Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions – TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

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

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

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

Comments - Commentaires

Title - Sujet
Tier 2 Informatics Professional Ser

Solicitation No. - N° de l'invitation	**Date**
W6369-17P5LL/B	2019-03-19

Client Reference No. - N° de référence du client
W6369-17P5LL

GETS Reference No. - N° de référence de SEAG
PW-$IPS-004-34777

File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
004ips.W6369-17P5LL	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2019-04-09

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☑

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Patel, Ankoor	004ips

Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 858-9403 ( )	( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
DEPARTMENT OF NATIONAL DEFENCE
101 COLONEL BY DR.
OTTAWA
Ontario
K1A0K2
Canada

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
See Herein	

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution
Informatics Professional Services Division/Division des services professionnels en informatique
Terrasses de la Chaudière 4th Floo
10 Wellington Street
Gatineau
Quebec
K1A0S5

Canada

BID SOLICITATION
FOR CONTRACTS AGAINST A SUPPLY ARRANGEMENT FOR TASK-BASED INFORMATICS PROFESSIONAL SERVICES (TBIPS)
FOR
THE DEPARTMENT OF NATIONAL DEFENCE

Table of Contents

List of Annexes to the Resulting Contract:
Annex A Statement of Work: Workstream 1 – Secret
Annex A Statement of Work: Workstream 2 – Top Secret

Appendix A to Annex A - Tasking Assessment Procedure
Appendix B to Annex A - Task Authorization (TA) Form
Appendix C to Annex A - Resources Assessment Criteria and Response Table: Workstream 1 – Secret
Appendix C to Annex A - Resources Assessment Criteria and Response Table: Workstream 2 – Top Secret
Appendix D to Annex A - Certifications at the TA stage

Annex B Basis of Payment

Annex C Security Requirements Check List
Appendix A to Annex C – Security Requirement Checklist Supplemental Security Guide – Workstream 1 – Secret
Appendix A to Annex C – Security Requirement Checklist Supplemental Security Guide – Workstream 2 – Top Secret

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

-Attachment 3.1: Bid Submission Form

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

-Attachment 4.1: Bid Evaluation Criteria: Workstream 1 – Secret
-Attachment 4.1: Bid Evaluation Criteria: Workstream 2 – Top Secret
-Attachment 4.2: Pricing Schedule

List of Attachment to Part 5 (Certifications):

-Attachment 5.1: Federal Contractors Program for Employment Equity – Certification

BID SOLICITATION
FOR CONTRACTS AGAINST A SUPPLY ARRANGEMENT FOR TASK-BASED INFORMATICS PROFESSIONAL SERVICES (TBIPS)
FOR
THE DEPARTMENT OF NATIONAL DEFENCE

PART 1 - GENERAL INFORMATION

1.1 Introduction

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

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

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

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

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

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

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

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

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

1.2 Summary

(a) This bid solicitation is a re-tender of the requirement described in bid solicitation number W6369-17P5LL/A dated 2019/02/13 with a bid closing date of 2019/03/06 at 14:00 EST; this document replaces the previous version entirely.

(b) This bid solicitation is being issued to satisfy the requirement of the Department of National Defence (the "**Client**") for Task-Based Informatics Professional Services (TBIPS) under the TBIPS Supply Arrangement (SA) method of supply.

(c) It is intended to result in the award of up to 2 contracts in each of 2 Workstreams, with each contract purchasing Work from only one Workstream. Each contract will be for 3 years plus 1 one-year irrevocable options allowing Canada to extend the term of the contract. Bidders do not have to submit a bid for each Workstream. In the event that a Bidder wants to bid on more than one Workstream, a separate technical bid should be submitted for each Workstream if the Bidder chooses to submit its bid in hard copies.

(d) There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 – Resulting Contract Clauses. For more information on personnel and organization security screening or security

clauses, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

(e) The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-Chile Free Trade Agreement (CCFTA), the Canada-Peru Free Trade Agreement (CPFTA), the Canada-Colombia Free Trade Agreement (CColFTA), the Canada-Panama Free Trade Agreement (CPanFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), the Canadian Free Trade Agreement (CFTA), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

(f) This procurement is subject to the Controlled Goods Program. The Defence production Act defines Canadian Controlled Goods as certain goods listed in Canada's Export Control List, a regulation made pursuant to the Export and Import Permits Act (EIPA).

(g) The Federal Contractor's Program (FCP) for employment equity applies to this procurement; see Part 5 – Certifications and Additional Information, Part 7 – Resulting Contract Clauses and the attachment titled "Federal Contractors Program for Employment Equity – Certification."

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

(i) This bid solicitation allows bidders to use the epost Connect service provided by Canada Post Corporation to transmit their bid electronically. Bidders must refer to Part 2 entitled "Bidder Instructions, and Part 3 entitled "Bid Preparation Instructions", of the bid solicitation, for further information.

(j) Only TBIPS SA Holders currently holding a TBIPS SA for Tier 2, in all resource categories of a given Workstream and in the National Capital Region under the EN578-170432 series of SAs are eligible to compete. The TBIPS SA EN578-170432 is incorporated by reference and forms part of this bid solicitation, as though expressly set out in it, subject to any express terms and conditions contained in this bid solicitation. The capitalized terms not defined in this bid solicitation have the meaning given to them in the TBIPS SA.

(k) SA Holders that are invited to compete as a joint venture must submit a bid as that joint venture SA Holder, forming no other joint venture to bid. Any joint venture must be already qualified under the SA #EN578-170432 as that joint venture at the time of bid closing in order to submit a bid.

(l) For each Workstream, the Resource Categories described below are required on an as and when requested basis in accordance with the TBIPS SA Annex "A":

WORKSTREAM 1 – SECRET

RESOURCE CATEGORY	SPECIFIC TASK TITLE	LEVEL OF EXPERTISE	ESTIMATED NUMBER OF RESOURCES REQUIRED
IT Security Methodology, Policy and Procedures Analyst	Security Technical Implementation Guide	LEVEL 2	2
PKI Specialist	PKI	LEVEL 3	3

IT Security Engineer	Network Security – Content Inspection	LEVEL 3	2
IT Security Design Specialist	Host Security	LEVEL 2	2
IT Security Design Specialist	Information Exchange Gateway (IEG)	LEVEL 3	1
IT Security Design Specialist	Network Security – Content Inspection	LEVEL 3	1
IT Security Design Specialist	Virtualisation Security	LEVEL 3	2
IT Security Design Specialist	NEPS ISS	LEVEL 3	1
Network Security Analyst	NEPS ISS	LEVEL 2	6
Network Security Analyst	Information Exchange Gateway (IEG)	LEVEL 2	1
Network Security Analyst	Network Security Monitoring (NSM)	LEVEL 3	3

WORKSTREAM 2 – TOP SECRET

RESOURCE CATEGORY	SPECIFIC TASK TITLE	LEVEL OF EXPERTISE	ESTIMATED NUMBER OF RESOURCES REQUIRED
IT Security Engineer	Configuration Management	LEVEL 3	1
IT Security Engineer	Information Exchange Gateway (IEG)	LEVEL 2	1
IT Security Engineer	Cyber Security Reference Architecture	LEVEL 3	1
IT Security Engineer	Cross Domain Solution - Access	LEVEL 3	1

IT Security Engineer	Cross Domain Solution - Transfer	LEVEL 2	2
IT Security Engineer	TS IEG / TS Zoning	LEVEL 2	1
IT Security Engineer	Network Security Monitoring - NSM	LEVEL 3	1
IT Security Design Specialist	Full Packet Capture	LEVEL 2	1
IT Security Design Specialist	Host Security	LEVEL 2	1
IT Security Design Specialist	ICAM and PKI	LEVEL 3	3
IT Security Design Specialist	Information Exchange Gateway (IEG)	LEVEL 3	1
IT Security Design Specialist	Cross Domain Solution - Access	LEVEL 3	1
IT Security Design Specialist	Host Security	LEVEL 3	1
IT Security Design Specialist	Network Security - Content Inspection	LEVEL 3	1
IT Security Design Specialist	Enterprise eGRC	LEVEL 3	1
Network Security Analyst	Network Security Monitoring (NSM)	LEVEL 3	1
Network Security Analyst	SIEM	LEVEL 3	1
Incidental Management Specialist	SIEM	LEVEL 3	1

1.3 Debriefings

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

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

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

(b) Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract(s).

(c) The 2003 (2018-05-22) Standard Instructions - Goods or Services - Competitive Requirements are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003 and this document, this document prevails.

(d) Subsection 3.a) of Section 01, Integrity provisions - bid of Standard Instructions 2003 incorporated by reference above is deleted in its entirety and replaced with the following:

(i) at the time of submitting an arrangement under the Request for Supply Arrangement (RFSA), the Bidder has already provided a list of names, as requested under the *Ineligibility and Suspension Policy*. During this procurement process, the Bidder must immediately inform Canada in writing of any changes affecting the list of names.

(e) Subsection 4 of Section 05, Submission of bids of Standard Instructions 2003 incorporated by reference above, is amended as follows:

Delete: 60 days

Insert: 180 days

(f) Subsection 1 of Section 08, Transmission by facsimile or by epost Connect of Standard Instructions 2003 incorporated by reference above, is deleted and replaced by the following:

1. Facsimile

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

2.2 Submission of Bids

(a) Bids must be submitted only to the Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and at the PWGSC address indicated on page one of the bid solicitation or through epost Connect if the Bidder chooses to use this service.

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

2.3 Enquiries - Bid Solicitation

(a) All enquiries must be submitted in writing to the Contracting Authority no later than 5 calendar days before the bid closing date. Enquiries received after that time may not be answered.

(b) Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as “proprietary” will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered with

copies to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.4 Former Public Servant

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

(b) **Definitions**

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

(i). an individual;

(ii). an individual who has incorporated;

(iii). a partnership made of former public servants; or

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

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

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

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

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

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

(i). name of former public servant;

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

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites

as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

(d) **Work Force Adjustment Directive**

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

If so, the Bidder must provide the following information:

(i). name of former public servant;

(ii). conditions of the lump sum payment incentive;

(iii). date of termination of employment;

(iv). amount of lump sum payment;

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

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

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

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

2.5 Applicable Laws

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

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

2.6 Improvement of Requirement During Solicitation Period

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

2.7 Volumetric Data

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

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

(a) **Epost Connect Bid Submission**

(i) If the Bidder chooses to submit its bid electronically, Canada requests that the Bidder submits its bid in accordance with section 08 of the 2003 Standard Instructions. Bidders are required to provide their bid in a single transmission. The epost Connect service has the capacity to receive multiple documents, up to 1GB per individual attachment.

(ii) The bid must be gathered per section and separated as follows:

(A) Section I: Technical Bid

(B) Section II: Financial Bid

(C) Section III: Certifications

(iii) For further information please refer to article 08 - Transmission by facsimile or by epost Connect at https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual/1/2003/23#transmission-by-facsimile.

(b) **Soft Copy Bid Submission (CD or USB)**

(i) If the Bidder chooses to submit its bid in soft copy via the PWGSC Bid Receiving Unit, Canada requests that the Bidder submits its bid in separate sections as follows:

(i) Section I: Technical Bid – One soft copy on a CD or USB key

(ii) Section II: Financial Bid – One soft copy on a CD or USB key

(iii) Section III: Certifications – One soft copy on a CD or USB key

(c) If the Bidder is simultaneously providing an epost Connect copy and soft copy of the bid and if there is a discrepancy between the wording of the epost Connect copy and soft copy, the wording of the epost Connect copy will have priority over the wording of the soft copy.

(d) Canada is not requesting a hard copy of the bid. However, if the Bidder submits a hard copy of its bid, and if there is a discrepancy between the wording of the soft or epost Connect copy and the hard copy, the wording of the soft or epost Connect copy will have priority over the wording of the hard copy.

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

(f) **Format for Bid**: Canada requests that Bidders follow the format instructions described below in the preparation of their bid:

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

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

(iii) include a title page at the front of each volume of the bid that includes the title, date, bid solicitation number, bidder's name and address and contact information of its representative; and

(iv) include a table of contents.

(g) **Canada's Policy on Green Procurement**: In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process. See the Policy on Green Procurement

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

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

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

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

(i) A Bidder, including related entities, will be permitted to submit only one bid in response to this bid solicitation. If a Bidder or any related entities participate in more than one bid (participating means being part of the Bidder, not being a subcontractor), Canada will provide those Bidders with 2 working days to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all the affected bids being disqualified. A single bid may contain bids to be awarded a contract in one or more Workstreams. However, a bid may not contain a bid from the Bidder, including related entities to be awarded more than one contract in any given Workstream.

(ii) For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity is a natural person, corporation, partnership, etc), an entity will be considered to be "**related**" to a Bidder if:

(A) they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);

(B) they are "related persons" or "affiliated persons" according to the Canada Income Tax Act;

(C) the entities have now or in the two years before bid closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

(D) the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

(iii) Individual members of a joint venture cannot participate in another bid in response to this bid solicitation, either by submitting a bid alone or by participating in another joint venture.
.

(i) Joint Venture Experience:

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

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

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

Example: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder have 3 years of experience providing maintenance service, and (b) that the bidder have 2 years of experience integrating hardware with complex

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

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

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

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

That show in total 100 billable days.

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

3.2 Section I: Technical Bid

(a) The technical bid consists of the following:

(i) **Bid Submission Form**: Bidders are requested to include the Bid Submission Form – Attachment "3.1" with their bids. It provides a common form in which bidders can provide information required for evaluation and contract award, such as a contact name and the Bidder's Procurement Business Number, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.

(ii) **Security Clearance**: Bidders are requested to submit the following security information for each of the proposed resources with their bids on or before the bid closing date:

SECURITY INFORMATION	
Name of individual as it appears on security clearance application form	
Level of security clearance obtained	
Validity period of security clearance obtained	
Security Screening Certificate and Briefing Form file number	

If the Bidder has not included the security information in its bid, the Contracting Authority will provide an opportunity to the Bidder to submit the security information during the evaluation period. If the Bidder has not submitted the security information within the period set by the Contracting Authority, its bid will be declared non-responsive.

(iii) **Substantiation of Technical Compliance**: The technical bid must substantiate the compliance with the specific articles of Attachment “4.1”, which is the requested format for providing the substantiation. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder or its proposed solution or resources comply is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be considered non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the bid - this information can be referenced in the "Bidder's Response" column of Attachment “4.1”, where Bidders are requested to indicate where in the bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

(iv) **Previous Similar Projects**: Where the bid must include a description of previous similar projects: (i) a project must have been completed by the Bidder itself (and cannot include the experience of any proposed subcontractor or any affiliate of the Bidder); (ii) a project must have been completed by the bid closing date; (iii) each project description must include, at minimum, the name and either the telephone number or e-mail address of a customer reference; and (iv) if more similar projects are provided than requested, Canada will decide in its discretion which projects will be evaluated. A project will be considered "similar" to the Work to be performed under any resulting contract if the project was for the performance of work that closely matches the Resource Categories identified In Annex A. Work will be considered to "closely match" if the work in the provided project is described in at least 50% of the points of responsibility listed in the description of the given Resource Category.

(v) **Proposed Resources**: The technical bid must include résumés for the resources as identified in Attachment “4.1". The same individual must not be proposed for more than one Resource Category or more than one Workstream. The Technical bid must demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to the proposed resources:

(A) Proposed resources may be employees of the Bidder or employees of a subcontractor, or these individuals may be independent contractors to whom the Bidder would subcontract a portion of the Work (refer to Part 5, Certifications).

(B) For educational requirements for a particular degree, designation or certificate, PWGSC will only consider educational programs that were successfully completed by the resource by the time of bid closing. If the degree, designation or certification was issued by an educational institution outside of Canada, the Bidder is requested to provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC). If the Bidder has not included the copy of the results in its bid, the Contracting Authority will provide an opportunity to the Bidder to submit it during the evaluation period. If the Bidder has not submitted the copy of the results within 2 working days of the request by the Contracting Authority, its bid will be declared non-responsive.

