized for opting not to submit against a particular Task Solicitation, providing that they communicate such decision to Contract Authority.

1.3.1 Clarification of a Task Solicitation

Should a Contractor require clarification on any part of a Task Solicitation, it is the responsibility of the Contractor to contact the Contract Authority 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 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 mandatory 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 mandatory 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 Task Solicitation and that the resource, if selected by SSC, will fulfill the engagement. Upon request by the SSC Contract Authority, the Contractor must provide a signed copy of its exclusivity agreement with the proposed resource for a specific Task Solicitation. A Contractor's failure to secure exclusive rights to the resource or resources submitted in the Contractor's proposal will result in a strike against a Contractor.

1.4 Stage 4 Evaluations 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 and completed contractor self-scoring grids for proposed resources will be 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 using the assessment summary template provided by Contract Authority. 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 applicable candidate's interview. If the Technical Authority decides to interview proposed resources, the Technical Authority will use the same interview scorecard to interview all resources proposed by Contractors. The Contract Authority reserves the right to attend interviews. 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.

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 using the assessment summary template provided by Contract Authority. In cases where interviews have been undertaken the Technical Authority will additionally provide to Contract Authority respective candidates interview scorecard results.

1.5 Stage 5—Task Authorization Award

All Contractors that have submitted proposals in response to a Task Solicitation will be provided evaluation results using the assessment summary template provided by Contract Authority.

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.

1.6 Stage 6—Commencement of Work

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.

1.6.1 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 multiple options for extensions as required by the Technical Authority. 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.

7.2.4 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 initial period of services during which the specified work will be performed.

7.2.5 Termination of a Task Authorization

The Contract Authority may, at its sole discretion, terminate all or any part of a Task Authorization. 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

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

To be validly issued, a Task Authorization must be signed by the Contracting Authority.

Any Task Authorization 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 Task Authorization is done at the Contractor's own risk. If the Contractor receives a Task Authorization that is not appropriately signed, the Contractor must notify the Contracting Authority.

7.2.7 Periodic Usage Reports

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.

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.

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

A. The Solicitation ID, Task Authorization number and the Task Authorization Revision number(s), if applicable;
B. Start and End Date of Task Authorization;
C. # of days contracted;
D. Category of Resource;
E. Firm Per Diem;
F. Resource Name ;
G. Total estimated cost specified in the TA (GST or HST extra);
H. Invoiced days by applicable month

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.

7.2.8 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.

7.3 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.

7.4 SECURITY REQUIREMENT

The following Security Requirement (SRCL and related clauses), 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, CONFIDENTIAL, or RELIABILITY STATUS, as required, granted or approved by CIISD/PWGSC. Until the security screening of the Contractor personnel required by this Contract has been completed satisfactorily by the CIISD, PWGSC, the Contractor personnel MAY NOT HAVE ACCESS to PROTECTED information or assets, and MAY NOT ENTER sites where such information or assets are kept, without an escort, provided by the department or agency for which the Work is being performed..

(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).

7.5 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 two 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.

7.5.1 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 A.

(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.

7.6 AUTHORITIES

(a) Contracting Authority

The Contracting Authority for the Contract is:

xxxxxx
180 rue Kent St, 13-K091
P.O. Box/CP 9808 STN T CSC
Ottawa, ON K1G 4A8
Email: xxxx@ssc-spc.gc.ca
Tel. | Tél. : 613-xxxxx

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

(b) **Technical Authority**

The Technical Authority for the Contract is:

(to be inserted at Contract award)

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:
E-mail address:

7.7 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.

7.8 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, signed timesheet by Technical Authority indicating days and hours worked by contractor;

(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 Non-Telecommunications
11 Laurier Street, PDP 3, 5A1
PO Box 9808 STN T CSC
Gatineau, Quebec
K1G 4A8

(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.

7.9 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.

7.10 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.

7.11 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.

7.12 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 (2011-05-16), Higher Complexity - Services;

(c) Annex B, Statement of Work, including its Appendices as follows;

(i) Appendix A to Annex B - Task Authorization Procedures

(ii) Appendix B to Annex B - Task Authorization Request and Acceptance Form

(iii) Appendix C to Annex B - Resource Assessment Criteria and Response Tables

(iv) Appendix D to Annex B - Certifications at the Task Authorization Stage

(d) Annex A, Basis of Payment;

(e) the signed Task Authorizations, including the required Appendices;

(f) Annex C, Insurance Requirements;

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

(h) 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.

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

Note to Bidders: Either clause 7.13or 7.14, whichever applies (based on whether the successful bidder is a Canadian Contractor or Foreign Contractor), will be included in any resulting contract.

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

7.15 INSURANCE REQUIREMENTS

(a) The Contractor must comply with the insurance requirements specified in Annex C. The Contractor must maintain the required insurance coverage for the duration of the Contract. Compliance with the insurance requirements does not release the Contractor from or reduce its liability under the Contract.

(b) The Contractor is responsible for deciding if additional insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any additional insurance coverage is at the Contractor's expense, and for its own benefit and protection.

(c) The Contractor must, if requested by the Contracting Authority, forward a Certificate of Insurance evidencing the insurance coverage and confirming that the insurance policy complying with the requirements is in force. Coverage must be placed with an Insurer licensed to carry out business in Canada. The Contractor must, if requested by the Contracting Authority, forward to Canada a certified true copy of all applicable insurance policies

7.16 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 (B) 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 sub-article (b).

7.17 JOINT VENTURE CONTRACTOR

(a) Supply Arrangement (SA) Holders who wish to submit their proposal as a joint venture must have already been qualified under the SA # EN578-055605/E as a joint venture

(b) 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]**.

(c) 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.

(d) 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.

(e) All the members are jointly and severally or solidarity liable for the performance of the entire Contract.

(f) 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.

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

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

7.18 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:

- the name, qualifications and experience of a proposed replacement immediately available for Work
- Security information on the proposed replacement as specified by Canada, if applicable
- If the resource for which the Task Authorisation was awarded does not commence Work, then any proposed replacement must have qualifications and experience that meets or exceeds the original resource. If the resource for which the Task Authorisation was awarded has commenced Work, and then departs, then any proposed resource replacement must have qualifications and experience that meet the original evaluation criteria. In either case, replacements must be deemed suitable by the Technical Authority.
- The Contract Authority in consultation with solicitation Technical Authority reserves the right to provide additional time for contractor to provide a replacement resource

Should attempts to secure a replacement resource from contractor fail, original task authorization will be cancelled and at the discretion of technical authority a new solicitation will be initiated.

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 meets or exceeds those obtained for the original resource and be acceptable to Canada. Upon assessment of the replacement, Canada may accept the replacement, exercise the rights in (ii) (A) above, or require another replacement in accordance with this sub article (c).

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.

7.19 SAFEGUARDING ELECTRONIC MEDIA

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

7.20 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.

7.21 ACCESS TO CANADA'S PROPERTY AND FACILITIES

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

7.22 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.

7.23 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.

7.24 Electronic Procurement & Payment Support

Electronic Procurements and Payment (EPP) System

i. SSC is working on an initiative that is expected to provide it with e-functionality from procurement through payment (the "EPP system"). SSC's suppliers will be required to interface with that functionality.
ii. Because the functionality will not be ready at the time of contract award, if Canada wishes for the Contractor to interface with the EPP system during the Contract Period, Canada will issue a
iii. Request for Quotation regarding the work required for the Contractor to interface with the EPP system. The Contractor's Quotation Response will not be subject to a Service Delivery Interval. The Quotation Response must include, at a minimum:
iv. Per diem rates for any resources who would perform the work and the level of effort required; and
v. Any costs for hardware or software that will be required, including development costs to be performed by third parties.

The Parties agree to work cooperatively to determine the work involved and a reasonable ceiling price for that work. If the Parties agree to proceed with that work, Canada will issue a Contract Amendment documenting the ceiling price associated with the work. The Contractor will be required to submit a Service Design for approval by Canada and the work associated with the development of any EPP system interfaces will be treated as a Service Project.

Canada will pay the Contractor, in arrears, up to the ceiling price established in the contract amendment, for actual time worked and any resulting deliverables in accordance with firm, all-inclusive per diem rates set out in the relevant contract amendment, with GST/HST extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday. When submitting its invoices, the Contractor must show the actual time worked by each resource, and/or the amount paid to any subcontractor. With respect to any expenses, the Contractor will be required to demonstrate the out-of- pocket amount spent and will be reimbursed without the addition of any overhead.

Annex 'A'

STATEMENT OF WORK

1.0 OBJECTIVE

To acquire three (3) 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. The initial period of the contract will be for 2 year with 2, one year optional extensions.

The objective of this SOW is to acquire the necessary IT security resources to design, build, and operate enterprise multi-tenant IT security environments on behalf of SSC and its partners.