(C) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of bid

closing and must continue, where applicable, to be a member in good standing of the profession or membership throughout the evaluation period and Contract Period. Where the designation or membership must be demonstrated through a certification, diploma or degree, such document must be current, valid and issued by the entity specified in this solicitation. If the entity is not specified, the issuer must have been an accredited or otherwise recognized body, institution or entity at the time the document was issued. If the degree, diploma or certification was issued by an educational institution outside of Canada, the Bidder is requested to provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC). If the Bidder has not included the copy of the results in its bid, the Contracting Authority will provide an opportunity to the Bidder to submit it during the evaluation period. If the Bidder has not submitted the copy of the results within 2 working days of the request by the Contracting Authority, its bid will be declared non-responsive.

(D) For work experience, PWGSC will not consider experience gained as part of an educational program, except for experience gained through a formal co-operative program at a post-secondary institution.

(E) For any requirements that specify a particular time period (e.g., 2 years) of work experience, PWGSC will disregard any information about experience if the technical bid does not include the relevant dates (month and year) for the experience claimed (i.e., the start date and end date). Canada will evaluate only the duration that the resource actually worked on a project or projects (from his or her start date to end date), instead of the overall start and end date of a project or a combination of projects in which a resource has participated.

(F) For work experience to be considered by Canada, the technical bid must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. Only listing experience without providing any supporting data to describe responsibilities, duties and relevance to the requirement, or reusing the same wording as the qualification requirements, will not be considered "demonstrated" for the purposes of the assessment. The Contractor should provide complete details as to where, when, month and year, and how, through which activities/responsibilities, the stated qualifications / experience were obtained. In situations in which a proposed resource worked at the same time on more than one project, the duration of any overlapping time period will be counted only once toward any requirements that relate to the individual's length of experience.

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

(A) In conducting its evaluation of the bids, Canada may, but will have no obligation to request that a bidder provide customer references. If Canada sends such a written request, the bidder will have 2 working days to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive. These customer references must each confirm if requested by PWGSC, the information required in Corporate Mandatory Requirement M1 for Workstream 1 and 2 of Attachment “4.1”.

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

“Has the Bidder provided your organization with the services described below?

*The Bidder must have been awarded at least 2 Government * informatics professional service† contracts.*

For each contract identified:

(a) *The value must be at least $5,000,000.00 ($5M) excluding applicable taxes;*
(b) *The duration must be at least two (2) years within the last eight (8) years from the closing date of this solicitation and cannot include option periods that have not been exercised;*
(c) *The Bidder must have provided at least five (5) resources simultaneously for a period of at least twelve (12) consecutive months; and*

Each contract used must also demonstrate that the Bidder has provided services to an organization with the following environment:

(e) At least 100 workstations on a classified network or secret network;
(f) Microsoft Windows workstation operating system (Windows XP, Windows Vista, Windows 7 and/or Windows 10); and
(g) Centralized software distribution and patch management.

** Government client may include a Federal, Provincial or Municipal Department/Agency or Crown Corporation.*
† Informatics Professional Services are professional services provided by the Bidder in support of an information technology or information management project or contract.

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

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

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

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

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

(vii) **Corporate Profile**: The Bidder is requested to provide a corporate profile, which should include an overview of the Bidder and any subcontractors, and/or authorized agents of the Bidder that would be involved in the performance of the Work on the Bidder's behalf. The Bidder is requested to provide a brief description of its size, corporate structure, years in business, business activities, major customers, number of employees and their geographic presence. This information is requested for information purposes only and will not be evaluated.

3.3 Section II: Financial Bid

(a) **Pricing**: Bidders must submit their financial bid in accordance with the Pricing Schedule provided in Attachment “4.2”. The total amount of Applicable Taxes must be shown separately, if applicable. Unless otherwise indicated, bidders must include a single, firm, all-inclusive per diem rate quoted in Canadian dollars in each cell requiring an entry in the pricing tables.

(b) **Variation in Resource Rates By Time Period**: For any given resource category, where the financial tables provided by Canada allow different firm rates to be charged for a resource category during different time periods:

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

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

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

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

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

(d) **All Costs to be Included**: The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option periods. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.

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

3.4 Section III: Certifications

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

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

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

(b) An evaluation team composed of representatives of the Client and PWGSC will evaluate the bids on behalf of Canada. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

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

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

(ii) **Requests for Further Information**: If Canada requires additional information in order to do any of the following pursuant to the Section entitled "Conduct of Evaluation" in 2003, Standard Instructions - Goods or Services - Competitive Requirements:

(A) verify any or all information provided by the Bidder in its bid; or

(B) contact any or all references supplied by the Bidder (e.g., references named in the résumés of individual resources) to verify and validate any information submitted by the Bidder,

the Bidder must provide the information requested by Canada within 3 working days of a request by the Contracting Authority.

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

4.2 Technical Evaluation

A separate technical evaluation will be conducted for each Workstream.

(a) **Mandatory Technical Criteria:**

(i) Each bid will be reviewed for compliance with the mandatory requirements of the bid solicitation. Any element of the bid solicitation that is identified specifically with the words "must" or "mandatory" is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.

(ii) The mandatory technical criteria are described in Attachment 4.1 – Bid Evaluation Criteria.

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

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

(ii) The rated requirements are described in Attachment 4.1 – Bid Evaluation Criteria.

(c) **Number of Resources Evaluated**:

Only a certain number of resources per Resource Category will be evaluated as part of this bid solicitation as identified in Attachment 4.1. Additional Resources will only be assessed after contract award once specific tasks are requested of the Contractor. After contract award, the Task Authorization process will be in accordance with Part 7 – Resulting Contract Clauses, the Article titled "Task Authorization". When a Task Authorization Form (TA Form) is issued, the Contractor will be requested to propose a resource to satisfy the specific requirement based on the TA Form's Statement of Work. The proposed resource will then be assessed against the criteria identified in the Contract's Statement of Work in accordance with Appendix C of Annex A.

(d) **Reference Checks**:

(i) Whether or not to conduct reference checks is discretionary. However, if PWGSC chooses to conduct reference checks for any given rated or mandatory requirement, it will check the references for that requirement for all bidders who have not, at that point, been found non-responsive.

(ii) For reference checks, Canada will conduct the reference check in writing by email. Canada will send all email reference check requests to contacts supplied by all the Bidders within a 48-hour period using the email address provided in the bid. Canada will not award any points and/or a bidder will not meet the mandatory experience requirement (as applicable) unless the response is received within 5 working days of the date that Canada's email was sent.

(iii) If Canada does not receive a response from the contact person within the 5 working days, Canada will not contact the Bidder and will not permit the substitution of an alternate contact person.

(iv) Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated.

(v) Points will not be allocated and/or a bidder will not meet the mandatory experience requirement (as applicable) if (1) the reference customer states he or she is unable or unwilling to provide the information requested, or (2) the customer reference is not a customer of the Bidder itself (for example, the customer cannot be the customer of an affiliate of the Bidder instead of being a customer of the Bidder itself). Nor will points be allocated or a mandatory met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder.

4.3 Financial Evaluation

(a) There are two possible financial evaluation methods for this requirement. The first method will be used if three or more bids are determined responsive (see (b) Financial Evaluation - Method A below). The second method will be used if fewer than three bids are determined responsive (see (c) Financial Evaluation - Method B below). A separate Financial Evaluated Price will be calculated for each Workstream.

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

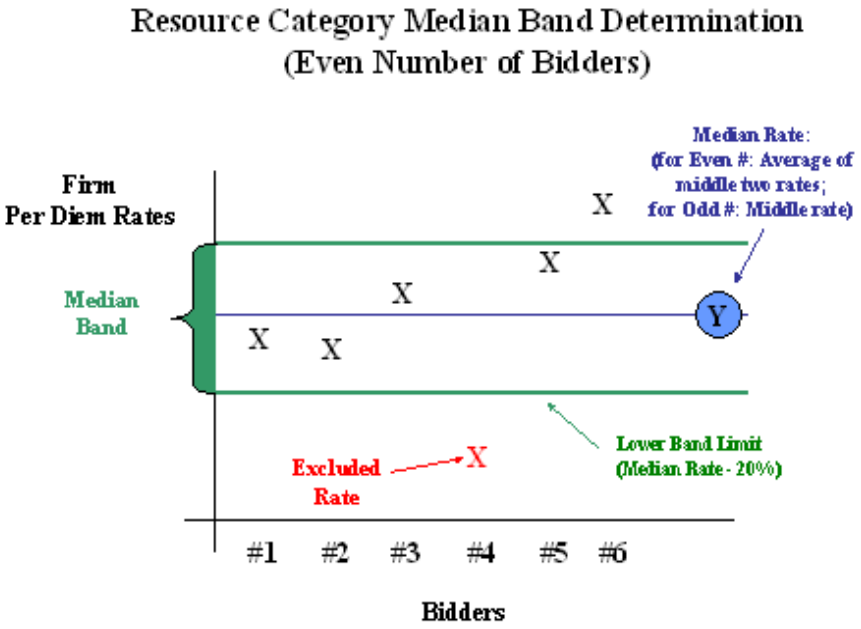
(i) Calculation of Total Bid Price: The financial evaluation will be conducted using the pricing tables completed by the Bidders and the Firm Per Diem Median Rate Evaluation Method explained below. A financial calculation will occur for each Bidder by multiplying its firm per diem rates, or Median Rate(s) if applicable, for the Initial Contract Period and the option period(s) with the estimated number of days of work for each period, for all the Resource Categories stated in Attachment 4.2 - Pricing Schedule. The sum of such rates will constitute the Total Bid Price for that Bidder.

(ii) Firm Per Diem Median Rate Evaluation

(A) Use: The firm per diem median rate calculation will apply to modify the rate to be assessed in the financial evaluation of a Bidder, where that Bidder submits a firm per diem rate for a resource category that is lower than the Lower Band Limit as calculated below. The firm per diem median rate calculation is for evaluation purposes only, and the actual submitted per diem rate will be used in any resulting contract in all instances.

(B) Calculation for both the Initial Contract Period and the Option Period medians: Using the per diem rate proposed for each individual Resource Category a Median Rate will be determined for each Resource Category for the Initial Contract Period, and for each of the option period(s). For each Resource Category, the Median Rate will be calculated using the median function in Microsoft Excel. A Lower Band Limit will be calculated for each Resource Category and will represent a range that encompasses the Median Rate to a value of minus (-) 15% of the Median Rate. If a Bidder bids a firm per diem rate for a Resource Category that is lower than the Lower Band Limit, that Bidder's financial evaluation will be conducted using a per diem rate equal to the Median Rate for that Resource Category.

For example, if the Median Rate (Y) is determined to be $500 for a Resource Category, the Lower Band Limit would be minus (-) 15% of $500, or $425. If a Bidder proposes a firm per diem rate that is lower than $425, the Median Rate of $500 will be used in the Bidder's financial evaluation for that Resource Category.



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

(i) **Calculation of Total Bid Price:** The financial evaluation will be conducted using the pricing tables completed by the Bidders. A financial calculation will occur for each Bidder by multiplying its firm per diem rates for the Initial Contract Period and the option period(s) with the estimated number of days of work for each period, for all the Resource Categories

stated in Attachment 4.2 - Pricing Schedule. The sum of such rates will constitute the Total Bid Price for that Bidder.

(d) Substantiation of Professional Services Rates

In Canada's experience, bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates bid for professional services, Canada may, but will have no obligation to, require price support in accordance with this Article. If Canada requests price support, it will be requested from all otherwise responsive bidders who have proposed a rate that is at least 15% lower than the median rate bid by all responsive bidders for the relevant resource category or categories. If Canada requests price support, the Bidder must provide the following information:

(i) an invoice (referencing a contract serial number or other unique contract identifier) that shows that the Bidder has provided and invoiced a customer (with whom the Bidder deals at arm's length) for services performed for that customer similar to the services that would be provided in the relevant resource category, where those services were provided for at least three months within the eighteen months before the bid solicitation closing date, and the fees charged were equal to or less than the rate offered to Canada;

(ii) in relation to the invoice in (i), evidence from the Bidder's customer that the services identified in the invoice include at least 50% of the tasks listed in the Statement of Work for the category of resource being assessed for an unreasonably low rate. This evidence must consist of either a copy of the contract (which must describe the services to be provided and demonstrate that at least 50% of the tasks to be performed are the same as those to be performed under the Statement of Work in this bid solicitation) or the customer's signed certification that the services subject to the charges in the invoice included at least 50% of the same tasks to be performed under the Statement of Work in this bid solicitation; and

(iii) in respect of each contract for which an invoice is submitted as substantiation, a résumé for the resource that provided the services under that contract that demonstrates that, in relation to the resource category for which the rates are being substantiated, the resource would meet the mandatory requirements and achieve any required pass mark for any rated criteria; and

(iv) the name, telephone number and, if available, e-mail address of a contact person at the customer who received each invoice submitted under (i), so that Canada may verify any information provided by the Bidder.

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

(e) Formulae in Pricing Tables

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

4.4 Basis of Selection

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

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

(a) A bid must comply with the requirements of the bid solicitation, meet all mandatory evaluation criteria and obtain the required pass marks for the point rated criteria identified in this bid solicitation to be declared responsive.

(b) The responsive bid that obtains the highest Total Bidder Score will be recommended for award of a contract. For any given Bidder, the greatest possible Total Technical Score is 70 while the greatest possible Total Financial Score is 30.

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

$$\frac{\text{Technical Score}}{\text{Maximum Technical Points (bidders, please refer to the maximum technical points in Attachment 4.1).}} \times 70 = \text{Total Technical Score}$$

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

$$\frac{\text{Lowest Financial Evaluated Price}}{\text{The Bidder's Financial Evaluated Price}} \times 30 = \text{Total Financial Score}$$

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

Total Technical Score + Total Financial Score = Total Bidder Score

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

(d) A maximum of two contract(s) for each Workstream may be awarded in total as a result of this solicitation.

(e) 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.

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

(i) when one contract is awarded, the amount of the Limitation of Expenditure will be determined at Canada's discretion;

(ii) where two contracts are awarded, the amount of the Limitation of Expenditure of each contract will be determined in accordance with the following:

(A) the Bidder with the highest Total Bidder Score will receive 55% of the funding initially allocated to that Workstream; and

(B) the Bidder with the next highest Total Bidder Score will receive 45% of the funding initially allocated for that Workstream.

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

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

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

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

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

5.1 Certifications Precedent to Contract Award and Additional Information

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

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

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list at the time of contract award.

Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list during the period of the Contract.

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

5.3 Additional Certifications Precedent to Contract Award

(a) Professional Services Resources

(i) By submitting a bid, the Bidder certifies that, if it is awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives.

(ii) By submitting a bid, the Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

(iii) If a Bidder has proposed any individual who is not an employee of the Bidder, by submitting a bid, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the

Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

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

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

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

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

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirement

(a) Before award of a contract, the following conditions must be met:

(i) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

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

(b) Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

(c) For additional information on security requirements, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (*http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html*) website.

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

6.2 Financial Capability

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

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

6.3 Controlled Goods Requirement

(a) SACC Manual clause A9130T (2014-11-27) Controlled Goods Program - Bid

(b) In the case of a joint venture bidder, each member of the joint venture must meet the requirements of the Controlled Goods Program.

PART 7 - RESULTING CONTRACT CLAUSES

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

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

7.1 Requirement

(a) _____ (the "**Contractor**") agrees to supply to the Client the services described in the Contract, including the Statement of Work, in accordance with, and at the prices set out in, the Contract. This includes providing professional services as and when requested by Canada, to one or more locations to be designated by Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.

(b) **Client**: Under the Contract, the "**Client**" is the Department of National Defence.

(c) **Reorganization of Client**: The Contractor's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Client. The reorganization, reconfiguration and restructuring of the Client includes the privatization of the Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the Contracting Authority or Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.

(d) **Defined Terms**: Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions or Supplemental General Conditions. Any reference to an Identified User in the Supply Arrangement is a reference to the Client. Also, any reference to a "deliverable" or "deliverables" includes all documentation outlined in this Contract. A reference to a "local office" of the Contractor means an office having at least one full time employee that is not a shared resource working at that location.