The Protective Services team has the responsibility to build and operate IT Security infrastructure on behalf of SSC and its partners that include but not limited to physical and virtual network/host based firewalls, web content filtering, virtual private networks, and the ancillary systems that support this infrastructure.

1.1 BACKGROUND

The Government of Canada created Shared Services Canada (SSC) on August 4, 2011, to fundamentally transform how the Government manages its information technology (IT) infrastructure. SCC reports to Parliament through the Minister of Public Works and Government Services Canada (PWGSC) and is part of the PWGSC portfolio. SSC is mandated to deliver email, data centre and telecommunication services to 43 federal departments and agencies (referred to as Partner Organizations). SSC also provides other optional services to government departments and agencies on a cost-recovery basis. A more efficient use of technology will increase productivity across departments and will help build a more modern public service.

The creation of SSC brought together people, processes, data, technology resources and assets from the 43 federal departments and agencies to improve the efficiency, reliability and security of the Government's IT infrastructure by;

- Working in partnership with key stakeholders;
- Adopting enterprise-wide approaches to establish manage and evolve IT infrastructure services;
- Establishing and implementing efficient and effective management processes in support of SSC's mandate.

SSC's first priority is to maintain and improve the delivery of IT-infrastructure services while renewing the Government's aging IT infrastructure. SSC's goal is to move 43 partner organizations from separate and often dissimilar infrastructure services to a set of consolidated, consistent more effective and cost efficient shared services for the GC. Addressing the challenges, opportunities, rewards and risks of an enterprise-wide approach in the development, delivery and management of SSC's services is fundamental to achieve SSC's goals.

SSC is organized around four lines of business as follows:

1)Service Management Branch

The Service Management Branch is responsible for the development of plans, designs and operations of SMDC services for the Government of Canada IT infrastructure. SMDC will provide full lifecycle management (strategy, plan, build, test, deploy, operate and decommission) for its service offerings.

2)Data Centres Branch

The Data Centres Branch functions include the end-to-end management of physical complexes; the establishment of computing environments for partner organizations and for SSC's internal needs across all computing platforms; and the

provision of technical support and certification for day-to-day operations, production applications and database computing environments.

3)Networks and End User

The Networks and End User Branch (NEUB) is responsible for the service management, operations, projects, as well as the design and planning aspects of the Government of Canada's network and end user services infrastructure that fall within SSC's scope. NEUB is comprised of six services that will collectively enhance end user services and technologies within SSC and across Government. The focus on savings and security will be maintained by identifying and implementing network and telecommunications services as one single enterprise.

NEUB key objectives include the rationalization and consolidation of its network and end user services that it delivers to partner organizations. In support of these objectives and SSC's vision, the branch will continue to deploy the Government of Canada's single-email solution; standardize, consolidate and re-engineer the delivery of end user devices across the Government of Canada; and support the provision and ongoing maintenance of global electronic data and communications networks.

4)Cyber and IT Security

Cyber and Information Technology Security Branch (CITS) is responsible for the development of plans, designs and operations of Cyber and IT security services for GC IT infrastructure and for GC Secret Infrastructure (GCSI) within SSC's mandate. The branch will develop business cases for design-ready Cyber and IT security and secret infrastructure services, and will develop and continuously improve Cyber and IT security architecture for the implementation, procurement and delivery of enterprise services based upon a framework founded on the fundamental functions of Prevention, Detection, Response, Recovery and Security Management. The branch fosters strategic relationships with central agencies and SSC's partners to develop policies, standards, technology guidance and ongoing oversight for cyber

Refer to the SSC website at http://publiservice.gc.ca/ssc-spc/no-oo/index-eng.html for a view of the organizational structure for SSC.

Programs and Projects

In light of both requirements, SSC has launched three transformation projects, and supports ongoing sustainability projects to ensure the delivery of the existing IT infrastructure and is already managing several large sustainability projects. The transition projects are expected to be ongoing for the next 3-4 years, in parallel with the planning and development of the transformation projects. In addition, SSC also supports various IT-related initiatives (i.e,. partner-led programs) within the 43 departments and agencies.

Contract resources are required to support the planning and execution of these SSC-led programs and projects, as well as work, on behalf of SSC, on partner-led programs.

Transformation Projects

The three SSC-led transformation projects are as follows:

1)Email Consolidation

The Government of Canada (GC) uses over 100 different email systems, with SSC's 43 partner organizations using approximately 63 assorted systems. With no common standards across the Public Service, compatibility is limited and interoperability is a major issue. SSC's objective is to move our partners towards one secure, reliable and cost-effective email system.

2)Data Centre Consolidation

Presently, the GC supports more than 450 data centres. These facilities were developed over many years in response to the independent service demands and requirements of individual departments. SSC's objective is to reduce the number of data centres across our partner organizations to fewer than 20 modern, secure and reliable centers.

3)Network Services Consolidation

There are currently hundreds of overlapping and uncoordinated electronic networks providing voice and data telecommunication services to over 300,000 users across the GC. These services must be modernized and harmonized. In the process, Information Technology and Cyber Security will be improved and more cost effective. SSC's objective is to design and build a secure and integrated telecommunications network to support GC operations from coast to coast and internationally.

1.2 SCOPE OF WORK

The Contractor must provide Informatics Professional Services in three (3) different resource categories, including:

TBIPS ID	**CATEGORY OF PERSONNEL**
B.13	Operations Support Specialist
C.6	IT Security Engineer
C.7	IT Security Incident Management Specialist

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).

Contents of the deliverables may vary and may include, for example: studies requiring a high-level, broad view of technology; specifications for services requiring an intimate knowledge- both theoretical and practical- of a particular technology; or proof of concepts and technology trials requiring operational knowledge and hands-on experience.

The resources will be engaged on working on the following technologies performing a number of activities including (engineering, design, integration, and operations. As time passes, new technologies will be introduced and others discontinued. The following is snap-shot of what is in use currently (Note that not all resources will work on all technologies):

Symantec Endpoint Protection
FireEye
Symantec Central Quarantine Server
Symantec Mail Security for Microsoft Exchange
Symantec Network Access Control (SNAC) and 6100 Gateway Enforcer
Bit 9 host security
Trend Micro Deep Security
McAfee ePolicy Orchestrator (ePO)
McAfee IPS/IPS technology
HP ArcSight ESM - Security information and event management
Riverbed Steelhead
HP TippingPoint IDS/IPS

Corero IPS (Top Layer)
ForeScout Network Access Control
RSA enVision
Blackstratus netForensics
IBM DataPower
IBM QRADAR (SIEM)
McAfee firewall
Linux – RedHat Enterprise Linux, CentOS, Ubuntu
Windows 7 workstations and Windows 2008, Windows 2012 servers
Bind Domain Name System Server (DNS) server
Tufin firewall policy manager
Sourcefire Intrusion Prevention System (IPS)
Damballa Advanced Threat Protection System
CA Spectrum Network Management System
McAfee Vulnerability Manager
Trustwave MailMarshal Email Security Gateway
McAfee Web Security Gateway
NetScout nGenius Packet Capture and Analyzer
Custom log analysis and event correlation software
Cisco ASA firewalls;
Cisco routers and switches
Cisco ASA SSL and IPSEC VPNs;
Cisco ASA1000v, ASAv, and VSG virtual firewalls;
Cisco Nexus 1000v, any L2/L3 physical network switch;
Cisco PNSC (Prime Network Services Controller);
Cisco Security Manager;
CheckPoint Secure Platform/Nokia/UTM firewalls(Appliances and Open Servers with Application Control);
CheckPoint SSL and IPSEC VPNs;
CheckPoint Multi-domain Manager/Provider1;
FortiGate - firewalls/VPN;
Websense – web filtering, proxy;
BlueCoat – web filtering, proxy;
Trend Micro - Deep Security for virtual and physical instances;
Citrix – Access Gateway and Net-Scaler;
SysLog NG - log management;
Traverse - network logging monitoring tool;
CyberArk – password management;
SafeNet (BlackShield);
Microsoft IAS Radius Server/Network Policy Server;
L3 Communications – Red Eagle and Talon;
Perl and shell scripting;
VMWare, VMView;
Dell SAN, iSCSI and switch zoning;
LDAP;
Infoman/Infoweb and Tivoli ticketing systems.
WatchGuard
Niksun

Possible related services could encompass 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 within the scope of respective sought categories):

1. Analyze IT Security statistics, tools and techniques;
2. Analyze security data and provide advisories and reports;
3. Prepare technical reports such as requirement analysis, options analysis, and technical architecture documents;

4. Provide security architecture design and engineering support;
5. Architecture of improvements and enhancements to the existing, in flight, and future enterprise deployment of Host Security systems for both the backend systems and the host-based software components. Host security includes AV, host firewall, host IDS, application control, whitelisting, and detonation technology;
6. Architecture of improvements and enhancements to the existing, in flight, and future enterprise deployment of network based IPS for both inline and out of line systems;
7. Architecture of improvements and enhancements to the existing, in flight, and future enterprise deployment of Security Information and Event Management (SIEM) Systems;
8. Architecture of improvements and enhancements to the existing, in flight, and future enterprise Border/Perimeter systems services, including firewalls, content filters, XML brokers, proxies, SPAM filters, DNS sinkholes, and VPN terminators;
9. Design the detailed technical solution to satisfy the various requirements provided by both SSC partners and within SSC. These requirements include business, functional, security, user, quality-of-service, integration, and implementation requirements. The requirements provided will range from high-level conceptual requirements to highly-detailed granular requirements;
10. Review the zoning of all current backend management components and design a solution that will bring up all backend systems to be fully compliant with GoC ITSG guidelines. Furthermore, ensure any new systems are properly designed to be compliant with ITSG;
11. Design and implement security countermeasures at the direction of incident response authorities within the GoC. This task often includes the detailed analyzing of a cyber attack (in some cases targeted) in order to develop custom-designed security policies to countermeasure;
12. Assist in the design work required to migrate the various backend systems to a system that will scale for government wide use as part of the SSC initiatives;
13. Design of endpoint protection policies including (but not limited to): Anti-virus, firewall, IPS, host integrity, and location switching/IDS/ firewall policies in an enterprise deployment;
14. Design a custom host based IDS signature to detect a particular network exploit that is not detected by a vendor provided signature;
15. Architecture design and management of an enterprise deployment of Gateway based Network Access Control;
16. Analysis of security logs for security events for the purpose of designing safeguards and countermeasures;
17. Analysis of emerging security threats and implementing policy changes to help mitigate against these new emerging threats;
18. Identify the technical requirements needed to develop and deploy a solution;
19. Analyze and evaluate alternative technology solutions to meet business problems;
20. Ensure the integration of all aspects of technology solutions;
21. Monitor industry trends to ensure that solutions fit with government and industry directions for technology;
22. Provide information, direction, and support for emerging technologies;
23. Perform impact analysis of technology changes;
24. Provide support to applications and/or technical support teams in the proper application of existing infrastructure;
25. Review application and program design or technical infrastructure design to ensure adherence to standards and to recommend performance improvements;
26. Carry out feasibility studies, trend/impact analysis, technology assessments, and propose system implementation plans pertaining to the IT security technologies being evaluated;
27. Provide operational and administrative support to applications and/or technical support teams within the existing infrastructure;
28. Provide operation and administrative support for task surrounding securing the backend systems F5 Layer 7 switches (including security modules);
29. Provide operation and administrative support for task surrounding securing the backend system Cisco switches and routers;

30. Provide operation and administrative support for the enterprise scaled Managed Secured File Transfer (MSFP) system;
31. Provide operation and administrative support for IDS/IPS units and the associated backend management systems (currently HP Tipping Point, McAfee IntruShield and Cisco Sourcefire). This includes recommending and implementing configurations in accordance with SSC acceptable use policies and security policies; monitoring the system through the user interface to investigate alerts as well as to raise and resolve incidents; monitoring logs to validate the deployed configuration; assessing user requests for permitting access to blocked content; and advising the SSC Technical Authority on the security risks of altering the configuration to accommodate new requirements;
32. Host based policy tuning specific to host behaviour patterns of malicious code (Symantec SEPM , McAfee ePO, Bit 9, and Trend Micro Deep Security products);
33. Implement host-based firewall security policies, including event filters;
34. Weekly testing of the host-based security policies to ensure that they defend against any recently released cyber security threats;
35. Initial investigation of end-users' complaints regarding errors in accessing websites. This task involves investigating the host-based security policies that impaired access to the site and either fixing the issue or escalating to more senior technical staff;
36. Daily log file monitoring of the security logs generated from the system firewalls, content checkers, proxies, host-based management servers, and load balancers;
37. Support for the system's host-based security software, anti-virus updates, and software interoperability issues;
38. Administrative and policy management for Gateway Network Access Control systems;
39. Administrative and policy management for FireEye detonation technology;
40. Administrative and policy management for IBM Datapower technology;
41. Extensive administrative and policy management for HP ArcSight ESM - Security information and event management;
42. Administrative support for Unix/Linux;
43. Administrative support for Windows XP, Windows 7, Windows Server 2003, 2008;
44. Administrative support for MacIntosh (Mac OS X);
45. Update existing SOPs and creating new SOPs to define the additional procedures required for the various organisations;
46. Assist in the preparation, technical review, testing and validation of host-based security solution;
47. Review and make recommendations with respect to relevant aspects of the IT security architectures and technologies, including risk identification;
48. Liaise with IT security system vendors in a technical capacity;
49. Attend and participate in technical specialist meetings as requested by the Technical Authority in order to offer subject matter expert advice;
50. Assist in the preparation of IT security related work items;
51. Attend technical meetings as requested by the Technical Authority;
52. Attend and assist the Project Technical Authority at internal and external Technical Liaison Meetings (TLMs), Technical Exchange Meetings (TEMs) and Project Review Meetings (PRMs);
53. Operate and maintain network management solutions based on the CA Spectrum Network Fault Management system. This includes configuring and performing periodic network discovery scans, configuring thresholds and watches for network devices and systems, and compiling management and alerting policies for network devices and systems;
54. Operate and maintain the McAfee Web Gateway (MWG) web proxy and security solution. This includes recommending and implementing configurations in accordance with acceptable use policies and security policies, formulating changes to the MWG security and access policies that control web access, monitoring the logs to validate the deployed configuration, assessing user requests for permitting access to blocked content, and advising the SSC Technical Authority on the security risks of permitting the requested content;

55. Operate and maintain Threat Protection Systems. This includes recommending and implementing configurations in accordance with SSC acceptable use policies and security policies, monitoring the system through the user interface to investigate alerts as well as to raise and resolve incidents, and monitoring the logs to validate the deployed configuration;
56. Operate and maintain the Vulnerability Manager (MVM) systems. This includes configuring the MVM system to perform vulnerability scans on networks and systems, examining vulnerability reports, prioritizing vulnerabilities for mitigation according to risk, and compiling, implementing and testing the effectiveness of mitigation strategies. The resource must also recommend access policies for system users and provide guidance to SSC and SSC regional personnel in mitigating vulnerabilities found within their local infrastructure;
57. Operate and maintain Internet mail gateway based on Trustwave MailMarshal Email Security Gateway, as well as the McAfee Firewall system. This includes formulating firewall policies to leverage McAfee's reputation service to distinguish between low risk senders and higher risk senders, formulating mail security policies for the reception and transmission of email based on sender reputation, monitoring firewall and mail gateway logs, and maintaining whitelists and blacklists;
58. Operate and maintain security event aggregation and correlation systems;
59. Provide systems administration and systems operations support, including setting up user access, user profiles, backup and recovery, day-to-day computer systems operations.
60. Perform software upgrades, and apply patches.
61. Provide customer interface to ensure requested changes are implemented.
62. Monitor computer workload trends and make adjustments to ensure optimum utilization of computer resources
63. Develop, implement, test and support the security policies used to protect operating systems and applications that host the various backend management applications;
64. Investigate additional security safeguards that could be added to protect the backend management systems;
65. Design solutions and then implement to re-scale the current backend management systems to accommodate GoC wide use;
66. Design and implement integration solutions between existing host-based systems to newly-emerging SSC Government wide IT systems;
67. Design and implement centralized vulnerability management backend management systems, including re-designing distributed systems into centralized systems;
68. Design and implement centralized management backend systems (network level). Including re-designing distributed systems into centralized systems;
69. Participate in the IAP process, in a supporting role, that includes Threat and Risk Assessment (TRA) and On-site Technical Vulnerabilities Assessment (OTVA);
70. Design and implant the client side system for the public works Managed Secure File Transfer (MSFT) application at an enterprise scale.
71. Analyzing security log files and reporting on security events to the incident handling authority(s);
72. Design and implement security safeguards and remediation at the direction of the incident handling authority(s);
73. Develop, implement and support the detailed technical solutions for the various business and security requirements provided by third-party stakeholders;
74. Test malicious code against the various security applications in an isolated lab environment. If the threat is not neutralized, develop and implement a countermeasure using the various security applications;
75. Design, modify, test, optimize and support host-based Intrusion Prevention signatures;
76. Design, modify, test, optimize and support host-based non-signature behavioural-based security policies;
77. Design, modify, test, optimize and support host-based firewall policies;
78. Design, modify, test, optimize and support location based security policies;
79. Investigate additional security safeguards that could be added to protect the backend management systems;