7.2 Task Authorization

(a) **As-and-when-requested Task Authorizations**: The Work or a portion of the Work to be performed under the Contract will be on an "as-and-when-requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract. The Contractor must not commence work until a validly issued TA has been issued by Canada and received by the Contractor. The Contractor acknowledges that any work performed before such issuance and receipt will be done at the Contractor's own risk.

(b) **Allocation of Task Authorizations**:

(i) More than one Contract has been awarded for this requirement. As a result, the Task Authorizations issued under this series of contracts will be allocated in accordance with the following:

(ii) At the time this series of contracts was awarded, each Contractor was allocated an amount of funding as specified in the Limitation of Expenditure in respect of Task

Authorizations based on the evaluation process described in the bid solicitation that resulted in the award of this series of contracts.

(iii) Canada will make a reasonable effort to ensure that the dollar value of the TAs issued to the Contractors are proportionally balanced throughout the Contract Period based on the funding allocated. A review of TAs issued to the Contractors will be conducted at six-month intervals and at the beginning of each fiscal year to confirm proportional utilization and distribution of the TAs. Should a contractor refuse a TA under the Contract or Canada determines the proposed resource(s) do not meet the minimum experience or other requirements of the categories identified in the TA, the next Contractor, under the same allocation process, will be offered the draft TA. The dollar value of the refused TA may be subtracted from the dollar value of the Contractor's Contract and may be re-allocated, at the Contracting Authority's sole discretion, in whole or in part, to one or more of the other contractors in that same Workstream. Should all Contractors refuse a TA under the Contract, Canada reserves the right to use other methods of supply.

(c) **Assessment of Resources Proposed at TA Stage**: Processes for issuing, responding to and assessing Task Authorizations are further detailed in Appendices A, B, C, and D of Annex A.

(d) **Form and Content of draft Task Authorization**:

(i) The Technical Authority will provide the Contractor with a description of the task in a draft Task Authorization using the form specified in Annex A.

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

(A) the task number;

(B) The date by which the Contractor's response must be received (which will appear in the draft Task Authorization, but not the issued Task Authorization);

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

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

(E) the start and completion dates;

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

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

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

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

(J) the language profile of the resources required;

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

(L) the price payable to the Contractor for performing the task, with an indication of whether it is a firm price or a maximum TA price (and, for maximum price task authorizations, the TA must indicate how the final amount payable will be determined; where the TA does not indicate how the final amount payable will be determined, the amount payable is the amount, up to the maximum, that the Contractor demonstrates was actually worked on the project, by submitting time sheets filled in at the time of the work by the individual resources to support the charges); and

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

(e) **Contractor's Response to Draft Task Authorization**: The Contractor must provide to the Technical Authority, within 2 working days of receiving the draft Task Authorization (or within any

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

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

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

(i) for any TA, inclusive of revisions, with a value less than or equal to $_____ (excluding Applicable Taxes), the TA must be signed by the Technical Authority; and

(ii) for any TA with a value greater than this amount, a TA must be signed by the Technical Authority and Contracting Authority.

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

(g) **Administration of Task Authorization Process for DND**: The administration of the Task Authorization process will be carried out by _____. This process includes monitoring, controlling and reporting on expenditures of the contract with task authorizations to the Contracting Authority.

(h) **Periodic Usage Reports**:

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

(ii) The quarterly periods are defined as follows:

(A) 1st quarter: April 1 to June 30;

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

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

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

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

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

(A) the Task Authorization number and the Task Authorization Revision number(s), if applicable;

(B) a title or a brief description of each authorized task;

(C) the name, Resource category and level of each resource involved in performing the TA, as applicable;

(D) the total estimated cost specified in the validly issued TA of each task, exclusive of Applicable Taxes;

(E) the total amount, exclusive of Applicable Taxes, expended to date against each authorized task;

(F) the start and completion date for each authorized task; and

(G) the active status of each authorized task, as applicable (e.g., indicate whether work is in progress or if Canada has cancelled or suspended the TA, etc.).

(iv) Each report must also contain the following cumulative information for all the validly issued TA's (as amended):

(A) the amount, exclusive of Applicable Taxes, specified in the Contract (as last amended, as applicable) as Canada's total liability to the Contractor for all validly issued TA's; and

(B) the total amount, exclusive of Applicable Taxes, expended to date against all validly issued TA's.

(i) **Refusal of Task Authorizations or Submission of a Response which is not Valid**: The Contractor is not required to submit a response to every draft TA sent to it by Canada. However, in addition to Canada's other rights to terminate the Contract, Canada may immediately, and without further notice, terminate the Contract for default in accordance with the General Conditions if the Contractor in at least three instances has either not responded or has not submitted a valid response when sent a draft TA. For greater clarity, each draft TA, which is identifiable by its task number, will only count as one instance. A valid response is one that is submitted within the required time period and meets all requirements of the draft TA issued, including proposing the required number of resources who each meet the minimum experience and other requirements of the categories identified in the draft TA at pricing not exceeding the rates set out in Annex B. Should a Contractor refuse a TA under the Contract, the next Contractor, under the same allocation process, will be offered the TA. The dollar value of the refused TA will be subtracted from the dollar value of the Contractor's Contract and may be re-allocated, at the Contracting Authority's sole discretion, in whole or in part, to one or more of the other contractors in that same Workstream. Should all Contractors refuse a TA under the Contract, Canada reserves the right to use other methods of supply.

(j) **Consolidation of TA's for Administrative Purposes**: The Contract may be amended from time to time to reflect all validly issued Task Authorizations to date, to document the Work performed under those TA's for administrative purposes.

7.3 Minimum Work Guarantee

(a) In this clause,

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

(ii) "**Minimum Contract Value**" means _____ (insert the applicable percentage of the Maximum Contract Value or a fixed dollar amount.

(b) Canada's obligation under the Contract is to request Work in the amount of the Minimum Contract Value or, at Canada's option, to pay the Contractor at the end of the Contract in accordance with sub-article (c), subject to sub-article (d). In consideration of such obligation, the Contractor agrees to stand in readiness throughout the Contract Period to perform the Work described in the Contract. Canada's maximum liability for work performed under the Contract must not exceed the Maximum Contract Value, unless an increase is authorized in writing by the Contracting Authority.

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

(d) Canada will have no obligation to the Contractor under this article if Canada terminates the entire Contract

(i) for default;

(ii) for convenience as a result of any decision or recommendation of a tribunal or court that the contract be cancelled, re-tendered or awarded to another supplier; or

(iii) for convenience within ten business days of Contract award.

7.4 Standard Clauses and Conditions

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

(a) **General Conditions**:

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

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

4. The total of the amounts, to which the Contractor is entitled to be paid under this section, together with any amounts paid, due or becoming due to the Contractor must not exceed the Contract Price.

5. Where the Contracting Authority terminates the entire Contract and the Articles of Agreement include a Minimum Work Guarantee, the total amount to be paid to the Contractor under the Contract will not exceed the greater of:

(a) the total amount the Contractor may be paid under this section, together with any amounts paid, becoming due other than payable under the Minimum Work Guarantee, or due to the Contractor as of the date of termination, or

(b) the amount payable under the Minimum Work Guarantee, less any amounts paid, due or otherwise becoming due to the Contractor as of the date of termination.

6. The Contractor will have no claim for damages, compensation, loss of profit, allowance arising out of any termination notice given by Canada under this section except to the extent that this section expressly provides. The Contractor agrees to repay immediately to Canada the portion of any advance payment that is unliquidated at the date of the termination.

(b) **Supplemental General Conditions**:

The following Supplemental General Conditions:

(i) 4002 (2010-08-16), Supplemental General Conditions - Software Development or Modification Services;

(ii) 4006 (2010-08-16), Supplemental General Conditions - Contractor to Own Intellectual Property Rights in Foreground Information;

(iii) 4008 (2008-12-12), Supplemental General Conditions - Personal Information;

apply to and form part of the Contract.

7.5 Security Requirement

WORKSTREAM 1 - SECRET

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER: PWGSC FILE #W6369-17-P5LL-S1 REVISED #2-CORRECTION

(a) The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Facility Security Clearance at the level of **NATO SECRET**, issued by the Canadian Industrial Security Directorate (CISD), **Public Works and Government Services Canada (PWGSC)**.

(b) This contract includes access to **Controlled Goods.** Prior to access, the contractor must be registered in the Controlled Goods Program of Public Works and Government Services Canada (PWGSC).

(c) The Contractor/Offeror personnel requiring access to PROTECTED/CLASSIFIED information, assets or sensitive work site(s) **must be a citizen of Canada or United States of America** and must EACH hold a valid personnel security screening at the level of **NATO SECRET**, granted or approved by CISD/PWGSC.

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

(e) The Contractor/Offeror personnel requiring access to **NATO CLASSIFIED** information, assets or sensitive work site(s) **must be a citizen of Canada or United States of America** and EACH hold a valid personnel security screening at the level of **NATO SECRET**, granted or approved by the appropriate delegated NATO Security Authority.

(f) The Contractor must complete and submit a Foreign Ownership, Control and Influence (FOCI) Questionnaire and associated documentation identified in the FOCI Guidelines for Organizations prior to contract award to identify whether a third party individual, firm or government can gain unauthorized access to **CLASSIFIED NATO** information/assets. Public Works and Government Services Canada (PWGSC) will determine if the company is “Not Under FOCI” or “Under FOCI”. When an organization is determined to be Under FOCI, PWGSC will ascertain if mitigation measures exist or must be put in place by the company so it can be deemed “Not Under FOCI through Mitigation”.

(g) The The contractor shall at all times during the performance of the contract possess a letter from PWGSC identifying the results of the FOCI assessment with a FOCI designation of Not Under FOCI or Not Under FOCI through Mitigation.

(h) All changes to Questionnaire and associated FOCI evaluation factors must immediately be submitted to the Industrial Security Sector (ISS) to determine if the changes impact the FOCI designation.

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

(j) The Contractor/Offeror must comply with the provisions of the:

i. Security Requirements Check List and security guide (if applicable), attached at Annex C;
ii. *Industrial Security Manual* (Latest Edition).

WORKSTREAM 2 – TOP SECRET

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER: PWGSC FILE #W6369-17-P5LL-S2 Revised #2

(k) The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Facility Security Clearance at the level of **TOP SECRET and NATO SECRET** issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

(l) This contract includes access to Controlled Goods. Prior to access, the contractor must be registered in the Controlled Goods Program of Public Works and Government Services Canada (PWGSC).

(m) The Contractor/Offeror personnel requiring access to PROTECTED/CLASSIFIED information, assets or sensitive work site(s) **must be a citizen of Canada and** must EACH hold a valid personnel security screening at the level of **TOP SECRET SIGINT and NATO SECRET, as required**, granted or approved by CISD/PWGSC.

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

(o) The Contractor/Offeror personnel requiring access to NATO CLASSIFIED information, assets or sensitive work site(s) **must be citizens of Canada** and EACH hold a valid personnel security screening at the level of **NATO SECRET**, granted or approved by the appropriate delegated NATO Security Authority.

(p) The Contractor must complete and submit a Foreign Ownership, Control and Influence (FOCI) Ques-tionnaire and associated documentation identified in the FOCI Guidelines for Organizations prior to con-tract award to identify whether a third party individual, firm or government can gain unauthorized access to **CLASSIFIED NATO** information/assets. Public Works and Government Services Canada (PWGSC) will determine if the company is “Not Under FOCI” or “Under FOCI”. When an organization is determined to be Under FOCI, PWGSC will ascertain if mitigation measures exist or must be put in place by the company so it can be deemed “Not Under FOCI through Mitigation”.

(q) The Contractor shall at all times during the performance of the contract possess a letter from PWGSC identifying the results of the FOCI assessment with a FOCI designation of Not Under FOCI or Not Under FOCI through Mitigation.

(r) All changes to Questionnaire and associated FOCI evaluation factors must immediately be submitted to the Industrial Security Sector (ISS) to determine if the changes impact the FOCI designation.

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

(t) The Contractor/Offeror must comply with the provisions of the:

i. Security Requirements Check List and security guide (if applicable), attached at Annex C;
ii. *Industrial Security Manual* (Latest Edition).

7.6 Contract Period

(a) **Contract Period**: The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:

(i) The "**Initial Contract Period**", which begins on the date the Contract is awarded and ends 3 years later; and

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

(b) **Option to Extend the Contract**:

(i) The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 1 additional one-year period(s) under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

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

7.7 Authorities

(a) Contracting Authority

The Contracting Authority for the Contract is:

Name: Ankoor Patel
Title: Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Directorate: Informatics and Telecommunications Systems Procurement Directorate
Address: 11 Laurier St., Gatineau, Québec
Telephone: (613) 858-9403
E-mail address: Ankoor.patel@tpsgc-pwgsc.gc.ca

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

(b) Technical Authority

The Technical Authority for the Contract is:

Name: _____
Title: _____

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

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

(c) **Contractor's Representative**

[Fill in or delete as applicable]

7.8 Proactive Disclosure of Contracts with Former Public Servants

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

7.9 Payment

(a) **Basis of Payment**

(i) **Professional Services provided under a Task Authorization with a Maximum Price**: For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked and any resulting deliverables in accordance with the firm all-inclusive per diem rates set out in Annex B, Basis of Payment, Applicable Taxes extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday**.**

(ii) **Travel and Living Expenses – National Joint Council Travel Directive**: The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal and private vehicle expenses provided in Appendices B, C and D of the *National Joint Council Travel Directive* and with the other provisions of the directive referring to “travellers”, rather than those referring to “employees”. All travel must have the prior authorization of the Technical Authority. Travel requests will only be considered for a work location which is located more than 100 kilometers from the particular DND facility within the NCR. The Contractor will be paid for actual time spent travelling at half the hourly rate. The hourly rate will be determined by dividing the firm per diem rate set out in Annex B by 7.5 hours. All payments are subject to government audit.

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

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

(b) **Limitation of Expenditure**

(i) Canada's total liability to the Contractor under the Contract must not exceed the amount set out on page 1 of the Contract, less any Applicable taxes. With respect to the amount set out on page 1 of the Contract, Customs duties are excluded and Applicable Taxes are included. Any commitments to purchase specific amounts or values of goods or services are described elsewhere in the Contract.

(ii) 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:

(A) when it is 75 percent committed, or

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

(C) as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

whichever comes first.

(iii) If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Providing this information does not increase Canada's liability.

(c) **Method of Payment for Task Authorizations with a Maximum Price**: For each Task Authorization validly issued under the Contract that contains a maximum price:

(i) Canada will pay the Contractor no more frequently than once a month in accordance with the Basis of Payment. The Contractor must submit time sheets for each resource showing the days and hours worked to support the charges claimed in the invoice.

(ii) Once Canada has paid the maximum TA price, Canada will not be required to make any further payment, but the Contractor must complete all the work described in the TA, all of which is required to be performed for the maximum TA price. If the work described in the TA is completed in less time than anticipated, and the actual time worked (as supported by the time sheets) at the rates set out in the Contract is less than the maximum TA price, Canada is only required to pay for the time spent performing the work related to that TA.

(d) **Time Verification**

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contractor must repay any overpayment, at Canada's request.

(e) **Payment Credits**

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

(A) If the Contractor does not provide a required professional services resource that has all the required qualifications within the time prescribed by the Contract, the Contractor must credit to Canada an amount equal to the per diem rate (based on a 7.5-hour workday) of the required resource for each day (or partial day) of delay in providing the resource, up to a maximum of 10 days.

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

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

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

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

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

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

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

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

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

(vi) **Audit Rights**: The Contractor's calculation of credits under the Contract is subject to verification by government audit, at the Contracting Authority's discretion, before or after payment is made to the Contractor. The Contractor must cooperate fully with Canada during the conduct of any audit by providing Canada with access to any records and systems that Canada considers necessary to ensure that all credits have been accurately

credited to Canada in the Contractor's invoices. If an audit demonstrates that past invoices contained errors in the calculation of the credits, the Contractor must pay to Canada the amount the audit reveals was required to be credited to Canada, plus interest, from the date Canada remitted the excess payment until the date of the refund (the interest rate is the Bank of Canada's discount annual rate of interest in effect on the date the credit was first owed to Canada, plus 1.25% per year). If, as a result of conducting an audit, Canada determines that the Contractor's records or systems for identifying, calculating or recording the credits are inadequate, the Contractor must implement any additional measures required by the Contracting Authority.