80. Design solutions and then implement to re-scale the current backend management systems to accommodate GoC wide use;
81. Design and implement integration solutions between existing host-based systems to newly-emerging SSC Government wide IT systems;
82. Design and implement centralized vulnerability management backend management systems, including re-designing distributed systems into centralized systems;
83. Design and implant the client side system for the public works Managed Secure File Transfer (MSFT) application at an enterprise scale;
84. Design and implement security countermeasures utilizing Services Oriented Architecture (SOA) technologies;
85. Day-to-day technical support of vulnerability management tool management system(s);
86. Day-to-day technical support of IDS/IPS management system(s);
87. Day-to-day technical support of the client side system for Managed Secure File Transfer application, including the various sub-systems used to transmit data from the various end-users into the central server(s) that hosts the MSFT client application;
88. Day-to-day technical support of the centralized malware quarantine servers;
89. Day-to-day technical support of Services Oriented Architecture (SOA) technologies;
90. Document and report security incidents;
91. Day-to-day technical support of the security components of operating systems such as SUSE and Red Hat Linux. This support includes the integrated firewall, file integrity checking systems, and user-based access controls;
92. Writing, executing testing plans including the set-up and maintains of multiple test environments;
93. Assisting in preparing project management documents based on Project Management Body of Knowledge (PMBOK) guidelines.
94. Perform lab testing to evaluate fixes, new features, and system interoperability;
95. Review, assess, develop alternatives, and recommendations for perimeter security approaches, technology, and processes;
96. Review perimeter security requirements and develop cost effective responses;
97. Provide network security expertise on multi-disciplinary project teams to develop design alternatives and implementation strategies;
98. Provide cross training and knowledge transfer to other support personnel;
99. Create and maintain the following:
    - Documentation: structured analysis and recommendations, weekly status reports, installation procedures, build books, maintenance procedures, business requirements analysis, network topologies, specifications and standards, design documentation, solution and implementation requests, support procedures, backup and restore procedures, etc;

2.0 GENERAL ROLE RESPONSIBILITIES

The following provides a description of the responsibilities, tasks and duties which could include but are not limited to be performed by each resource category.

B.13 OPERATIONS SUPPORT SPECIALIST

1. Provide systems administration and systems operations support, including setting up user access, user profiles, backup and recovery, day-to-day computer systems operations.
2. Perform software upgrades, and apply patches.
3. Provide customer interface to ensure requested changes are implemented.
4. Monitor computer workload trends and make adjustments to ensure optimum utilization of computer resources.
5. Analyze security data and provide advisories and reports
6. Conduct impact analysis for new software implementations, major configuration changes and patch management
7. Develop proof-of-concept models and trials for IT Security
8. Design/develop IT Security protocols
9. Identify and analyze technical threats to, and vulnerabilities of, networks
10. Analyze IT Security tools and techniques
11. Complete tasks related to authorization and authentication in physical and logical environments

12. Prepare tailored IT Security alerts and advisories from open and closed sources
13. Complete tasks directly supporting the departmental IT Security and Cyber Protection Program
14. Prepare implementation plans for particular technologies.
15. Installs and monitors particular facets of technology.
16. Configures and optimizes technical installations.
17. Troubleshoots, and responds to user problems.
18. Maintain up to date knowledge of particular technologies and products supporting that technology.
19. Prepare implementation plans for particular technologies.
20. Installs and monitors particular facets of technology.
21. Configures and optimizes technical installations.
22. Troubleshoots, and responds to user problems.
23. Maintain up to date knowledge of particular technologies and products supporting that technology.
24. Develop and document detailed statement of requirements for the proposed platform.
25. Analyze functional requirements to identify information, procedures and decision flows.
26. Evaluate existing procedures and methods, identify and documents database content, structure, and application sub-systems, and develop data dictionary.
27. Define and document interfaces of manual to automated operations within sub-systems, to external systems and between new and existing systems.
28. Define input/output sources, including detailed plan for technical design phase, and obtain approval for system proposals.
29. Design and document in detail all system components, interfaces and operational environment.
30. Design data structures and files, sub-systems and modules, programs, batch, on line, and production monitoring procedures, testing strategy and systems.
31. Document system design, concepts and facilities, present and obtain approval of detailed system designs.
32. Produce operational systems including all forms, manuals, programs, data files and procedures.
33. Develop and document detailed statement of requirements for the proposed platform.
34. Analyze functional requirements to identify information, procedures and decision flows.
35. Evaluate existing procedures and methods, identify and documents database content, structure, and application sub-systems, and develop data dictionary.
36. Define and document interfaces of manual to automated operations within sub-systems, to external systems and between new and existing systems.
37. Define input/output sources, including detailed plan for technical design phase, and obtain approval for system proposals.
38. Design and document in detail all system components, interfaces and operational environment.
39. Design data structures and files, sub-systems and modules, programs, batch, on line, and production monitoring procedures, testing strategy and systems.
40. Document system design, concepts and facilities, present and obtain approval of detailed system designs.
41. Produce operational systems including all forms, manuals, programs, data files and procedures.
42. Install, configure, integrate, policy fine-tune, operate, monitor performance, and detect faults in the system for:
    a. Host and network intrusion detection and prevention systems;
    b. Network and computer forensics systems;
    c. Firewalls, VPNs and network devices;
    d. Enterprise network vulnerability tools;
    e. Malicious code, anti-spam and content management tools;
    f. File integrity tools;
    g. Remote management utilities;
    h. Enterprise Security Management (ESM)/Security Information Management (SIM) systems;
    i. Data preservation and archiving utilities;
    j. 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

C.6 IT SECURITY ENGINEER

1. Review, analyze, evaluate and/or apply:
    a) Directory Standards such as X.400, X.500, and SMTP Operating Systems such as MS, Unix, Linux, and Novell
    b) Networking Protocols such as HTTP, FTP, and Telnet
    c) Secure IT architectures fundamentals, standards, communications and security protocols such as IPSec, IPv6,SSL, and SSH
    d) IT Security protocols at all layers of the Open Systems Interconnection (OSI) and Transmission Control
    e) Protocol/Internet Protocol (TCP/IP) stacks
    f) Domain Name Services (DNS) and Network Time Protocols (NTP)
    g) Network routers, multiplexers and switches
    h) Application, host and/or Network hardening and security best practices such as shell scripting, service identification, and access control
    i) Intrusion detection/prevention systems(HIDS/HIPS), Network-based Intrusion Defence Systems, malicious code defence, file integrity, Enterprise Security Management, Security Information and Event Management (SIEM) Systems and/or firewalls
    j) Data Parsing
    k) Wireless technology
    l) Cryptographic Algorithms

2. Identify the technical threats to, and vulnerabilities of, networks
3. Manage the IT Security configuration
4. Analyze IT Security tools and techniques
5. Analyze the security data and provide advisories and reports
6. Analyze IT Security statistics(to include security log analysis)
7. Prepare technical reports such as IT Security Solutions option analysis and implementation plans
8. Provide Independent Verification and Validation (IV&V) support to IT Security related projects
9. Provide operational support for firewalls / VPNs / web content filtering infrastructure by performing change requests, resolving incidents, monitoring system availability and performance;
10. Provide engineering support through planning and implementing complex changes in large scale (10,000+ users) multi-tenant networked environments;
11. Perform lab testing to evaluate fixes, new features, and system interoperability;
12. Review, assess, develop alternatives, and recommendations for perimeter security approaches, technology, and processes;
13. Review perimeter security requirements and develop cost effective responses;
14. Provide network security expertise on multi-disciplinary project teams to develop design alternatives and implementation strategies;
15. Provide cross training and knowledge transfer to other support personnel;
16. Create and maintain the following:
    - Documentation: structured analysis and recommendations, weekly status reports, installation procedures, build books, maintenance procedures, business requirements analysis, network topologies, specifications and standards, design documentation, solution and implementation requests, support procedures, backup and restore procedures, etc;

C.7 SENIOR IT SECURITY INCIDENT MANAGEMENT SPECIALIST

1. Collection, consumption, and analysis of cyber intelligence reports, cyber intrusion reports, and news related to information security, covering new threats, vulnerabilities, products, and research.
2. Continuous threat analysis
3. Countermeasure deployment coordination
4. Monitoring, detection, and analysis of potential intrusions in real time and through historical trending on security-relevant data sources

5. Response to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures
6. Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior as appropriate
7. Analysis of security-relevant data In-depth analysis of potential intrusions and of tips forwarded from other SOC members
8. Analysis leveraging various data artifacts to determine the who, what, when, where, and why of an intrusion—its extent, how to limit damage, and how to recover
9. Document the details of this analysis, usually with a recommendation for further action
10. Assist in coordinating response actions and incident reporting
11. Countermeasure Implementation: Implementation of response actions to an incident to deter, block, or cut off adversary presence or damage.
12. Malware and Implant Analysis: Extracting malware (viruses, Trojans, implants, droppers, etc.) from network traffic or media images and analyzing them to determine their nature.
13. Interfacing with other SOC teams (Canada, Five Eyes, Third party service provider SOCs)
14. Incident Response Coordination: Work with affected constituents to gather further information about an incident, understand its significance, and assess mission impact.
15. The Duty Analyst log must be continuously updated throughout the DA shift. The log must contain the following, but is not limited to:
    - Daily cyber-observables of interest
    - Activities/accomplishment report for management review; and concerns
16. Additional tasks include but are not limited to:
    - Prepare work plans and schedules of work;
    - Respond to security/cyber related incidents/attacks;
    - Write/modify SIM correlation rules;
    - Tune IDS/IPS systems;
    - Create/modify IDS/IPS signatures;
    - Analyze of events in depth and provide recommendations;
    - Assess vulnerabilities and provide recommendations;
    - Produce reports, analysis and recommendations related to threats;
    - Collect, collate, analyze and disseminate public information related to networked computer threats and vulnerabilities, security incidents and incident response;
    - Configure intrusion detection systems, firewalls and content checkers;
    - Extract and analyze reports and logs;
    - Configure/update virus scanners;
    - Provide support to multiple partners, clients;
    - Create tickets and monitor the ticketing systems and respond to Incident Requests (IR's);
    - Scrip to automate tasks;
    - Prepare and/or deliver IT Security threat, vulnerability and/or risk briefings;
    - Work with other GC resources in the performance of their work as required;
    - Perform tasks directly supporting the departmental IT Security and Cyber Protection Program;
    - Maintain and recommending enhancements to the security posture; and
    - Make technical and procedural recommendations and enhancements in coordination with the other members of the teams.

3.0 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 and quarter.
- Progress report and timesheet must also be included when sending the invoice.

3.1 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.

4.0 Constraints

4.1 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.

4.2 Work Guidance

The resource will work under the guidance of a Technical Authority/Manager

4.3 Status Reports

Status reports need to be included with all invoices from contractor.

4.4 Support Resources

The resource will be provided with office resources but is required to provide computing device.

4.5 Security Clearance

The resource must be cleared to a minimum of **Level 2 - Secret** throughout the course of the contract. Bidder must specify security clearance file number and expiration date.

4.6 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, at locations as 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. On-call and overtime may be required.

4.7 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.

4.8 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.

4.9 Language Requirements

The resource must be able to communicate in English effectively, both orally and written. Given that this position will require the candidate to write architectural documents, it is essential that the candidates have extensive experience in writing such documents.

5.0 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.

6.0 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.

7.0 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.

Annex 'B'

BASIS OF PAYMENT

1. Professional Services

In accordance with the Contract, the Contractor will be paid the following firm all inclusive per diem rates for work pursuant to this Contract, GST /HST extra .

FOR THE INITIAL CONTRACT PERIOD (2 YEARS)	
Category of Personnel	**Firm Per Diem Rate**
Operations Support Specialist	
IT Security Engineer	
IT Security Incident Management Specialist	

FOR OPTION YEAR 1 (1 YEAR)	
Category of Personnel	**Firm Per Diem Rate**
Operations Support Specialist	
IT Security Engineer	
IT Security Incident Management Specialist	

FOR OPTION YEAR 2 (1 YEAR)	
Category of Personnel	**Firm Per Diem Rate**
Operations Support Specialist	
IT Security Engineer	
IT Security Incident Management Specialist	

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 honor, 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 20% 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 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.
(v) 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.

Appendix A to Annex A
Resource Assessment Criteria and Response Tables

(TO BE USED AFTER CONTRACT IS AWARDED)

To facilitate resource assessment, Contract Holders must prepare and submit a response to a Task Solicitation using the template provided with solicitation. When completing the resource grids, the specific information, which demonstrates the requested criteria and reference to the page number of the resume, should be incorporated so that the evaluator can verify this information. It is not acceptable that the tables should contain all the project information from the resume. Only the specific answer should be provided.

RESOURCE ASSESSMENT CRITERIA AND RESPONSE TEMPLATES

The following Level III mandatory category criteria are provided for information purposes only which will be used to evaluate resources at the Task Solicitation (TS) stage. In solicitations where non Level III resource requirements are sought **M1** will be edited accordingly.

3.1.1 Operations Support Specialist
3.1.2 IT Security Engineer
3.1.3 IT Security Incident Management Specialist

Criteria	Mandatory Requirement	Bidders Demonstrated Response	Page #
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 **ten years** (in the last 15 years) performing duties and responsibilities under sought category. The Bidder must clearly substantiate and demonstrate that the proposed resource(s) have at minimum of ten(10) years' experience performing tasks similar to those specified in solicitation SOW.		
M2	Must hold a minimum of a valid 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 may be used to create evaluation grids for a proposed resource in the relevant resource category of the Task Solicitation process. Contract Holders should anticipate that for each resource solicitation the number of point related criteria could number between 6 to 12 items.

Criteria	Point-Rated Criteria		Bidders Demonstrated Response	Insert Page #
R1	The bidder should demonstrate how the proposed resource has *COMPLEX* (*EXTENSIVE* or *INTERMEDIATE*)* experience providing *FIREWALL* *SUPPORT* and *DOCUMENTATION*.			
R2	The bidder should demonstrate how the proposed resource has *COMPLEX* (*EXTENSIVE* or *INTERMEDIATE*)* experience providing *VPN* *SUPPORT* and *DOCUMENTATION*.			
R3	The bidder should demonstrate how the proposed resource has *COMPLEX* (*EXTENSIVE* or *INTERMEDIATE*)* experience providing *URL FILTERING* *SUPPORT* and *DOCUMENTATION*.			
R4	The bidder should demonstrate how the proposed resource			

Criteria	Point-Rated Criteria		Bidders Demonstrated Response	Insert Page #
	has *COMPLEX* (*EXTENSIVE* or *INTERMEDIATE*) experience providing *NETWORK EQUIPMENT* *SUPPORT* and *DOCUMENTATION*.			
R5	The bidder should demonstrate how the proposed resource has *COMPLEX* (*EXTENSIVE* or *INTERMEDIATE*) experience providing *SYSTEM/APPLICATION* *SUPPORT* and *DOCUMENTATION*.			
R6	The bidder should demonstrate how the proposed resource has *COMPLEX* (*EXTENSIVE* or *INTERMEDIATE*) experience providing *SECURITY SOFTWARE* *SUPPORT* and *DOCUMENTATION*.			
R7	The proposed resource must demonstrate *EXTENSIVE* or *INTERMEDIATE* experience providing 3rd level troubleshooting, identifying performance challenges and proposing improvements, and the *DOCUMENTATION* of these *COMPLEX* environments.			
R8	The bidder should demonstrate how the proposed resource has *EXTENSIVE* experience leading projects in a *COMPLEX* environment resulting in the creation of topologies, specifications, equipment definitions, resource requirements, and implementation plans for *FIREWALL*, *VPN*, *URL FILTERING*, *NETWORK EQUIPMENT*, *SYSTEM/ APPLICATION*, and *SECURITY SOFTWARE* projects and *SUPPORT* issues.			
R9	The bidder should demonstrate how the proposed resource has PERL, shell scripting (LINUX, VMWARE, Windows) in a *FIREWALL*, *VPN*, *URL FILTERING*, *NETWORK EQUIPMENT*, *SYSTEM/APPLICATION*, and *SECURITY SOFTWARE* environment.			
R10	The bidder should demonstrate how the proposed resource has experience with Incident and Change Management processes including familiarity with Infoman/ Infoweb, and Tivoli ticket management systems.			
R11	The bidder should demonstrate how the proposed resource has experience working with peers and clients in a *COMPLEX* *FIREWALL*, *VPN*, *URL FILTERING*, *SYSTEM/APPLICATION*, and *SECURITY SOFTWARE* environment. (Maximum 20 points)		• 3-5 years: 5 points • 6-9 years: 10 points • 10+ years: 20 points	
R12	The bidder should demonstrate how the proposed resource has experience in the *SUPPORT* of Blackshield Cryptocard, MS IAS/NPS Radius server, LDAP, in a *SYSTEM/APPLICATION* environment.		1 year 5 points 2-4 years: 10 points 5+ years: 20 points	
R13	The bidder should demonstrate how the proposed resource has experience in implementing *COMPLEX* *FIREWALL*, *VPN*, *URL FILTERING* *SYSTEM/APPLICATION*, and *SECURITY SOFTWARE* applying the government of Canada policies, regulations, directives, and the complete guideline series concerning IT security (e.g. ITSG-33)		1 year 5 points 2-4 years: 10 points 5+ years: 20 points	
R14	The bidder should demonstrate how the proposed resource has experience in planning and implementing *COMPLEX* *FIREWALL*, *VPN*, *URL FILTERING* *SYSTEM/APPLICATION*, and *SECURITY SOFTWARE* environments. (Maximum 60 points)		• *FIREWALL* (5 points) • *VPN* (5 points) • *URL FILTERING* (5 points) • *SYSTEM/APPLICATION* (5 points) • *SECURITY SOFTWARE* (5 points) or • Combination of 3 environments (20 points)	