(f) **No Responsibility to Pay for Work not performed due to Closure of Government Offices**

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

(ii) If, as a result of any strike or lock-out, the Contractor or its employees, subcontractors or agents cannot obtain access to government premises and, as a result, no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if the Contractor had been able to gain access to the premises

7.10 Invoicing Instructions

(a) The Contractor must submit invoices in accordance with the information required in the General Conditions.

(b) The Contractor's invoice must include a separate line item for each subparagraph in the Basis of Payment provision, and must show all applicable Task Authorization numbers.

(c) By submitting invoices, the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.

(d) The Contractor must provide the original and two copies of each invoice to the Technical Authority, and a copy to the Contracting Authority.

7.11 Certifications and Additional Information

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

7.12 Federal Contractors Program for Employment Equity - Default by Contractor

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

7.13 Applicable Laws

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

7.14 Priority of Documents

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

(a) these Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement;

(b) Supplemental General Conditions, in the following order:

(i) 4002 (2010-08-16), Supplemental General Conditions - Software Development or Modification Services;

(ii) 4006 (2010-08-16), Supplemental General Conditions - Contractor to Own Intellectual Property Rights in Foreground Information;

(iii) 4008 (2008-12-12), Supplemental General Conditions - Personal Information.

(c) General Conditions 2035 *(*2018-06-21*)*, Higher Complexity - Services;

(d) Annex A, Statement of Work – Annex A;

(i) Appendix A to Annex A - Tasking Assessment Procedure;

(ii) Appendix B to Annex A - Task Authorization (TA) Form;

(iii) Appendix C to Annex A - Resource Assessment Criteria and Response Table;

(iv) Appendix D to Annex A - Certifications at the TA stage;

(e) Annex B, Basis of Payment;

(f) Annex C, Security Requirements Check List;

(g) the validly issued Task Authorizations and any required certifications (including all of their annexes, if any); and

(h) the Contractor's bid dated _____ *(insert date of bid) (if the bid was clarified or amended, insert the time of contract award)*, as clarified on _____ "or" as amended _____ *(insert date(s) of clarification(s) or amendment(s) if applicable.)*

7.15 Defence Contract

(a) SACC Manual clause A9006C (2017-07-16) Defence Contract

7.16 Foreign Nationals (Canadian Contractor)

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

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

7.17 Foreign Nationals (Foreign Contractor)

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

7.18 Insurance Requirements

(a) **Compliance with Insurance Requirements**

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

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

(iii) The Contractor should forward to the Contracting Authority within ten (10) days after the date of award of the Contract a Certificate of Insurance evidencing the insurance coverage. Coverage must be placed with an Insurer licensed to carry out business in Canada and the Certificate of Insurance must confirm that the insurance policy complying with the requirements is in force. If the Certificate of Insurance has not been completed and submitted as requested, the Contracting Authority will so inform the Contractor and provide the Contractor with a time frame within which to meet the requirement. Failure to comply with the request of the Contracting Authority and meet the requirement within the time period will constitute a default under the General Conditions. The Contractor must, if requested by the Contracting Authority, forward to Canada a certified true copy of all applicable insurance policies.

(b) **Commercial General Liability Insurance**

(i) The Contractor must obtain Commercial General Liability Insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature, but for not less than $2,000,000 per accident or occurrence and in the annual aggregate.

(ii) The Commercial General Liability policy must include the following:

(A) Additional Insured: Canada is added as an additional insured, but only with respect to liability arising out of the Contractor's performance of the Contract. The interest of Canada should read as follows: Canada, as represented by Public Works and Government Services Canada.

(B) Bodily Injury and Property Damage to third parties arising out of the operations of the Contractor.

(C) Products and Completed Operations: Coverage for bodily injury or property damage arising out of goods or products manufactured, sold, handled, or distributed by the Contractor and/or arising out of operations that have been completed by the Contractor.

(D) Personal Injury: While not limited to, the coverage must include Violation of Privacy, Libel and Slander, False Arrest, Detention or Imprisonment and Defamation of Character.

(E) Cross Liability/Separation of Insureds: Without increasing the limit of liability, the policy must protect all insured parties to the full extent of coverage provided. Further, the policy must apply to each Insured in the same manner and to the same extent as if a separate policy had been issued to each.

(F) Blanket Contractual Liability: The policy must, on a blanket basis or by specific reference to the Contract, extend to assumed liabilities with respect to contractual provisions.

(G) Employees and, if applicable, Volunteers must be included as Additional Insured.

(H) Employers' Liability (or confirmation that all employees are covered by Worker's compensation (WSIB) or similar program)

(I) Broad Form Property Damage including Completed Operations: Expands the Property Damage coverage to include certain losses that would otherwise be excluded by the standard care, custody or control exclusion found in a standard policy.

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

(K) If the policy is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.

(L) Owners' or Contractors' Protective Liability: Covers the damages that the Contractor becomes legally obligated to pay arising out of the operations of a subcontractor.

(M) Advertising Injury: While not limited to, the endorsement must include coverage for piracy or misappropriation of ideas, or infringement of copyright, trademark, title or slogan.

(c) **Errors and Omissions Liability Insurance**

(i) The Contractor must obtain Errors and Omissions Liability (a.k.a. Professional Liability) insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature but for not less than $1,000,000 per loss and in the annual aggregate, inclusive of defence costs.

(ii) If the Professional Liability insurance is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.

(iii) The following endorsement must be included:

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

7.19 Controlled Goods Program

(a) SACC Manual clause A9131C (2014-11-27) Controlled Goods Program - Contract

(b) SACC Manual SACC Manual clause B4060C (2011-05-16) Controlled Goods

7.20 Limitation of Liability - Information Management/Information Technology

(a) This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this Article, even if it has been made aware of the potential for those damages.

(b) **First Party Liability**:

(i) The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:

(A) any infringement of intellectual property rights to the extent the Contractor breaches the section of the General Conditions entitled "Intellectual Property Infringement and Royalties";

(B) physical injury, including death.

(ii) The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

(iii) Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

(iv) The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (i)(A) above.

(v) The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

(A) any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and

(B) Any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of .75 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the cell titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $1,000,000.00.

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

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

(c) **Third Party Claims**:

(i) Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

(ii) If Canada is required, as a result of joint and several liability or joint and solidarily liable, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite Sub-article (i), with respect to special, indirect, and consequential damages of third parties covered by this Section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death;

damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

(iii) The Parties are only liable to one another for damages to third parties to the extent described in this Sub-article (c).

7.21 Joint Venture Contractor

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

(b) With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:

(i) _____ has been appointed as the "representative member" of the joint venture Contractor and has fully authority to act as agent for each member regarding all matters relating to the Contract;

(ii) by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and

(iii) all payments made by Canada to the representative member will act as a release by all the members.

(c) All the members agree that Canada may terminate the Contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.

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

(e) The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.

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

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

7.22 Professional Services - General

(a) The Contractor must provide professional services on request as specified in this Contract. All resources provided by the Contractor must meet the qualifications described in the Contract (including those relating to previous experience, professional designation, education, language proficiency and security clearance) and must be competent to provide the required services by any delivery dates described in the Contract.

(b) If the Contractor fails to deliver any deliverable (excluding delivery of a specific individual) or complete any task described in the Contract on time, in addition to any other rights or remedies available to Canada under the Contract or the law, Canada may notify the Contractor of the deficiency, in which case the Contractor must submit a written plan to the Technical Authority within ten working days detailing the actions that the Contractor will undertake to remedy the deficiency. The Contractor must prepare and implement the plan at its own expense.

(c) In General Conditions 2035, the Article titled "Replacement of Specific Individuals" is deleted and the following applies instead:

Replacement of Specific Individuals

(i) If the Contractor is unable to provide the services of any specific individual identified in the Contract to perform the services, the Contractor must within five working days of having this knowledge, the individual's departure or failure to commence Work (or, if Canada has requested the replacement, within ten working days of Canada's notice of the requirement for a replacement) provide to the Contracting Authority:

(A) the name, qualifications and experience of a proposed replacement immediately available for Work; and

(B) security information on the proposed replacement as specified by Canada, if applicable.

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

(ii) Subject to an Excusable Delay, where Canada becomes aware that a specific individual identified under the Contract to provide services has not been provided or is not performing, the Contracting Authority may elect to:

(A) exercise Canada's rights or remedies under the Contract or at law, including terminating the Contract in whole or in part for default under the Article titled "Default of the Contractor", or

(B) assess the information provided under (c) (i) above or, if it has not yet been provided, require the Contractor to propose a replacement to be rated by the Technical Authority. The replacement must have qualifications and experience that are similar or exceed those obtained for the original resource and be acceptable to Canada. Upon assessment of the replacement, Canada may accept the replacement, exercise the rights in (ii) (A) above, or require another replacement in accordance with this sub-article (c).

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

(iii) The Contractor must not, in any event, allow performance of the Work by unauthorized replacement persons. The Contracting Authority may order that an original or replacement resource stop performing the Work. In such a case, the Contractor must immediately comply with the order. The fact that the Contracting Authority does not order a resource to stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.

(iv) The obligations in this article apply despite any changes that Canada may have made to the Client's operating environment.

7.23 Safeguarding Electronic Media

(a) Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

(b) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.24 Representations and Warranties

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

7.25 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.

7.26 Transition Services at End of Contract Period

(a) The Contractor agrees to execute the transition tasks identified within Annex A of the Statement of Work, in the period leading up to the end of the Contract Period, to transition from the Contractor to a new contract with another supplier. Using a valid Task Authorization (TA), the Transition Services performed under the Contract will be on an "as-and-when-requested basis", and utilize the resources at its all-inclusive per diem rates set out in Annex B – Basis of Payment.

(b) Transition Services at End of Contract Period is the period that commences with the establishment by DND of a new contractual or other agreement for the provision of IM/IT Engineering and Architecture services to DND before the End of Contract Period. It includes activities that must be undertaken by the Contractor to ensure the smooth, efficient and complete transition without interruption of support to DND.

(c) At the request of the Technical Authority, the Contractor must submit a comprehensive Transition-Out Plan to ensure the efficient, complete and secure:

(i) Transitioning of services to DND or to a third party chosen by DND;
(ii) Transitioning of all assets owned by Canada (including the application source code, database and full data including stored reports) to DND or to a third party chosen by DND; and

(iii) Contractor must deliver the Transition-Out Plan NLT 10 business days of the commencement of the Transition Services at End of Contract Period.

(d) Following acceptance of the Transition-Out Plan by the Technical Authority, the Contractor must undertake all obligations contained within the Transition-Out Plan, in accordance with the Transition-Out schedule approved by DND and included within the Transition-Out Plan; in addition to the following:

(i) The Contractor must provide transfer of knowledge to DND or to DND's delegated third party, in accordance with the schedule and the method to be used as outlined in the Transition-Out Plan, as accepted by DND;

(ii) The Contractor must respond to queries regarding Transition-Out activities and any in-progress work to ensure a smooth transition to DND or DND's delegated third party and to ensure uninterrupted service; and

(iii) During the Transition-Out period, the Contractor is responsible for complete and continued support of IM/IT Engineering and Architecture services to DND, and the completion of any in-progress work, in accordance with the Transition-Out Plan.

7.27 Identification Protocol Responsibilities

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

(a) Contractor Representatives who attend a Government of Canada meeting (whether internal or external to Canada's offices) must identify themselves as Contractor Representatives prior to the commencement of the meeting, to ensure that each meeting participant is aware of the fact that the individual is not an employee of the Government of Canada;

(b) During the performance of any Work at a Government of Canada site, each Contractor Representative must be clearly identified at all times as being a Contractor Representative; and

(c) If a Contractor Representative requires the use of the Government of Canada's e-mail system in the performance of the Work, then the individual must clearly identify him or herself as an agent or subcontractor of the Contractor in all electronic mail in the signature block as well as under "Properties." This identification protocol must also be used in all other correspondence, communication, and documentation.

(d) If Canada determines that the Contractor is in breach of any obligation stated in this Article, upon written notice from Canada the Contractor must submit a written action plan describing corrective measures it will implement to eliminate the recurrence of the problem. The Contractor will have five working days to deliver the action plan to the Client and the Contracting Authority, and twenty working days to rectify the underlying problem.

(e) In addition to any other rights it has under the Contract, Canada may terminate the Contract for default if the corrective measures required of the Contractor described above are not met.

ANNEX A

STATEMENT OF WORK

WORKSTREAM 1 - SECRET

The document follows in PDF format.

A Word version of this document is available by sending a request by e-mail to ankoor.patel@tpsgc-pwgsc.gc.ca.

ANNEX A

STATEMENT OF WORK

WORKSTREAM 2 – TOP SECRET

The document follows in PDF format.

A Word version of this document is available by sending a request by e-mail to ankoor.patel@tpsgc-pwgsc.gc.ca.

APPENDIX A TO ANNEX A

TASKING ASSESSMENT PROCEDURE

1. Where a requirement for a specific task is identified, a draft Task Authorization Form (TA Form) as attached at Appendix B to Annex A will be provided to the Contractor in accordance with the allocation methodology stated in the Contract Article titled "Allocation of Task Authorizations". Once a draft TA Form is received, the Contractor must submit to the Technical Authority a quotation of rates to supply the requested Resource Categories based on the information identified in the TA Form, as well as its corresponding proposed resource(s). The quotation must be signed and submitted to Canada within the time for response identified in the TA Form. The Contractor will be given a minimum of 48 hours (or any longer time period specified in the draft TA) turnaround time to submit a quotation.

2. With each quotation the Contractor must propose the required number of resources and for each proposed resource the Contractor must supply a résumé, the requested security clearance information and must complete the Response Tables at Appendix C of Annex A applicable to the Resource Categories identified in the draft TA. The same individual must not be proposed for more than one Resource Category. The résumés must demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). The résumés must also demonstrate that the proposed resource meets the other requirements identified in the TA. With respect to the proposed resources:

   (i) Proposed resources may be employees of the Contractor or employees of a subcontractor, or these individuals may be independent contractors to whom the Contractor would subcontract a portion of the Work. (Refer to Appendix D to Annex A, Certifications).

   (ii) For educational requirements for a particular degree, designation or certificate, Canada will only consider educational programmes that were successfully completed by the resource before the date the draft TA was first issued to the Contractor.

   (iii) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of draft TA issuance and must continue, where applicable, to be a member in good standing of the profession or membership throughout the assessment period and Contract Period. Where the designation or membership must be demonstrated through a certification, diploma or degree, such document must be current, valid and issued by the entity specified in this Contract or if the entity is not specified, the issuer must have been an accredited or otherwise recognized body, institution or entity at the time the document was issued.

   (iv) For work experience, Canada will not consider experience gained as part of an educational programme, except for experience gained through a formal co-operative programme at a post-secondary institution.

   (v) For any requirements that specify a particular time period (e.g., 2 years) of work experience, Canada will disregard any information about experience if the résumé does not include the relevant dates (month and year) for the experience claimed (i.e., the start date and end date). Canada will evaluate only the duration that the resource actually worked on a project or projects (from his or her start date to end date), instead of the overall start and end date of a project or a combination of projects in which a resource has participated.

   (vi) A résumé must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. Only listing experience without providing any supporting data to describe responsibilities, duties and relevance to the requirement, or reusing the same wording as the TA Form, will not be considered "demonstrated" for the purposes of the assessment. The Contractor should

provide complete details as to where, when, month and year, and how, through which activities/responsibilities, the stated qualifications / experience were obtained. In situations in which a proposed resource worked at the same time on more than one project, the duration of any overlapping time period will be counted only once toward any requirements that relate to the individual's length of experience.