Criteria	Point-Rated Criteria		Bidders Demonstrated Response	Insert Page #
			• Combination of 4 environments (45 points) • Combination of 5 environments (60 points)	
R15	The bidder should demonstrate how the proposed resource has familiarity with SSC and / or PWGSC service management and change management processes. (Maximum 10 points)		• 1–2 years: 3 points • 3-5 years: 6 points • 6+ years: 10 points	
R16	The bidder should demonstrate how the proposed resource has provided knowledge transfers and cross training to piers and colleagues. (Maximum 30 points)		• 3-4 years: 5 points • 4 -5 years: 10 points • 5- 6 years: 20 points • 6+ years: 30 points	
R17	The bidder should demonstrate how the proposed resource has experience with good written communication skills in solution development. (Maximum 30 points)		• – 4 years: 5 points • – 6 years: 10 points • 6+ years: 30 points	
R18	The bidder should demonstrate how the proposed resource has experience working on and participating with teams in meeting deadlines. Maximum 40 points)		• 3–5 projects (5 points) • 5–10 projects (20 points) • 10–15 projects (30 points) • 15 + projects (40 points)	
R19	Proposed candidates holds valid TOP SECRET Security Clearance with CISD, Public Works and Government Services Canada (PWGSC)		5 points	
R20	The proposed resources hold current and valid certifications through industry recognized certification bodies in the one of the following fields: …… Alternate certifications may be submitted for review and consideration by Technical Authority Proof of certification must be provided.		3 points per certification to a maximum of 15 points (5 certifications)	
R21	The bidder should demonstrate that the proposed resource, in addition to being fluent in English, is also fully fluent in French.		0 point Unilingual 5 points Bilingual	

NOTE to Technical Authorities …. Interviews

If upon the completion of solicitation technical evaluations there exists tie high scores, Technical Authorities have the option of requesting informal interviews to only candidates with the tied scores in order to evaluate suitability and communication skills including confirming their last 12 months of experience as they relate to sought requirements. It is the Technical Authorities responsibility to notify the Contract Authority that they wish to undertake this action.

In the event that such a request is not submitted to Contract Authority, as per vehicle contract the Task Authorization will be awarded to tie contract holder/candidate with the lowest per diem rate.

DEFINITIONS:

EXTENSIVE experience refers to a depth of experience in the IT field that would normally be acquired over a period of ten (10) or more years, within the last fourteen (14) years. Extensive experience candidates are characterized as those that have had full accountability for significant deliverables. The resource is required to have specific knowledge and experience with IP protocols and their behavior, OSI model and Transmission Control Protocol /Internet Protocol (TCP/IP) stack, Network routed/routing protocols and switching methodologies, and IT Security best practices. Best practices include the application of the government of Canada policies, regulations, directives, and the complete guideline series concerning IT security (e.g. ITSG-33).

INTERMEDIATE experience refers to a depth of experience in the IT field that would normally be acquired over a period of five (5) or more years, within the last eight (7) years. Intermediate experience candidates are characterized as those that have had accountability for delivering on portions and activities within a project but not baring the full accountability role as an extensive

experienced candidate would. The resource is required to have specific knowledge and experience with IP protocols and their behavior, OSI model and Transmission Control Protocol /Internet Protocol (TCP/IP) stack, Network routed/routing protocols and switching methodologies, and IT Security best practices. Best practices include the application of the government of Canada policies, regulations, directives, and the complete guideline series concerning IT security (e.g. ITSG-33).

COMPLEX refers to an IT security infrastructure/project/initiative in an environment that supports 10,000 users or more and also had no less than 6 multi-tenant enterprise data centre environments in the last 3 years; in a addition any three (3) or more of the following:
- A multi-tier diverse set of technologies requiring integration from various pier groups such as networking, data centre, and mid-range systems;
- Has a large number of stakeholders with diverse interests both internally, and partner organizations;
- Requirements for high reliability and availability (99.9%);
- Is considered critical to fulfilling the mandate of the organization;
- Requires specialised expertise and/or state of the art technology;
- Is considered a large-scale undertaking requiring a substantial budget with many inputs, outputs and dependencies.

FIREWALL refers to both physical and virtual firewalls in both single and multi-context mode using routed and transparent modes with current software versions and those released within the last 3 years by vendors including, but not limited to Cisco ASA, VSG/ASAv, ASA1000v, Checkpoint, and FortiGate. This would include **COMPLEX** knowledge of routing, NAT (Network Address Translation), ACL (Access Control Lists), and Authentication mechanisms.

VPN refers to both physical and virtual devices using current software versions and those released within the last 7 years by vendors including, but not limited to Cisco, Checkpoint, Asset (Fortigate, L3, General Dynamics) using protocols including, but not limited to SSL, IPsec, and asset (Type 1 encryption). This would include **COMPLEX** knowledge of routing, NAT (Network Address Translation), ACL (Access Control Lists), and Authentication mechanisms.

URL FILTERING refers to both physical and virtual devices using current software versions and those released within the last 3 years by vendors including, but not limited to Websense and Bluecoat. Knowledge specifically required for Websense products include the V5000, V10000, Websense Security Gateway, and for Bluecoat the Proxy SG. The configuration of the URL filtering system, its implementations, policies and procedures are also required. Knowledge of the integration between the Websense and Bluecoat systems and network TAPs, port aggregators (Anue, Netoptics) is necessary for troubleshooting purposes.

NETWORK EQUIPMENT refers to knowledge of both physical and virtual switched networking devices by vendors including, but not limited to Cisco, Avaya, Brocade, HP, and Dell.

SYSTEM/APPLICATION refers to software and hardware by vendors including, but not limited to Red Hat, Ubuntu, Microsoft, Citrix, VMWare, Dell, HP, and Open Source vendors for uses including, but not limited to server hardware, O/S, and application support. SPECIFICALLY REQUIRED: Windows 7/Server 2008R2 and LINUX OS support in both virtualized and non-virtualized environments, Active Directory, Apache, VMWare, VMView, LDAP, Logging (SYSLOG-NG), MS SQL, PHP/DokuWiki, DELL Servers, SANS, and iSCSI SAN switches.

SECURITY SOFTWARE refers to software and utilities by vendors including, but not limited to Cisco, CheckPoint, CyberArk, SafeNet, Trend Micro, Traverse, and Open Source vendors for uses including, but not limited to security management, Deep Security (DSM, DSVA, DVA), password management. SPECIFICALLY REQUIRED: SafeNet <Blackshield>, CheckPoint Multi-Domain Manager/Provider 1, Cisco Prime Network Services Controller & Security Manager, and Trend Micro Deep Security, MS IAS/Network Policy Server Radius Server.

DOCUMENTATION refers to the candidate's ability to create electronic documentation in both textual (written) and diagram form of any solution created by the candidate, or any existing *FIREWALL*, *VPN*, *URL FILTERING*, *SYSTEM/APPLICATION*, and *SECURITY SOFTWARE* solution using off the shelf applications including, but not limited to DokuWiki, MS Visio, MS Project, MS Word, MS Excel, MS Access, or equivalent Open Source Office automation suite. In certain circumstances it will be necessary to update the helpdesk ticketing systems such as Infoman/Infoweb and/or Tivoli with information relevant to the issues discovered, or changes made in the processes that differ from documented process.

SUPPORT refers to the candidate's ability to design any software and/or hardware solution and architecture within the realm of *FIREWALL*, *VPN*, *URL FILTERING*, *SYSTEM/APPLICATION*, and *SECURITY SOFTWARE*. The candidate's knowledge must include the ability to configure any and all portions of the solution, create full **DOCUMENTATION**, and finally, to be able to operationally support (troubleshoot and return to online status during outages) all solutions created by them or their fellow team members. Knowledge transfer is expected for both fellow team members, and other GOC work entities that interact with these software and/or hardware solutions.