3. The qualifications and experience of the proposed resources will be assessed against the requirements set out in Appendix C to Annex A to determine each proposed resource's compliance with the mandatory and rated criteria. Canada may request proof of successful completion of formal training, as well as reference information. Canada may conduct reference checks to verify the accuracy of the information provided. If reference checks are done, they will be conducted in writing by e-mail (unless the contact at the reference is only available by telephone). Canada will not assess any points or consider a mandatory criterion met unless the response is received within 5 working days. On the third working day after sending out the e-mails, if Canada has not received a response, Canada will notify the Contractor by e-mail, to allow the Contractor to contact its reference directly to ensure that it responds to Canada within 5 working days. Wherever information provided by a reference differs from the information supplied by the Contractor, the information supplied by the reference will be the information assessed. Points will not be allocated or a mandatory criteria considered as met if the reference customer is not a customer of the Contractor itself (for example, the customer cannot be the customer of an affiliate of the Contractor). Nor will points be allocated or a mandatory criteria considered as met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Contractor. Crown references will be accepted.

4. During the assessment of the resources proposed, should the references for two or more resources required under that TA either be unavailable or fail to substantiate the required qualifications of the proposed resources to perform the required services, the Contractor’s quotation may be found to be non-responsive.

5. Only quotations that meet all of the mandatory criteria will be considered for assessment of the point rated criteria. Each resource proposed must attain the required minimum score for the point rated criteria for the applicable Resource Category. If the minimum score for any proposed resource is less than what is required, the Contractor's quotation will be found to be non-responsive.

6. Once the quotation has been accepted by the Technical Authority, the TA Form will be signed by Canada and provided to the Contractor for signature. The TA Form must be appropriately signed by Canada prior to commencement of any work. The Contractor must not commence work until a validly issued TA Form (the Task Authorization) has been received, and any work performed in its absence is done at the Contractor's own risk.

APPENDIX B TO ANNEX A
TASK AUTHORIZATION FORM

All invoices/progress claims must show the referenced Contract and Task numbers. Toutes les factures doivent indiquer les numéros du contrat et de la tâche.		Contract no. - No du contrat
		Task no. - No de la tâche
Amendment no. - No de la modification	Increase/Decrease - Augmentation/Réduction	Previous value - Valeur précédente
To - À	**TO THE CONTRACTOR** You are requested to supply the following services in accordance with the terms of the above referenced Contract. Only services included in the Contract can be supplied against this task. Please advise the undersigned if the completion date cannot be met. Invoices/progress claims shall be prepared in accordance with the instructions set out in the contract. À L'ENTREPRENEUR Vous êtes prié de fournir les services suivants en conformité des termes du contrat mentionné ci-dessus. Seules les services mentionnés dans le contrat doivent être fournis à l'appui de cette demande. Prière d'aviser le signataire si la livraison ne peut se faire dans les délais prescrits. Les factures doivent être établies selon les instructions énoncées dans le contrat. _____ _____ Date for the Department of National Defence pour le ministère de la Défence nationale	
Delivery location - Expédiez à		
Delivery/Completion date - Date de livraison/d'achèvement From - De : To - À :		

Contract item no. No d'article du contrat	Services	Cost Prix
	Applicable Taxes **Taxes applicables**	
	Total	
	THE CONTRACTOR HEREBY ACCEPTS THE TASK AUTHORIZATION IDENTIFIED ABOVE : _____ _____ Name (type or print) Title (type or print) _____ _____ Signature Date	

APPLICABLE ONLY TO PWGSC CONTRACTS: The Contracting Authority signature is required when the total value of the DND 626 exceeds the threshold specified in the Contract.

NE S'APPLIQUE QU'AUX CONTRATS DE TPSGC : La signature de l'autorité contractante est requise lorsque la valeur totale du formulaire DND 626 est supérieure au seuil précisé dans le contrat.

_____
for the Department of Public Works and Government Services
pour le ministère des Travaux publics et services gouvernementaux

DND 626 (01-05)

APPENDIX C TO ANNEX A

RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLE

WORKSTREAM 1 - SECRET

The documents follows in PDF format.

A Word version of this document is available by sending a request by e-mail to ankoor.patel@tpsgc-pwgsc.gc.ca.

APPENDIX C TO ANNEX A

RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLE

WORKSTREAM 2 – TOP SECRET

The documents follows in PDF format.

A Word version of this document is available by sending a request by e-mail to ankoor.patel@tpsgc-pwgsc.gc.ca.

APPENDIX D TO ANNEX A

CERTIFICATIONS AT THE TA STAGE

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

1. CERTIFICATION OF EDUCATION AND EXPERIENCE

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

_____ _____

Print name of authorized individual & sign above Date

2. CERTIFICATION OF AVAILABILITY OF PERSONNEL

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

_____ _____

Print name of authorized individual & sign above Date

3. CERTIFICATION OF STATUS OF PERSONNEL

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

_____ _____

Print name of authorized individual & sign above Date

4. CERTIFICATION OF LANGUAGE – English

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

_____ _____

Print name of authorized individual & sign above Date

ANNEX B

BASIS OF PAYMENT

WORKSTREAM 1:

Resource Category	Specific Task Title	Level	Contract Period 1 (YR 1)	Contract Period 2 (YR 2)	Contract Period 3 (YR 3)	Option Period 1 (YR 4)
IT Security Methodology, Policy and Procedures Analyst	Security Technical Implementation Guide	2				
PKI Specialist	PKI	3				
IT Security Engineer	Network Security – Content Inspection	3				
IT Security Design Specialist	Host Security	2				
IT Security Design Specialist	Information Exchange Gateway (IEG)	3				
IT Security Design Specialist	Network Security – Content Inspection	3				
IT Security Design Specialist	Virtualisation Security	3				
IT Security Design Specialist	NEPS ISS	3				
Network Security Analyst	NEPS ISS	2				
Network Security Analyst	Information Exchange Gateway (IEG)	2				
Network Security Analyst	Network Security Monitoring (NSM)	3				

WORKSTREAM 2:

Resource Category	Specific Task Title	Level	Contract Period 1 (YR 1)	Contract Period 2 (YR 2)	Contract Period 3 (YR 3)	Option Period 1 (YR 4)
IT Security Engineer	Configuration Management	3				
IT Security Engineer	Information Exchange Gateway (IEG)	2				
IT Security Engineer	Cyber Security Reference Architecture	3				
IT Security Engineer	Cross Domain Solution - Access	3				
IT Security Engineer	Cross Domain Solution - Transfer	2				
IT Security Engineer	TS IEG / TS Zoning	2				
IT Security Engineer	Network Security Monitoring (NSM)	3				
IT Security Design Specialist	Full Packet Capture	2				
IT Security Design Specialist	Host Security	2				
IT Security Design Specialist	ICAM and PKI	3				
IT Security Design Specialist	Information Exchange Gateway (IEG)	3				
IT Security Design Specialist	Cross Domain Solution - Access	3				
IT Security Design Specialist	Host Security	3				

IT Security Design Specialist	Network Security - Content Inspection	3				
IT Security Design Specialist	Enterprise eGRC	3				
Network Security Analyst	Network Security Monitoring (NSM)	3				
Network Security Analyst	SIEM	3				
Incidental Management Specialist	SIEM	3				

ANNEX C
SECURITY REQUIREMENTS CHECK LIST

WORKSTREAM 1 AND WORKSTREAM 2

The documents follows in PDF format.

APPENDIX A TO ANNEX C

Security Requirement Checklist Supplemental Security Guide – Workstream 1 – Secret

The documents follows in PDF format.

APPENDIX A TO ANNEX C

Security Requirement Checklist Supplemental Security Guide – Workstream 2 – Top Secret

The documents follows in PDF format.

ATTACHMENT 3.1

BID SUBMISSION FORM

BID SUBMISSION FORM		
Bidder's full legal name		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Bidder's Procurement Business Number (PBN) [see the Standard Instructions 2003] **[Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]**		
Jurisdiction of Contract: Province or territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Bidder's Proposed Site(s) or Premises Requiring Safeguard Measures. See Part 3 for instructions. **(Note: Procurement Officers should delete if this requirement was not included in Part 6)**	Address of proposed site or premise: _____ City: _____ Province: _____ Postal Code: _____ Country: _____	
Former Public Servants See the Article in Part 2 of the bid solicitation entitled Former Public Servant for a definition of "Former Public Servant".	Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
	Is the Bidder a FPS who received a lump sum payment under the terms of the Work Force Adjustment Directive? Yes ____ No ____	

<table>
<tr><td></td><td colspan="2">If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"</td></tr>
<tr><td rowspan="2">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.]</td><td colspan="2"></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3">Workstream covered by this bid: Bidders should indicate which Stream they are proposing to supply in this bid (If the bidder has submitted bid for one or more Streams, please only indicate the Stream covered by this bid).</td><td>Workstream</td><td>Yes/No</td></tr>
<tr><td>Workstream 1</td><td></td></tr>
<tr><td>Workstream 2</td><td></td></tr>
<tr><td colspan="3">On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:
1. The Bidder considers itself and its proposed resources able to meet all the mandatory requirements described in the bid solicitation;
2. This bid is valid for the period requested in the bid solicitation;
3. All the information provided in the bid is complete, true and accurate; and
4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.</td></tr>
<tr><td>Signature of Authorized Representative of Bidder</td><td colspan="2"></td></tr>
</table>

ATTACHMENT 4.1
BID EVALUATION CRITERIA
WORKSTREAM 1 - SECRET

The Bid Evaluation Criteria document follows in PDF format.

A Word version of this document is available by sending a request by e-mail to ankoor.patel@tpsgc-pwgsc.gc.ca.

ATTACHMENT 4.1
BID EVALUATION CRITERIA
WORKSTREAM 2 - TOP SECRET

The Bid Evaluation Criteria document follows in PDF format.

A Word version of this document is available by sending a request by e-mail to ankoor.patel@tpsgc-pwgsc.gc.ca.

ATTACHMENT 4.2
PRICING SCHEDULE

In respect of the "Estimated Number of Days" listed below in (C*) the estimated number of days is for evaluation purposes only during the solicitation process and does not represent a commitment of the future usage.

WORKSTREAM 1:

Initial Contract Period:

Contract Period One (YR. 1)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Methodology, Policy and Procedures Analyst	Security Technical Implementation Guide	2	300	$	$
PKI Specialist	PKI	3	720	$	$
IT Security Engineer	Network Security – Content Inspection	3	480		
IT Security Design Specialist	Host Security	2	300		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		
IT Security Design Specialist	Network Security – Content Inspection	3	240		
IT Security Design Specialist	Virtualisation Security	3	300		

IT Security Design Specialist	NEPS ISS	3	240		
Network Security Analyst	NEPS ISS	2	720		
Network Security Analyst	Information Exchange Gateway (IEG)	2	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	720		
			Total Price Contract Period One		$ **<TBD>**

Contract Period Two (YR. 2)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Methodology, Policy and Procedures Analyst	Security Technical Implementation Guide	2	420	$	$
PKI Specialist	PKI	3	720	$	$
IT Security Engineer	Network Security – Content Inspection	3	480		
IT Security Design Specialist	Host Security	2	420		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		
IT Security Design Specialist	Network Security – Content Inspection	3	240		
IT Security Design Specialist	Virtualisation Security	3	420		

IT Security Design Specialist	NEPS ISS	3	240		
Network Security Analyst	NEPS ISS	2	1200		
Network Security Analyst	Information Exchange Gateway (IEG)	2	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	720		
				Total Price Contract Period One	$ **<TBD>**

Contract Period Three (YR. 3)

(A)	(B)	(C)	(D)	(E)	(F)
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Methodology, Policy and Procedures Analyst	Security Technical Implementation Guide	2	480	$	$
PKI Specialist	PKI	3	720	$	$
IT Security Engineer	Network Security – Content Inspection	3	480		
IT Security Design Specialist	Host Security	2	480		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		
IT Security Design Specialist	Network Security – Content Inspection	3	240		

IT Security Design Specialist	Virtualisation Security	3	480		
IT Security Design Specialist	NEPS ISS	3	240		
Network Security Analyst	NEPS ISS	2	1440		
Network Security Analyst	Information Exchange Gateway (IEG)	2	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	720		
				Total Price Contract Period One	$ **<TBD>**

Option Periods:

Option Period 1 (YR. 4)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Methodology, Policy and Procedures Analyst	Security Technical Implementation Guide	2	480	$	$
PKI Specialist	PKI	3	720	$	$
IT Security Engineer	Network Security – Content Inspection	3	480		
IT Security Design Specialist	Host Security	2	480		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		

IT Security Design Specialist	Network Security – Content Inspection	3	240		
IT Security Design Specialist	Virtualisation Security	3	480		
IT Security Design Specialist	NEPS ISS	3	240		
Network Security Analyst	NEPS ISS	2	1440		
Network Security Analyst	Information Exchange Gateway (IEG)	2	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	720		
				Total Price Contract Period One	$ **<TBD>**

Total Bid Price:	
(Total Price Contract Period One + Total Price Contract Period Two + Total Price Contract Period Three + Total Price Option Period One)	$ **<TBD>**

WORKSTREAM 2:

Initial Contract Period:

Contract Period One (YR. 1)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Engineer	Configuration Management	3	240	$	$
IT Security Engineer	Information Exchange Gateway (IEG)	2	240	$	$
IT Security Engineer	Cyber Security Reference Architecture	3	240		
IT Security Engineer	Cross Domain Solution - Access	3	240		
IT Security Engineer	Cross Domain Solution - Transfer	2	480		
IT Security Engineer	TS IEG / TS Zoning	2	240		
IT Security Engineer	Network Security Monitoring (NSM)	3	240		
IT Security Design Specialist	Full Packet Capture	2	240		
IT Security Design Specialist	Host Security	2	240		
IT Security Design Specialist	ICAM and PKI	3	720		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		

IT Security Design Specialist	Cross Domain Solution - Access	3	240		
IT Security Design Specialist	Host Security	3	240		
IT Security Design Specialist	Network Security - Content Inspection	3	240		
IT Security Design Specialist	Enterprise eGRC	3	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	240		
Network Security Analyst	SIEM	3	240		
Incidental Management Specialist	SIEM	3	240		
			Total Price Contract Period One		$ **<TBD>**

Contract Period Two (YR. 2)

(A)	(B)	(C)	(D)	(E)	(F)
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Engineer	Configuration Management	3	240	$	$
IT Security Engineer	Information Exchange Gateway (IEG)	2	240	$	$
IT Security Engineer	Cyber Security Reference Architecture	3	240		
IT Security Engineer	Cross Domain Solution - Access	3	240		

IT Security Engineer	Cross Domain Solution - Transfer	2	480		
IT Security Engineer	TS IEG / TS Zoning	2	240		
IT Security Engineer	Network Security Monitoring (NSM)	3	240		
IT Security Design Specialist	Full Packet Capture	2	240		
IT Security Design Specialist	Host Security	2	240		
IT Security Design Specialist	ICAM and PKI	3	720		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		
IT Security Design Specialist	Cross Domain Solution - Access	3	240		
IT Security Design Specialist	Host Security	3	240		
IT Security Design Specialist	Network Security - Content Inspection	3	240		
IT Security Design Specialist	Enterprise eGRC	3	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	240		
Network Security Analyst	SIEM	3	240		
Incidental Management Specialist	SIEM	3	240		
				Total Price Contract Period One	$ **<TBD>**

Contract Period Three (YR. 3)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Engineer	Configuration Management	3	240	$	$
IT Security Engineer	Information Exchange Gateway (IEG)	2	240	$	$
IT Security Engineer	Cyber Security Reference Architecture	3	240		
IT Security Engineer	Cross Domain Solution - Access	3	240		
IT Security Engineer	Cross Domain Solution - Transfer	2	480		
IT Security Engineer	TS IEG / TS Zoning	2	240		
IT Security Engineer	Network Security Monitoring (NSM)	3	240		
IT Security Design Specialist	Full Packet Capture	2	240		
IT Security Design Specialist	Host Security	2	240		
IT Security Design Specialist	ICAM and PKI	3	720		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		
IT Security Design Specialist	Cross Domain Solution - Access	3	240		

IT Security Design Specialist	Host Security	3	240		
IT Security Design Specialist	Network Security - Content Inspection	3	240		
IT Security Design Specialist	Enterprise eGRC	3	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	240		
Network Security Analyst	SIEM	3	240		
Incidental Management Specialist	SIEM	3	240		
				Total Price Contract Period One	$ **<TBD>**

Option Periods:

Option Period 1 (YR. 4)					
(A)	**(B)**	**(C)**	**(D)**	**(E)**	**(F)**
Resource Category	**Specific Task Title**	**Level**	**Estimated Number of Days**	**Firm Per Diem Rate or Median Rate (if applicable)**	**Total Cost (D x E)**
IT Security Engineer	Configuration Management	3	240	$	$
IT Security Engineer	Information Exchange Gateway (IEG)	2	240	$	$
IT Security Engineer	Cyber Security Reference Architecture	3	240		
IT Security Engineer	Cross Domain Solution - Access	3	240		
IT Security Engineer	Cross Domain Solution - Transfer	2	480		

IT Security Engineer	TS IEG / TS Zoning	2	240		
IT Security Engineer	Network Security Monitoring (NSM)	3	240		
IT Security Design Specialist	Full Packet Capture	2	240		
IT Security Design Specialist	Host Security	2	240		
IT Security Design Specialist	ICAM and PKI	3	720		
IT Security Design Specialist	Information Exchange Gateway (IEG)	3	240		
IT Security Design Specialist	Cross Domain Solution - Access	3	240		
IT Security Design Specialist	Host Security	3	240		
IT Security Design Specialist	Network Security - Content Inspection	3	240		
IT Security Design Specialist	Enterprise eGRC	3	240		
Network Security Analyst	Network Security Monitoring (NSM)	3	240		
Network Security Analyst	SIEM	3	240		
Incidental Management Specialist	SIEM	3	240		
				Total Price Contract Period One	$ **<TBD>**

Total Bid Price:	
(Total Price Contract Period One + Total Price Contract Period Two + Total Price Contract Period Three + Total Price Option Period One)	$ **<TBD>**

ATTACHMENT 5.1

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY - CERTIFICATION

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

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

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

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the Employment Equity Act.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 permanent full-time and/or permanent part-time employees.