ATTACHMENT 1 to Part 3

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		

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

CORPORATE ASSESSMENT AND RESPONSE TEMPLATE Mandatory Evaluation Criteria			
The Bidder MUST demonstrate that they meet the following <u>mandatory</u> criteria			
Criteria	**Mandatory Requirement**	**Demonstrated Experience**	**Insert Page #**
M1	The Bidder must demonstrate that it has billed a combined minimum number of days, under the TBIPS SO/SA or equivalent*, for the following category. **Category of Personnel** / **Mandatory Minimum Number of Billable Days** Operations Support Specialist IT Security Engineer IT Security Incident Management Specialist **16000** The services provided must have been provided under a **maximum of seven (7) contracts.** It is not necessary for each contract to demonstrate all categories of personnel. The experience must occur within the seven (7) years prior to the RFP closing date. The experience may occur at **any time during the seven year period.** For the reference contract to be considered: • The referenced contracts must be undertaken within Canada or in the continental USA. • The reference contract must have been contracted directly with the Bidder and not with the Bidder's subcontractor or affiliate. • The client organization must not be a partner or sub-contractor of the Bidder or other entity that does not have an at arm's length with the Bidder. • The following information MUST be included (as indicated in Table 1 contained in PART 2 of APPENDIX C TO ANNEX B): a) The name (first and last) of the resource that was billed under the contract in the identified TBIPS resource category (or equivalent*); b) The total number of days billed for the specific resource under the contract in the identified TBIPS resource category(or equivalent*); c) The name of the client organization and project (if applicable); d) Contract number; and e) The period of the contract, i.e. start and end date (month/year) ***Definition of equivalent:** For the purposes of mandatory		

	requirement #M1, Canada will accept as equivalent to the identified TPIBS Category, resources that delivered services similar to the responsibilities listed in both TBIPS SA, and the General Roles Responsibilities of the Statement of Work (Annex "B"). This applies to all three Categories of personnel. **Note:** The onus is on the bidder to clearly demonstrate the equivalency. Failure to do so will result in non-compliancy. **Note**: The Bidder is requested to include complete client contact information for each contract (used to demonstrate experience) including name, title, and telephone number or e-mail address. Canada reserves the right to request client contact information, at any time during the evaluation process, for the purposes of verification. Upon request by Canada, the Bidder will have a minimum of 48 hours to provide the required information. If the information is not provided within the period specified in the request, Canada reserves the right to declare the bid non-responsive.		
M2	**Facility Security Clearance** The Bidder must demonstrate that it holds a valid Government of Canada Facility Security Clearance at the level of Secret issued by PWGSC-CISD and maintain this clearance throughout the duration of the ensuing contract.		

4. Point-Rated Technical Criteria

Point Rated Criteria

Proposals, that meet all of the mandatory qualifications, will be further evaluated against the following rated requirements. A Technical Proposal Score out of 70 points, will be computed using the formulas below

Technical Evaluation Criteria	Maximum Score	Technical Scoring Formula
R.1 Corporate Experience in Key Areas	**100**	
R.2 Risk Mitigation Strategy	**180**	
Sub-Total	**280**	**Bidders Score (out of 280) / 280 *70 points**
Technical Proposal Score	**70 Points**	

The Bidder should demonstrate that they meet the following point-rated criteria				
Criteria	**Point-Rated Requirement**	**Max Points**	**Demonstrated Experience**	**Insert Page #**
R1	**Corporate Experience in Key Areas** The Bidder should demonstrate contract experience, within the last five years, providing professional services resources to support IM/IT requirements in the following areas of expertise: • Data Centre Operations – Including the end-to-end management of physical IT computing facilities; the establishment of computing environments; and the provision of technical support for day-to-day operations, production applications and database computing environments. (maximum 2 projects) • Cyber and Information Technology Security – Including planning, designing and/or operating Cyber and IT security services such as Cyber and IT Security prevention, detection, response, recovery and management. (maximum 2 projects) For reference contract to be considered: • The reference project must have had a minimum cumulative level of effort of 600 days billed by the Bidder (across all categories) against the reference contract. • The reference contract must have been contracted directly with the Bidder and not with the Bidder's subcontractor or affiliate. • The client organization must not be a partner or sub-contractor of the Bidder or other entity that does not have an at arm's length with the Bidder. • The following information MUST be included (as indicated in Table 3 contained in PART 2 of APPENDIX C TO ANNEX B): a) The name of the client organization and project (if applicable); b) Contract number; c) The total number of days billed under the contract within the identified area of expertize; d) The period of the contract, i.e. start and and date (month/year); and e) List of the categories that were billed under the contract. **Note:** The Bidder is requested to include complete client contact information for each contract (used to demonstrate experience) including name, title, and telephone number or e-mail address. Canada reserves the right to request client contact information, at any time during the evaluation process, for the purposes of verification. Upon request by Canada, the Bidder will have a minimum of 48 hours to provide the required information. If the information is not provided within the period specified in the	**100**		

	request, Canada reserves the right to give the referenced project / named resource no further consideration and award 0 points. **Evaluation Criteria:** The Bidder will be awarded a maximum of 100 points (up to 25 points per project, to the maximum # identified above) for each referenced project that clearly describes deliverables and meets the below requirements. **Note:** The Bidder must provide for each project reference under separate applicable headings their response for each rated area. Canada reserves the right to give the referenced project no further consideration and award 0 points if bidder's response does not follow above. **A. Data Centre Operations**: up to 25 points, where the Bidder's contracted scope of work includes: ➢ **5 points**- end-to-end management of physical IT computing facilities; ➢ **5 points**- the establishment of computing environments; ➢ **5 points**- the provision of technical support and maintenance for day-to-day operations; ➢ **5 points**- the provision of technical support and maintenance for production applications; ➢ **5 points**- the provision of technical support and maintenance of database computing environments. **B. Cyber and Information Technology Security:** up to 25 points, where the Bidder's contracted scope of work includes: ➢ **10 points**- the planning and or design of Cyber and IT security prevention solutions; ➢ **10 points**- implementing and/or operating Cyber and IT security prevention solutions; ➢ **5 points**- implementing and/or operating of Cyber and IT security detection and response solutions.			
R2	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 Canada (SSC) within 5 days of receipt of a TA Request. 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. 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 **The extent to which the proposed risk mitigation strategy is thoroughly and clearly described**. The Bidders response will be awarded points as follows: **40 points** • **40 points - Very Good** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a profound understanding • **34 points - Good** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a strong understanding • **28 points - Acceptable** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a moderate understanding • **15 points - Unsatisfactory** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates an incomplete understanding • **0 points** Response is poorly written and demonstrates little value to SSC **Relevance of the proposed risk mitigation strategy to ensure the timely provision of qualified resources** The Bidders response will be awarded points as follows: **40 points** • **40 points - Very Good** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a profound understanding • **34 points - Good** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a strong understanding • **28 points - Acceptable** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a moderate understanding • **15 points - Unsatisfactory** Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates an incomplete understanding • **0 points** Response is poorly written and demonstrates little value to SSC			

	Contract Management Plan **100 Points** **The Bidder must provide a plan as to how the resulting contract will be managed.** **The Bidder should describe its proposed Contract Management Plan specifically addressing measures it proposes to manage the resulting contract the following elements:** **A. Experience of proposed Account Support Team;** **B. Approach to transitioning resources and to replacing departing resources when / where needs;** **C. Scalability of Bidders client engagement operations;** **D. Experience with supporting legacy systems / environments;** **E. Experience with supplying and retaining high-demand skillsets associated with this bid.** Each of the elements will be evaluated according to the following point scheme: **20 points - Very Good** • Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a profound understanding of the element **17 points - Good** • Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a strong understanding of the element **14 points - Acceptable** • Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates a moderate understanding of the element **7 points - Unsatisfactory** • Response proposes a strategy (i.e. methods, process and/or activities) which demonstrates an incomplete understanding of the element **0 points** • Response is poorly written and demonstrates little value to SSC			

	SAMPLE – R.1 Demonstrated Corporate Experience in Key Areas					
IT/IM Area of Expertise	**Max # Points**	**Client Organization / Project Name**	**Contract #**	**Total # of Billed Days**	**Contract Period**	**Resource Categories (billed under contract)**
	Data Centre Operations					
Reference Project #1	25					
Reference Project #2	25					
Sub-total	**50**					
	Cyber & IT Security					
Reference Project #1	25					
Reference Project #2	25					
Sub-total	**50**					
TOTAL R.2	**100**					

SAMPLE

RESPONSE TEMPLATE FOR BID EVALUATION CRITERIA

Table 1 – M.1 Demonstrated Corporate Experience

Resource Category	Resource Name	# of Billed Days		Client Organization /Project Name	Contract #	Contract Period
Operations Support Specialist						
	<Insert lines as required>					
Sub-total (all reference contracts)		#####				
IT Security Engineer						
	<Insert lines as required>					
Sub-total (all reference contracts)		#####				
IT Security Incident Management Specialist						
	<Insert lines as required>					
Sub-total (all reference contracts)		#####				

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 (2 YEARS)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Security Operations Specialist - Level 3	
IT Security Engineer- Level 3	
IT Security and Incident Management Specialist - Level 3	

FOR THE OPTION YEAR 1 (1 YEAR)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Security Operations Specialist - Level 3	
IT Security Engineer- Level 3	
IT Security and Incident Management Specialist - Level 3	

FOR THE OPTION YEAR 2 (1 YEAR)	
Category of Personnel	**Bidders Proposed Per Diem Rate**
Security Operations Specialist - Level 3	
IT Security Engineer- Level 3	
IT Security and Incident Management Specialist - Level 3	

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.