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

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

OR

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

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

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

ANNEX A – STATEMENT OF WORK
WORKSTREAM 1 - SECRET

1. BACKGROUND

1.1. The Directorate Information Management Engineering and Integration (DIMEI), leads the Department of National Defence/Canadian Armed Forces (DND/CAF) in the engineering, testing and integration of Information Management / Information Technology (IM/IT) infrastructure capabilities. DIMEI supports the Defence Chief Information Officer (DCIO) as Chief Engineer and Chief Architect, and is also involved in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and cyber security. DIMEI identifies opportunities within the current technical architecture to improve efficiency, reduce complexity and costs, and to increase interoperability with partner organisations. The section responsible for Cyber Security Engineering and Architecture Services is currently known as DIMEI 3.

1.2. The Cyber Security Engineering and Architecture Services (DIMEI 3) consists of 6 core services:

1.2.1. Technical Security Guidance: Consist of the development, interpretation, or implementation of technical IT security standards, and related processes;

1.2.2. Identity Credential and Access Management: Consists of the implementation and enhancement of DND enterprise Public Key Infrastructure (PKI) solutions and to establish PKI interoperability with other departments and allies;

1.2.3. Network Security: Consists of the transformation of network security through Availability Protection, Transmission Integrity and Transmission Confidentiality of DND networks; and perimeter security by providing content inspection, identification, authorization and logging of traffic when traversing network perimeters;

1.2.4. Host, Application and Data Security: Consists of engineering, guidance and integration support to implement validated host, application and data security solutions in DND/CAF environments;

1.2.5. Monitoring and Response: Consists of engineering, deployment and support of Logging, Audit and Monitoring technical solutions in support of the Department's Cyber Threat Detection and Misuse Detection missions; and

1.2.6. Security Engineering and Validation: Consists of assessing the technical security posture of systems prior to the implementation portion of a given System Design Life Cycle.

2. OBJECTIVE

2.1. This requirement is for the provision of IM/IT Engineering and Architecture services to DND. Work performed under this Contract will provide support for all IM/IT systems and services in the Classified and Designated Domains related to the cyber security of the previously defined six core services.

3. SCOPE

3.1. The work will involve planning and implementing new capabilities as well as enhancing existing capabilities. There will be a variety of products and equipment to be supported which will generate requirements for different knowledge, skills and experience.

3.2. Resources will be working primarily with DND DIMEI personnel. However, there will be occasions when resources will be working with other DND organizations in support of initiatives to improve the security of IM/IT DND/CAF systems.

4. APPLICABLE DOCUMENTS

4.1. The Technical Authority (TA) will provide resources with documents as required to successfully accomplish the assigned tasks. Resources must perform the work in accordance with the DND/CAF approved versions of these documents.

4.2. Resources must keep all documents and proprietary information confidential and maintain all documentation in a secure area. All materials belonging to DND must be returned upon completion of the Contract.

5. CONSTRAINTS

5.1. Resources must be available to work on DND premises within the National Capital Region (NCR) between the hours of 07:00 to 18:00, Monday to Friday (with the exception of statutory holidays as defined by the province of work), unless otherwise agreed upon by the Contractor and the TA.

5.2. All work performed outside of normal business hours must be pre-approved by the TA in writing. Should a resource anticipate that the 7.5 hour workday stipulated in the contract may be exceeded, approval must be obtained from the TA prior to work being carried out in excess of such period.

6. TRANSITION PERIOD

6.1. In order to ensure continuity, a Transition Period will be required following contract award to the new Contractor of this requirement. This Transition Period is intended to allow the new Contractor to prepare resources, assume responsibility and reach a steady state of activity and also to allow the incumbent Contractor to complete specific ongoing activities. The incumbent transfers responsibility for current and planned activities at the end of this Transition Period to the new Contractor.

6.1.1. The Transition Period will commence at date of contract award and be for a duration of approximately two (2) months following contract award. In order to ensure a transition from the current support IM/IT Engineering and Architecture services to the full implementation of the services depicted in this SOW, with no break in support and no disruption to DND processes and operations, the Contractor will be required to complete the following:

6.1.1.1. The Contractor must provide a detailed Transition Plan, within three (3) weeks after contract award, in accordance with the agreed timelines, to ensure that all resources and activities will transition efficiently and allow for orderly and timely set up in order to fully meet all DND requirements of the SOW. Transition Plan development will be done in collaboration with DND and will be approved by the Technical Authority; and

6.1.1.2. In accordance with the Transition Plan, the transition concludes with the transfer of responsibilities from the incumbent to the Contractor.

6.2. Transition Plan: the Contractor must describe its approach, methodology and risk assessment management for meeting the requirements of the Transition Period.

6.2.1. The description must include, as a minimum, the following components:

a. Scope, goals and objective of the transition;
b. The activities to be accomplished during the Transition Period;
c. The resources and level of effort to accomplish each of the activities;
d. The roles and responsibilities of key personnel;
e. Risk assessment management; and
f. Proposed timelines for all activities and sub-activities related milestones.

7. TASKS AND DELIVERABLES

7.1. **C.2 - Information Technology Security Methodology, Policy and Procedures Analyst - Level 2**

Specific Task Title: Security Technical Implementation Guide

The Level 2 IT Security Methodology, Policy and Procedures Analysts (Security Technical Implementation Guide) must:

7.1.1. Create work plans and schedules of work;
7.1.2. Provide guidance on the technical implementation of various standardized security control guidelines;
7.1.3. Provide guidance on Security Content Automation Protocol (SCAP);
7.1.4. Compose security policy and/or requirements documentation;
7.1.5. Conduct technical configurations (e.g. build, system design, hardening guides, test plans, etc.) and compose engineering implementation documentation for new security products;
7.1.6. Perform security architecture design and engineering support;
7.1.7. Write technical reports such as options analysis or technical architecture documents;
7.1.8. Produce security advisories and reports based on the analysis of security data;
7.1.9. Provide input to DIMEI teams on the technical implementation of hardening for:
7.1.9.1. Hypervisors and operating systems (e.g.: VMWare, Microsoft Windows, etc.);
7.1.9.2. Client or server applications (e.g.: web browsers, email servers, etc.); and
7.1.9.3. Networking devices (e.g.: routers, load balancers, etc.).
7.1.10. Implement test automation and automated configuration validation;
7.1.11. Develop and implement Secure Technical Implementation Guides (STIGs);
7.1.12. Participate in weekly or bi-weekly meetings and working groups as requested by the TA; and
7.1.13. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.2. **C.5 – Public Key Infrastructure (PKI) Specialist - Level 3**

Specific Task Title: PKI

The Level 3 Public Key Infrastructure (PKI) Specialists must:

7.2.1. Create work plans and schedules of work;

7.2.2. Review, design, and develop PKI-related engineering process documents including but not limited to: requirements, solution architectures, build and configuration documents, test plans, standard operating procedures (SOPs), user guides, system performance and capacity planning metrics and business continuity planning and disaster recovery;

7.2.3. Review, analyse and integrate PKI solutions into enterprise services including:

7.2.3.1. Active Directory;

7.2.3.2. X.500 directory services;

7.2.3.3. Malicious code and host-based protection; and/or

7.2.3.4. Firewall services;

7.2.4. Develop and enable PKI with the following existing technologies:

7.2.4.1. Firewall;

7.2.4.2. Email;

7.2.4.3. Webserver; and

7.2.4.4. Active Directory.

7.2.5. Architect, design, develop, test, document and implement PKI solutions including but not limited to, Microsoft Certificate Authority, Card Management Solution (CMS), identity management solutions, smart card technologies, smart card software and PKI-compliant applications;

7.2.6. Design, test, document and integrate PKI with Virtual Private Network solutions;

7.2.7. Develop PKI Certificate Policy, Certificate Practice Statements (CPS), and policy compliance inspection and audits;

7.2.8. Develop and provide training material package relevant to PKI; and

7.2.9. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.3. **C.6 – Information Technology Security Engineer - Level 3**

Specific Task Title: Network Security - Content Inspection

The Level 3 IT Security Engineers (Network Security - Content Inspection) must:

7.3.1. Create work plans and schedules of work;

7.3.2. Configure, integrate and troubleshoot firewalls;

7.3.3. Review, analyse and evaluate proxy technologies;

7.3.4. Configure, integrate and troubleshoot networking equipment;

7.3.5. Analyse, implement, and ensure compliance with Information Technology Security Guidance (ITSG) zoning and security control guidelines;

7.3.6. Integrate IT security solution proof of concepts into production;

7.3.7. Review, design, and develop engineering process documents including but not limited to: requirements, solution architectures, build and configuration documents, test plans, standard operating procedures (SOPs), user guides, system performance and capacity planning metrics and business continuity planning and disaster recovery;

7.3.8. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.3.9. Develop and provide awareness training material package relevant to IT security engineering; and

7.3.10. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.4. **C.7 – Information Technology Security Design Specialist - Level 2**

Specific Task Title: Host Security

The Level 2 IT Security Design Specialists (Host Security) must:

7.4.1. Create work plans and schedules of work;

7.4.2. Evaluate Host Security technologies and document an analysis for management;

7.4.3. Design, engineer, install, configure, and test endpoint protection security software in an enterprise environment;

7.4.4. Implement centrally managed host-based endpoint security policies;

7.4.5. Apply IT security end-point protection policies to an enterprise level system;

7.4.6. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.4.7. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.4.8. Develop and provide awareness training material package relevant to IT security design; and

7.4.9. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.5. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Information Exchange Gateway (IEG)

The Level 3 IT Security Design Specialist (Information Exchange Gateway) must:

7.5.1. Create work plans and schedules of work;

7.5.2. Design, engineer, install, configure, test, troubleshoot, support and maintain the following security networking equipment and technologies:

7.5.2.1. Guards and Gateways;

7.5.2.2. Firewalls;

7.5.2.3. Border Protection Services;

7.5.2.4. Data Diodes;

7.5.2.5. Web Proxies; and

7.5.2.6. Mail Transfer Agents.

7.5.3. Design, engineer, install, configure, test, troubleshoot, support and maintain the following IT products and infrastructure:

7.5.3.1. Microsoft Network Operating System;

7.5.3.2. IP Networks;

7.5.3.3. Application Integration; and

7.5.3.4. Virtualization.

7.5.4. Review, design, and develop engineering process documents including but not limited to: requirements, solution architectures, build and configuration documents, test plans, standard operating procedures (SOPs), user guides, system performance and capacity planning metrics and business continuity planning and disaster recovery;

7.5.5. Configure, integrate and provision networking equipment and technologies;

7.5.6. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.5.7. Develop and provide awareness training material package relevant to IT security design; and

7.5.8. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.6. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Network Security – Content Inspection

The Level 3 IT Security Design Specialist (Network Security - Content Inspection) must:

7.6.1. Create work plans and schedules of work;

7.6.2. Configure, integrate and provision network load balancers;

7.6.3. Review, analyse and evaluate Intrusion Detection Systems (IDS), application aware traffic generators, and encryption technologies;

7.6.4. Configure, integrate and troubleshoot firewalls;

7.6.5. Configure, integrate and troubleshoot networking equipment;

7.6.6. Analyse, implement, and ensure compliance on supported networks in accordance with Information Technology Security Guidance (ITSG) zoning and security control guidelines as issued from the Communications Security Establishment (CSE);

7.6.7. Integrate IT security solution proof of concepts into production;

7.6.8. Review, design, and develop engineering process documents including but not limited to: requirements, solution architectures, build and configuration documents, test plans, standard operating procedures (SOPs), user guides, system performance and capacity planning metrics and business continuity planning and disaster recovery;

7.6.9. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.6.10. Develop and provide awareness training material package relevant to IT security design; and

7.6.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.7. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Virtualization Security

The Level 3 IT Security Design Specialists (Virtualization Security) must:

7.7.1. Prepare work plans and schedules of work;

7.7.2. Configure, integrate and implement virtualization technologies;

7.7.3. Design virtual desktop infrastructure solutions;

7.7.4. Review, design, and develop engineering process documents including but not limited to: requirements, solution architectures, build and configuration documents, test plans, standard operating procedures (SOPs), user guides, system performance and capacity planning metrics and business continuity planning and disaster recovery;

7.7.5. Analyse, implement, and ensure compliance on supported networks in accordance with Information Technology Security Guidance (ITSG) zoning and security control guidelines as issued from the Communications Security Establishment (CSE);

7.7.6. Provide guidance to properly secure virtualized infrastructures;

7.7.7. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.7.8. Develop and provide awareness training material package relevant to IT security design; and

7.7.9. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.8. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

The Level 3 IT Security Design Specialist (National Endpoint Protection System In-Service Support) must:

7.8.1. Prepare work plans and schedules of work;

7.8.2. Design, build, test and implement Stormshield Endpoint Security Software (Version 7.x or higher) in an enterprise environment;

7.8.3. Design, build, test and implement Symantec Enterprise Protection security solution (Version 12.x or higher) in an enterprise environment;

7.8.4. Analyse Endpoint Security tools and techniques and document potential IT security threats to DIMEI's systems;

7.8.5. Review detailed security logs and security user to provide trend analysis, advisories and reports of possible IT security threats;

7.8.6. Analyse IT security statistics;

7.8.7. Prepare technical reports such as requirements analysis, options analysis, technical architecture documents, etc.;

7.8.8. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.8.9. Develop and provide awareness training material package relevant to IT security design; and

7.8.10. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.9. **C.8 – Network Security Analyst - Level 2**

Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

The Level 2 Network Security Analysts (National Endpoint Protection System In-Service Support) must:

7.9.1. Prepare work plans and schedules of work;

7.9.2. Support and maintain Symantec Endpoint Protection security software (Version 12.x or higher) in an enterprise environment;