APPENDIX B TO ANNEX A

CERTIFICATIONS AT THE TASK AUTHORIZATION STAGE

1. Education and Experience

The Contractor certifies that all the information provided in the resume(s) and supporting material submitted, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Contractor to be true and accurate. Furthermore, the Contractor warrants that the individual(s) proposed is capable of performing the Work described in the Contract. Canada reserves the right to verify any information provided in this regard, and untrue statements may result in the TA response being declared non-responsive or another action the Minister may consider appropriate.

_____ _____

Print name of authorized individual & sign above Date

2. Status of Personnel

If the Contractor has proposed any individual in fulfillment of this Contract who is not an employee of the Contractor, the Contractor hereby certifies that it has written permission from such person (or the employer of such person) to propose the services of such person in relation to the work performed in fulfillment of this Contract and to submit such person's resume to Canada. The Contractor must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Contractor.

_____ _____

Print name of authorized individual & sign above Date

3. Availability of Personnel

The Contractor certifies that, should it be authorized to provide the services under any TA resulting from this Contract, the resource(s) proposed in the TA response will be available to commence performance of the Work within a reasonable time from the date of acceptance of the Task Authorization, or within the time specified in the TA Form, and will remain available to perform the Work in relation to the fulfillment of the requirement.

_____ _____

Print name of authorized individual & sign above Date

4. Certification of Language

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

_____ _____

Print name of authorized individual & sign above Date

Annex "C" Insurance Requirements

Commercial General Liability Insurance

1. Commercial General Liability insurance shall be effected by the Contractor and maintained in force throughout the duration of the Contract, in an amount usual for a contract of this nature, but, in any case, for a limit of liability **NOT LESS THAN $2,000,000** per accident or occurrence and in the annual aggregate.

2. The following endorsements must be included:

   (a) Additional Insured: Canada is included as an additional insured, but only with respect to liabilities that may arise from the Contractor's own negligence in the performance of the Contract.

   The interest of Canada as additional insured should read as follows: Canada, represented by [insert client department's name] and/or Public Works and Government Services Canada.

   (b) Notice of Cancellation or Amendment: The Insurer agrees to provide the Contracting Authority thirty (30) calendar days written notice of policy cancellation.
   (c) Cross Liability: Without increasing the limit of liability, the policy shall protect all insured parties to the full extent of coverage provided. Further, the policy shall apply to each Insured in the same manner and to the same extent as if a separate policy had been issued to each.
   (d) Contractual Liability: The policy shall, on a blanket basis or by specific reference to this Contract, extend to assumed liabilities with respect to contractual insurance provisions.
   (e) Contingent Employer's Liability: To protect the Contractor for liabilities arising in the management and administration of statutory and contractual entitlements of its employees.
   (f) Employees and (where applicable) Volunteers as Additional Insured: All employees and (where applicable) volunteers, on behalf of the Contractor, shall be included as additional insured.
   (g) Voluntary Medical Payments, $5,000 per person, $25,000 per accident: To provide for expenses incurred in instances of minor accidental bodily injuries without determination of liability.
   (h) Non-owned Automobile: To protect the Contractor for liabilities arising by its use of vehicles owned by other Parties.
   (i) Products and Completed Operations Broad Form: While not limited to, the endorsement should include service, assembly and repair activities as well as material, parts or equipment furnished in connection with the work performed by the Contractor or on its behalf.

Errors and Omissions Liability Insurance

1. Errors and Omissions Liability insurance shall be effected by the Contractor and maintained in force throughout the duration of the Contract in an amount usual for a contract of this nature, but, in any case, for a limit of liability **NOT LESS THAN $1,000,000** per loss and in the annual aggregate, inclusive of defence costs.
2. If this is a claim made policy and the duration of the Contract exceeds the policy term; in the event of cancellation or non-renewal of the policy, an Extended Claims Reporting Endorsement, minimum twelve (12) months, must be secured by the Contractor.
3. The following endorsement must be included:

   Notice of Cancellation or Amendment: The Insurer agrees to provide the Contracting Authority thirty (30) calendar days written notice of cancellation.

   Department of Justice,
   284 Wellington Street, Room SAT-6042,
   Ottawa, Ontario, K1A 0H8

For other provinces and territories, send to:

Senior General Counsel,
Civil Litigation Section,
Department of Justice
234 Wellington Street, East Tower
Ottawa, Ontario K1A 0H8

(A) A copy of the letter must be sent to the Contracting Authority. Canada reserves the right to co-defend any action brought against Canada. All expenses incurred by Canada to co-defend such actions will be at Canada's expense. If Canada decides to co-defend any action brought against it, and Canada does not agree to a proposed settlement agreed to by the Contractor's insurer and the plaintiff(s) that would result in the settlement or dismissal of the action against Canada, then Canada will be responsible to the Contractor's insurer for any difference between the proposed settlement amount and the amount finally awarded or paid to the plaintiffs (inclusive of costs and interest) on behalf of Canada.

(B) Errors and Omissions Liability Insurance

(i) The Contractor must obtain Errors and Omissions Liability (a.k.a. Professional Liability) insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature but for not less than $1,000,000 per loss and in the annual aggregate, inclusive of defence costs.
(ii) If the policy is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.
(iii) The following endorsement must be included:

Notice of Cancellation: The Insurer will endeavour to provide the Contracting Authority thirty (30) days written notice of cancellation.

Annex "D" Code of Conduct and Certification
Adresse de courriel / E-mail Address:
Ministère/Department:
Dénomination sociale complète du fournisseur / Complete Legal Name of Supplier
Adresse du fournisseur / Supplier Address
NEA du fournisseur / Supplier PBN
Numéro de la demande de soumissions (ou numéro du contrat proposé) Solicitation Number (or proposed Contract Number)
Membres du conseil d'administration (Utilisez le format - Prénom Nom) Board of Directors (Use format - first name last name)
1. Membre / Director
2. Membre / Director
3. Membre / Director
4. Membre / Director
5. Membre / Director
6. Membre / Director
7. Membre / Director
8. Membre / Director
9. Membre / Director
10. Membre / Director
Autres Membres/ Additional Directors:

ATTACHMENT 3 TO PART 4

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**
Sample A	**100** (50 pts. per period)	$400.00	$400.00	$420.00	$450.00	$450.00	$450.00
Sample B	**150** (75 pts. Per period)	$550.00	$550.00	$600.00	$650.00	$580.00	$600.00
Sample C	**150** (75 pts. Per period)	$800.00	$800.00	$420.00	$450.00	$450.00	$450.00
TOTAL	**400**						

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

(Median 1)	For the **Sample A** 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 **Sample A** 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 **Sample B** 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 **Sample B** 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 **Sample C** 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 **Sample C** 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.

STEP 2 – POINT ALLOCATION	
Bidder 1:	
Sample A - Contract Period	= 50 points (lowest rate within the lower and upper median band limits)
Sample A - Option Year 1	= 50 points (lowest rate within the lower and upper median band limits)
Sample B - Contract Period	= 75 points (lowest rate within the lower and upper median band limits)
Sample B - Option Year 1	= 75 points (lowest rate within the lower and upper median band limits)
Sample C - Contract Period	= 0 (proposed rate is above the upper median band limit)
Sample C - Option Year 1	= 0 (proposed rate is above the upper median band limit)
Bidder 2:	
Sample A - Contract Period	= 47.62 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample A - Option Year 1	= 44.44 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample B - Contract Period	= 68.8 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample B - Option Year 1	= 63.5 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample C - Contract Period	= 75 points (lowest rate within the lower and upper median band limits)
Sample C - Option Year 1	= 75 points (lowest rate within the lower and upper median band limits)
Bidder 3:	
Sample A - Contract Period	= 44.44 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample A - Option Year 1	= 44.44 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample B - Contract Period	= 71.12 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)

Sample B - Option Year 1	= 68.75 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample C - Contract Period	= 70 points (lowest proposed rate within upper and lower band limits divided by bidders proposed rate times points available)
Sample C - Option Year 1	= 75 points (lowest rate within the lower and upper median band limits)
STEP 3 - TOTAL FINANCIAL SCORE	
Bidder 1 50+ 50+75+75+0+0 = Total Financial Score of 250 points out of a possible 400 points **Bidder 2** 47.62+ 44.44+68.8+63.5+75+75 = Total Financial Score of 374.36 points out of a possible 400 points **Bidder 3** 44.44 + 44.44+71.12+68.75+70+75 = Total Financial Score of 373.75 points out of a possible 400 points	

Annex E 'Security Requirement Checklist'