7.9.3. Support and maintain McAfee ePolicy Orchestrator software in an enterprise environment;

7.9.4. Support and maintain Stormshield Endpoint Security software (Version 7.x or higher) in an enterprise environment;

7.9.5. Implement and maintain endpoint protection servers host-based firewall policies;

7.9.6. Implement and maintain endpoint protection servers host-based Intrusion Prevention Systems (HIPS) rules;

7.9.7. Implement, code and maintain F5 Big-IP iRules;

7.9.8. Configure and support various endpoint security software applications on Microsoft Windows 7, Windows 10, Windows Server 2008, and/or Windows Server 2012;

7.9.9. Installation, break/fix, backup and restore Microsoft Search and Query Language (SQL) databases;

7.9.10. Support and maintain Syslog servers;

7.9.11. Identify and analyse the technical threats to, and vulnerabilities of, networks;

7.9.12. Perform network security impact analysis for new software implementations, major configurations changes and patch management;

7.9.13. Participate in weekly or bi-weekly meetings and working groups as requested by the TA; and

7.9.14. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.10. **C.8 – Network Security Analyst - Level 2**

Specific Task Title: Information Exchange Gateway (IEG)

The Level 2 Network Security Analyst (Information Exchange Gateway) must:

7.10.1. Prepare work plans and schedules of work;

7.10.2. Design, engineer, install, configure, test, troubleshoot, support and maintain the following security networking equipment and technologies:

7.10.2.1. Firewalls;

7.10.2.2. Web Proxies; and

7.10.2.3. Mail Transfer Agents.

7.10.3. Review, design, and develop engineering process documents including but not limited to: requirements, solution architectures, build and configuration documents, test plans, standard operating procedures (SOPs), user guides, system performance and capacity planning metrics and business continuity planning and disaster recovery;

7.10.4. Configure and integrate networking equipment and technologies, including implementing dynamic routing protocols;

7.10.5. Configure, integrate and implement IP network technologies;

7.10.6. Configure, integrate and implement Windows Server 2008 (or more recent) Active Directory (AD) and Domain Name System (DNS);

7.10.7. Design and configure application traffic distribution using load balancers;

7.10.8. Configure, integrate and implement virtualization technologies;

7.10.9. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.10.10. Develop and provide awareness training material package relevant to IT security design; and

7.10.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.11. **C.8 – Network Security Analyst - Level 3**

Specific Task Title: Network Security Monitoring (NSM)

The Level 3 Network Security Analysts (Network Security Monitoring) must:

7.11.1. Prepare work plans and schedules of work;

7.11.2. Provide IT security incident detection, analysis and handling services;

7.11.3. Monitor and analyse security log files for IT security threats;

7.11.4. Monitor, configure, tune and optimize Security Information and Event Management tools and/or Full Packet Capture tools;

7.11.5. Review, develop and implement incident handling and escalation process flows;

7.11.6. Participate in weekly or bi-weekly meetings and working groups as requested by the TA; and

7.11.7. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

8. REPORTING REQUIREMENTS

8.1. A monthly progress report must be completed by the Contractor for each resource and submitted to the TA at the beginning of the following month, with a copy to accompany the monthly invoice. At a minimum, each progress report must document the following information:

8.1.1. All significant activities performed in the period covered that may impact the performance of the work;

8.1.2. Status of any outstanding activities that may extend beyond normal timelines;

8.1.3. Description of any problems encountered which will require attention or escalation; and

8.1.4. Any recommendations to update procedures.

8.2. All reports must be provided in a format acceptable to the TA.

9. LANGUAGE REQUIREMENTS

9.1. The individual Task Authorizations will specify the language requirements:

9.1.1. All tasks will require resources fluent in the English language. Fluent means that the individuals must be able to communicate orally and in writing without any assistance and with minimal errors.

10. LOCATION OF WORK

10.1. All work must be completed at DND facilities within the NCR.

11. TRAVEL

11.1. Costs associated with local travel within the NCR will not be reimbursed.

11.2. In the event that travel is required outside of the NCR during the period of this contract, 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 markup or profit. All travel outside of the NCR must be approved by the TA in advance, in writing.

ANNEX A – STATEMENT OF WORK
WORKSTREAM 2 – TOP SECRET

1. BACKGROUND

1.1. The Directorate Information Management Engineering and Integration (DIMEI), leads the Department of National Defence/Canadian Armed Forces (DND/CAF) in the engineering, testing and integration of Information Management / Information Technology (IM/IT) infrastructure capabilities. DIMEI supports the Defence Chief Information Officer (DCIO) as Chief Engineer and Chief Architect, and is also involved in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and cyber security. DIMEI identifies opportunities within the current technical architecture to improve efficiency, reduce complexity and costs, and to increase interoperability with partner organisations. The section responsible for Cyber Security Engineering and Architecture Services is currently known as DIMEI 3.

1.2. The Cyber Security Engineering and Architecture Services (DIMEI 3) consists of 6 core services:

1.2.1. Technical Security Guidance: Consist of the development, interpretation, or implementation of technical IT security standards, and related processes;

1.2.2. Identity Credential and Access Management: Consists of the implementation and enhancement of DND enterprise Public Key Infrastructure (PKI) solutions and to establish PKI interoperability with other departments and allies;

1.2.3. Network Security: Consists of the transformation of network security through Availability Protection, Transmission Integrity and Transmission Confidentiality of DND networks; and perimeter security by providing content inspection, identification, authorization and logging of traffic when traversing network perimeters;

1.2.4. Host, Application and Data Security: Consists of engineering, guidance and integration support to implement validated host, application and data security solutions in DND/CAF environments;

1.2.5. Monitoring and Response: Consists of engineering, deployment and support of Logging, Audit and Monitoring technical solutions in support of the Department's Cyber Threat Detection and Misuse Detection missions; and

1.2.6. Security Engineering and Validation: Consists of assessing the technical security posture of systems prior to the implementation portion of a given System Design Life Cycle.

2. OBJECTIVE

2.1. This requirement is for the provision of IM/IT Engineering and Architecture services to DND. Work performed under this Contract will provide support for all IM/IT systems and services in the Classified and Designated Domains related to the cyber security of the previously defined six core services.

ANNEX A – STATEMENT OF WORK
WORKSTREAM 2 – TOP SECRET

3. SCOPE

3.1. The work will involve planning and implementing new capabilities as well as enhancing existing capabilities. There will be a variety of products and equipment to be supported which will generate requirements for different knowledge, skills and experience.

3.2. Resources will be working primarily with DND DIMEI personnel. However, there will be occasions when resources will be working with other DND organizations in support of initiatives to improve the security of IM/IT DND/CAF systems.

4. APPLICABLE DOCUMENTS

4.1. The Technical Authority (TA) will provide resources with documents as required to successfully accomplish the assigned tasks. Resources must perform the work in accordance with the DND/CAF approved versions of these documents.

4.2. Resources must keep all documents and proprietary information confidential and maintain all documentation in a secure area. All materials belonging to DND must be returned upon completion of the Contract.

5. CONSTRAINTS

5.1. Resources must be available to work on DND premises within the National Capital Region (NCR) between the hours of 07:00 to 18:00, Monday to Friday (with the exception of statutory holidays as defined by the province of work), unless otherwise agreed upon by the Contractor and the TA.

5.2. All work performed outside of normal business hours must be pre-approved by the TA in writing. Should a resource anticipate that the 7.5 hour workday stipulated in the contract may be exceeded, approval must be obtained from the TA prior to work being carried out in excess of such period.

6. TRANSITION PERIOD

6.1. In order to ensure continuity, a Transition Period will be required following contract award to the new Contractor of this requirement. This Transition Period is intended to allow the new Contractor to prepare resources, assume responsibility and reach a steady state of activity and also to allow the incumbent Contractor to complete specific ongoing activities. The incumbent transfers responsibility for current and planned activities at the end of this Transition Period to the new Contractor.

6.1.1. The Transition Period will commence at date of contract award and be for a duration of approximately two (2) months following contract award. In order to ensure a transition from the current support IM/IT Engineering and Architecture services to the full implementation of the services depicted in this SOW, with no break in support and no disruption to DND processes and operations, the Contractor will be required to complete the following:

6.1.1.1. The Contractor must provide a detailed Transition Plan, within three (3) weeks after contract award, in accordance with the agreed timelines, to ensure that all resources and activities will transition efficiently and allow for orderly and timely set up in order to fully meet all DND requirements of the SOW. Transition Plan development will be done in collaboration with DND and will be approved by the Technical Authority; and

6.1.1.2. In accordance with the Transition Plan, the transition concludes with the transfer of responsibilities from the incumbent to the Contractor.

6.2. Transition Plan: the Contractor must describe its approach, methodology and risk assessment management for meeting the requirements of the Transition Period.

6.2.1. The description must include, as a minimum, the following components:

a. Scope, goals and objective of the transition;
b. The activities to be accomplished during the Transition Period;
c. The resources and level of effort to accomplish each of the activities;
d. The roles and responsibilities of key personnel;
e. Risk assessment management; and
f. Proposed timelines for all activities and sub-activities related milestones.

7. TASKS AND DELIVERABLES

7.1. **C.6 – Information Technology Security Engineer - Level 3**

Specific Task Title: Configuration Management

The Level 3 - IT Security Engineer (Configuration Management) must:

7.1.1. Create work plans and schedules of work;
7.1.2. Plan and implement IT security solutions for DND network environments;
7.1.3. Perform IT security architecture design and engineering support;
7.1.4. Plan, develop, implement and integrate vulnerability assessment solutions;
7.1.5. Develop and implement a vulnerability management program for a large scale DND organization;
7.1.6. Provide options analysis of the most recent IT security tools and techniques;
7.1.7. Perform analysis of security data (e.g. event monitoring, asset discovery, threat risks, incident reports, etc.) and provision of advisories and reports;
7.1.8. Plan, develop, implement and integrate IT asset discovery and configuration management database (CMDB) solutions;
7.1.9. Plan, develop, implement and integrate automated configuration compliance auditing solutions;

7.1.10. Review, design, and develop engineering and technical reports, including but not limited to: requirements analysis, hardening guides and technical architecture documents;

7.1.11. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.1.12. Develop and provide awareness training material package relevant to IT security engineering; and

7.1.13. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.2. **C.6 – Information Technology Security Engineer - Level 2**

Specific Task Title: Information Exchange Gateway (IEG)

The Level 2 - IT Security Engineer (Information Exchange Gateway) must:

7.2.1. Create work plans and schedules of work;

7.2.2. Engineer, design, configure, integrate and implement:

7.2.2.1. Firewall solutions;

7.2.2.2. Web proxy solutions;

7.2.2.3. Mail transfer agent (MTA) solutions;

7.2.2.4. Border Protection Service solutions;

7.2.2.5. SSL, HTTPS, HTTP, IPSec and SMTP solutions;

7.2.2.6. Virtualisation solutions; and

7.2.2.7. Windows 2008 (or more recent) Active Directory and Domain Name System.

7.2.3. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.2.4. Engineer, configure, integrate and provision of networking technologies;

7.2.5. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.2.6. Develop and provide awareness training material package relevant to IT security engineering; and

7.2.7. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.3. **C.6 – Information Technology Security Engineer - Level 3**

Specific Task Title: Cyber Security Reference Architecture

The Level 3 - IT Security Engineer (Cyber Security Reference Architecture) must:

7.3.1. Create work plans and schedules of work;

7.3.2. Review, identify, analyse, design, implement and manage IT security architectures;

7.3.3. Apply IT security risk management processes;

7.3.4. Design, implement and configure IT intrusion detection and protection methods;

7.3.5. Design, implement and configure system monitoring;

7.3.6. Design, implement and configure IT enterprise services such as directory, single sign-on, email, backup, or distributed database;

7.3.7. Design, implement and configure IT defence in depth principles;

7.3.8. Develop technical reports and engineering documents, including but not limited to: requirements analysis, configuration documents and technical architecture documents;

7.3.9. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.3.10. Develop and provide awareness training material package relevant to IT security engineering; and

7.3.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.4. **C.6 – Information Technology Security Engineer - Level 3**

Specific Task Title: Cross Domain Solution – Access

The Level 3 - IT Security Engineer (Cross Domain Solution - Access) must:

7.4.1. Create work plans and schedules of work;

7.4.2. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.4.3. Configure, integrate and implement Microsoft Windows Server 2008 (or more recent version), Active Directory (AD) and Domain Name System (DNS);

7.4.4. Design and implement network security controls and policies;

7.4.5. Configure and integrate firewall technologies;

7.4.6. Design and deliver virtual desktop services;

7.4.7. Design, configure and implement and change management of networking technologies;

7.4.8. Design, configure and implement of role-based and rule-based access control models;

7.4.9. Design, configure and implement IPSec tunneling schemes;

7.4.10. Analyse, configure, integrate and implement a broad range of security technologies including, but not limited to:

7.4.10.1. Directory Standards such as SMTP;

7.4.10.2. Networking Protocols such as HTTP, FTP and Telnet; and

7.4.10.3. Secure IT architecture fundamentals, standards, communications and security protocols such as IPSec, IPv6, SSL, TLS, SMTP and SSH;

7.4.11. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.4.12. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.4.13. Develop and provide awareness training material package relevant to IT security engineering; and

7.4.14. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.5. **C.6 – Information Technology Security Engineer Level 2**

Specific Task Title: Cross Domain Solution – Transfer

The Level 2 - IT Security Engineers (Cross Domain Solution - Transfer) must:

7.5.1. Create work plans and schedules of work;

7.5.2. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.5.3. Configure, integrate and implement Microsoft Windows Server 2008 (or more recent version) Active Directory (AD) and Domain Name System (DNS);

7.5.4. Configure and integrate the following:

7.5.4.1. High Assurance Guard technologies;

7.5.4.2. Firewall technologies; and/or

7.5.4.3. Mail Transfer Agent technologies;

7.5.5. Engineer, design, configure and integrate email content filters, data loss prevention and virtualized solutions;

7.5.6. Analyse, configure, integrate and implement a broad range of security technologies including, but not limited to:

7.5.6.1. Directory Standards such as SMTP;

7.5.6.2. Networking Protocols such as HTTP, FTP and Telnet; and

7.5.6.3. Secure IT architecture fundamentals, standards, communications and security protocols such as IPSec, IPv6, SSL, TLS, SMTP and SSH;

7.5.7. Engineer, configure, integrate and provision of networking technologies;

7.5.8. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.5.9. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.5.10. Develop and provide awareness training material package relevant to IT security engineering; and

7.5.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.6. **C.6 – Information Technology Security Engineer - Level 2**

Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

The Level 2 - IT Security Engineer (TS Information Exchange Gateway and TS Zoning) must:

7.6.1. Create work plans and schedules of work;

7.6.2. Configure and integrate the following:

7.6.2.1. Firewall technologies;

7.6.2.2. Web Proxy technologies;

7.6.2.3. Mail Transfer Agent technologies; and/or

7.6.2.4. Border Protection Service solutions;

7.6.3. Engineer, configure, integrate and implement a broad range of security technologies including, but not limited to:

7.6.3.1. Directory Standards such as SMTP;

7.6.3.2. Networking Protocols such as HTTP, FTP and Telnet; and

7.6.3.3. Secure IT architecture fundamentals, standards, communications and security protocols such as IPSec, IPv6, SSL, TLS, SMTP and SSH;

7.6.4. Engineer, configure, integrate and implement Microsoft Windows Server 2008 (or more recent version) Active Directory (AD) and Domain Name System (DNS);

7.6.5. Engineer, configure and integrate email content filters, data loss prevention and virtualized solutions;;

7.6.6. Engineer, configure integrate and provision of networking technologies;

7.6.7. Design network security monitoring solutions based on Information Technology Security Guidance (ITSG) zoning and security control guidelines;

7.6.8. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.6.9. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.6.10. Develop and provide awareness training material package relevant to IT security engineering; and

7.6.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.7. **C.6 - Information Technology Security Engineer - Level 3**

Specific Task Title: Network Security Monitoring (NSM)

The Level 3 - IT Security Engineer (Network Security Monitoring) must:

7.7.1. Create work plans and schedules of work;

7.7.2. Compose and maintain Security Information and Event Management (SIEM) or Full Packet Capture (FPC) technical documents;

7.7.3. Design network security monitoring solutions based on Information Technology Security Guidance (ITSG) zoning and security control guidelines;

7.7.4. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.7.5. Design, deploy and integrate SIEM tools and/or FPC tools in a production environment;

7.7.6. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.7.7. Develop and provide awareness training material package relevant to IT security engineering; and

7.7.8. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.8. **C.7 – Information Technology Security Design Specialist - Level 2**

Specific Task Title: Full Packet Capture

The Level 2 - IT Security Design Specialist (Full Packet Capture) must:

7.8.1. Create work plans and schedules of work;

7.8.2. Design, deploy, administer and troubleshoot local and wide-area network communication infrastructure components;

7.8.3. Administer Linux (or Linux variant);

7.8.4. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.8.5. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.8.6. Develop and provide awareness training material package relevant to IT security design; and

7.8.7. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.9. **C.7 – Information Technology Security Design Specialist - Level 2**

Specific Task Title: Host Security

The Level 2 - IT Security Design Specialist (Host Security) must:

7.9.1. Create work plans and schedules of work;

7.9.2. Evaluate Host Security technologies and provide detailed analysis for management;

7.9.3. Design, engineer, install, configure, and test endpoint protection security software in an enterprise environment;

7.9.4. Implement centrally managed host-based endpoint security policies;

7.9.5. Apply IT Security end-point protection policies to an enterprise level system;

7.9.6. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.9.7. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.9.8. Develop and provide awareness training material package relevant to IT security design; and

7.9.9. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.10. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

The Level 3 - IT Security Design Specialists (Identity, Credential and Access Management, and Public Key Infrastructure) must:

7.10.1. Create work plans and schedules of work;

7.10.2. Review, analyse and apply architectural methods, frameworks, and models such as TOGAF, US government FEAP, Canadian government BTEP, Zachman, SABSA Security Architecture Framework, etc.;

7.10.3. Review, analyse and apply:

7.10.3.1. IT security architectures and standards;

7.10.3.2. Market technologies and trends; and

7.10.3.3. Best practices and standards;

7.10.4. Produce and deliver IT security threat, implication, vulnerability and risk briefings to senior managers;

7.10.5. Analyse, design and establish PKI interoperability with other departments and allies;

7.10.6. Analyse and develop ICAM and PKI architecture requirements design, process development, and process mapping;

7.10.7. Perform Security Assessment and Authorization (SA&A) processes;

7.10.8. Review, design, and develop engineering process documents such as System Design Specifications, Standard Operating Procedures (SOP), Concept of Operations, System Implementation Plans, Life Cycle Support Plans, etc.;

7.10.9. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.10.10. Develop and provide awareness training material package relevant to IT security design; and

7.10.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.11. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Information Exchange Gateway (IEG)

The Level 3 - IT Security Design Specialist (Information Exchange Gateway) must:

7.11.1. Create work plans and schedules of work;

7.11.2. Design, engineer, install, configure, test, support and maintain the following IT products:

7.11.2.1. Guards and Gateways;
7.11.2.2. Firewalls;
7.11.2.3. Border Protection Services;
7.11.2.4. Data Diodes;
7.11.2.5. Web Proxies;
7.11.2.6. Mail Transfer Agent;
7.11.2.7. Microsoft Network Operating Systems;
7.11.2.8. IP Networks;
7.11.2.9. Application Integration; and
7.11.2.10. Virtualisation.

7.11.3. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.11.4. Configure, integrate, and provision networking technologies, including routers and switches;

7.11.5. Analyse, configure, integrate and implement a broad range of security technologies including, but not limited to:
7.11.5.1. Directory Standards such as SMTP;
7.11.5.2. Networking Protocols such as HTTP, FTP and Telnet; and
7.11.5.3. Secure IT architecture fundamentals, standards, communications and security protocols such as IPSec, IPv6, SSL, TLS, SMTP and SSH;

7.11.6. Configure, integrate and implement Microsoft Windows Server 2008 (or more recent version) Active Directory and Domain Name System in an enterprise level system;

7.11.7. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.11.8. Develop and provide awareness training material package relevant to IT security design; and

7.11.9. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.12. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Cross Domain Solution - Access

The Level 3 - IT Security Design Specialist (Cross Domain Solution - Access) must:

7.12.1. Create work plans and schedules of work;

7.12.2. Review, analyse and apply architectural methods, frameworks, and models such as TOGAF, US government FEAP, Canadian government BTEP and GSRM, Zachman, etc.;

7.12.3. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.12.4. Prepare technical reports for Cross Domain Solutions such as requirements analysis, options analysis, technical architecture documents, mathematical risk modeling, etc.;

7.12.5. Configure, integrate and implement Microsoft Windows Server 2008 (or more recent version) Active Directory (AD) and Domain Name System (DNS);

7.12.6. Perform the design implementation and change management of network security controls and policies;

7.12.7. Perform the design implementation and change management of virtual desktop services;

7.12.8. Perform the design implementation and change management of networking technologies;

7.12.9. Perform the design implementation and change management of role-based and rule-based access control models;

7.12.10. Perform the design implementation and change management of IPSec tunneling schemes;

7.12.11. Analyse IT Security tools and techniques related to Cross Domain Solutions;

7.12.12. Analyse security data and provide advisories and reports related to Cross Domain Solutions;

7.12.13. Perform security architecture design and engineering support;

7.12.14. Perform data security classification studies;

7.12.15. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.12.16. Develop and provide awareness training material package relevant to IT security design; and

7.12.17. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.13. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Host Security

The Level 3 - IT Security Design Specialist (Host Security) must:

7.13.1. Create work plans and schedules of work;

7.13.2. Evaluate Host Security technologies and provide analysis for management;

7.13.3. Design, engineer, install, configure, and test endpoint protection security software in an enterprise environment;

7.13.4. Implement centrally managed host-based endpoint security policies;

7.13.5. Apply IT Security end-point protection policies to an enterprise level system;

7.13.6. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.13.7. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.13.8. Develop and provide awareness training material package relevant to IT security design; and

7.13.9. Perform other tasks related to this labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.14. **C.7 – Information Technology Security Design Specialist - Level 3**

Specific Task Title: Network Security-Content Inspection

The Level 3 - IT Security Design Specialist (Network Security-Content Inspection) must:

7.14.1. Create work plans and schedules of work;

7.14.2. Review, analyse and ensure DND's conformity with Federal, Provincial and Territorial IT security policies, zoning and security control guidelines;

7.14.3. Integrate IT security solution proof of concepts into production environment;

7.14.4. Configure, integrate, troubleshoot and maintain firewalls in a production environment;

7.14.5. Configure, integrate and provision of networking technologies;

7.14.6. Configure, integrate and maintain virtualisation technology;

7.14.7. Configure and monitor intrusion detection systems;

7.14.8. Configure, integrate and provision of load balancers;

7.14.9. Participate in weekly or bi-weekly meetings and working groups as requested by the TA;

7.14.10. Develop and provide awareness training material package relevant to IT security design; and

7.14.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.15. **C.7 – Information Technology Security Design Specialist - Level 3**;

Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)

The Level 3 - IT Security Design Specialist (Enterprise Governance, Risk and Compliance (eGRC) must:

7.15.1. Create work plans and schedules of work;

7.15.2. Develop and implement an Enterprise Governance, Risk, and Compliance (eGRC) program;

7.15.3. Assess applied security controls, evaluate threats and risks to an IT system, and interpret and apply ITSG-33;

7.15.4. Define and implement different stages of an IT security project, such as defining requirements, engineer solutions, etc.

7.15.5. Review, design, and develop engineering process documents such as System Design Specifications, Build / Configuration documents, Concept of Operations, System Implementation Plans, Test Plans, Test Reports, Life Cycle Support Plans, etc.;

7.15.6. Review Security Assessment and Authorisation (SA&A) processes;

7.15.7. Analyse and provide reports on IT security architecture design;

7.15.8. Design network security monitoring solutions based on Information Technology Security Guidance (ITSG) zoning and security control guidelines;

7.15.9. Participate in weekly or monthly meetings and working groups as requested by the TA;

7.15.10. Develop and provide awareness training material package relevant to IT security design; and

7.15.11. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.16. **C.8 – Network Security Analyst - Level 3**;

Specific Task Title: Network Security Monitoring

The Level 3 - Network Security Analyst (Network Security Monitoring) must:

7.16.1. Create work plans and schedules of work;

7.16.2. Monitor and analyse security log files ;

7.16.3. Collect and analyse malicious code from hosts and network traffic;

7.16.4. Monitor, configure, and tune Security Information and Event Management (SIEM) tools or Full Packet Capture (FPC) tools;

7.16.5. Perform network security monitoring and log analysis to detect malicious activity;

7.16.6. Provide IT security incident detection, analysis and handling services using automated SIEM tools;

7.16.7. Operate and configure all aspects of a SIEM solution;

7.16.8. Review, develop and implement incident handling and escalation process flows;

7.16.9. Participate in weekly or monthly meetings and working groups as requested by the TA; and

7.16.10. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.17. **C.8 – Network Security Analyst - Level 3**

Specific Task Title: Security Information and Event Management (SIEM)

The Level 3 - Network Security Analyst (Security Information and Event Management) must:

7.17.1. Create work plans and schedules of work;

7.17.2. Monitor and analyse security log files;

7.17.3. Design and implement SIEM use cases for servers and workstations;

7.17.4. Build, configure and troubleshoot Linux servers;

7.17.5. Configure and provide technical support to SIEM tool ArcSight;

7.17.6. Deploy and operate all aspects of a SIEM solution;

7.17.7. Perform network security monitoring and log analysis to detect malicious activity;

7.17.8. Participate in weekly or monthly meetings and working groups as requested by the TA; and

7.17.9. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

7.18. **C.12 – Incident Management Specialist - Level 3;**

Specific Task Title: Security Information and Event Management (SIEM)

The Level 3 - Incident Management Specialist (Security Information and Event Management (SIEM) must:

7.18.1. Create work plans and schedules of work;

7.18.2. Implement and provide technical support for the SIEM tool ArcSight;

7.18.3. Design and implement SIEM use cases for servers and workstations;

7.18.4. Build, configure and troubleshoot Linux servers;

7.18.5. Review, design, and develop technical documents related to SIEM, such as Administrative Guidelines, In-Service Support Guidelines, Standard Operating Procedures, test plans, etc.;

7.18.6. Perform network security monitoring and log analysis to detect malicious activity;

7.18.7. Deploy and operate all aspects of a SIEM solution;

7.18.8. Participate in weekly or monthly meetings and working groups as requested by the TA; and

7.18.9. Develop and provide awareness training material package relevant to IT security design; and

7.18.10. Perform other tasks related to this TBIPS labour category as designated by the TA in support of the departmental IT Security and Cyber Protection Program.

8. REPORTING REQUIREMENTS

8.1. A monthly progress report must be completed by the Contractor for each resource and submitted to the TA at the beginning of the following month, with a copy to accompany the monthly invoice. At a minimum, each progress report must document the following information:

8.1.1. All significant activities performed in the period covered that may impact the performance of the work;

8.1.2. Status of any outstanding activities that may extend beyond normal timelines;

8.1.3. Description of any problems encountered which will require attention or escalation; and

8.1.4. Any recommendations to update procedures.

8.2. All reports must be provided in a format acceptable to the TA.

9. LANGUAGE REQUIREMENTS

9.1. The individual Task Authorizations will specify the language requirements:

9.1.1. All tasks will require resources fluent in the English language. Fluent means that the individuals must be able to communicate orally and in writing without any assistance and with minimal errors;

10. LOCATION OF WORK

10.1. All work must be completed at DND facilities within the NCR.

ANNEX A – STATEMENT OF WORK
WORKSTREAM 2 – TOP SECRET

11. TRAVEL

11.1. Costs associated with local travel within the NCR will not be reimbursed.

11.2. In the event that travel is required outside of the NCR during the period of this contract, 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 markup or profit. All travel outside of the NCR must be approved by the TA in advance, in writing.

APPENDIX C TO ANNEX A

RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLE

WORKSTREAM 1 - SECRET

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

RESOURCE CRITERIA

MANDATORY CRITERIA

C.2 - Information Technology Security Methodology, Policy and Procedures Analyst - Level 2
Specific Task Title: Security Technical Implementation Guide

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.2 - Information Technology Security Methodology, Policy and Procedures Analyst - Level 2 Specific Task Title: Security Technical Implementation Guide				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the past ten (10) years authoring security policy and/or requirements documentation.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the past ten (10) years authoring technical configuration and/or implementation documentation.			
	Compliant (Yes/No)?			

C.5 Public Key Infrastructure (PKI) Specialist – Level 3
Specific Task Title: PKI

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.5 Public Key Infrastructure (PKI) Specialist – Level 3 Specific Task Title: PKI				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience within the past fifteen (15) years designing and delivering PKI solutions.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years developing System Engineering documentation (e.g. Options Analysis, Design, Build, Test and Implementation)			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of combined experience within the past five (5) years integrating PKI solutions with enterprise services including: • Active Directory; • X.500 directory services; • Malicious code and host-based protection; and • Firewall services.			
	Compliant (Yes/No)?			

C.6 Information Technology Security Engineer – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as an IT Security Engineer.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of combined experience within the past eight (8) years configuring, integrating and troubleshooting Firewalls.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years configuring and integrating networking equipment.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the past ten (10) years engineering secure environments while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of combined experience within the past seven (7) years designing, engineering, installing, configuring, and testing endpoint protection security capabilities in an enterprise IT environment. Endpoint protection security capabilities experience must include two (2) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME).			
M3	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience applying IT Security end-point protection policies in an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following security networking equipment: • Guards and Gateways; • Firewalls; • Border Protection Services; • Data Diodes; • Web proxies; and • Mail Transfer Agent. A minimum of two years of experience is required for each of the above technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M2	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following IT products and infrastructure: • Microsoft Network Operating System; • IP Networks; • Applications Integration; and • Virtualization. A minimum of three years of experience is required for each of the above technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the past six (6) years working with common classified networks at the Secret and/or Top Secret level.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years configuring and integrating networking equipment.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the past eight (8) years configuring, integrating and troubleshooting Firewalls.			
M5	The Contractor must demonstrate that the resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Virtualization Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Virtualization Security				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of eight (8) years of experience working with virtualization technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as an Information Technology Security Design Specialist			
M2	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience within the past eight (8) years in the architectural design, build, test, implementation, and in-service support of Stormshield Endpoint Security Software to an enterprise wide environment of at least 15,000 users.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 2
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 2 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years working as a Network Security Analyst			
M2	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience within the past five (5) years maintaining Symantec Endpoint Protection security software in an enterprise environment of at least 15,000 users.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience within the past five (5) years maintaining McAfee ePolicy Orchestrator software in an enterprise environment of at least 15,000 users.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience within the past five (5) years maintaining Stormshield Endpoint Security software in an enterprise environment of at least 15,000 users.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 2
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 2 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating network technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as a Network Security Analyst.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the past ten (10) years monitoring and analyzing security log files from an enterprise network of at least 500 users.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the past eight (8) years monitoring, configuring and tuning Security Information and Event Management (SIEM) tools and/or Full Packet Capture tools in a production environment.			
	Compliant (Yes/No)?			

RATED CRITERIA

C.2 - Information Technology Security Methodology, Policy and Procedures Analyst - Level 2
Specific Task Title: Security Technical Implementation Guide

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.2 - Information Technology Security Methodology, Policy And Procedures Analyst - Level 2 Specific Task Title: Security Technical Implementation Guide					
R1	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years performing security architecture design.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on or implementing security hardening of hypervisors and operating systems (e.g. VMware vSphere, Microsoft Hyper-V, Microsoft Windows, Unix/Linux, etc.).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on or implementing the security hardening of client or server applications (e.g. web browsers, document viewers/editors, database servers, email servers, web servers, etc.).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on implementing the security hardening of networking devices (e.g. routers, switches, load balancers, proxies, etc.).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R5	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years implementing test automation and automated configuration validation.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R6	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years developing or implementing baseline technical security configurations.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R7	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on Security Content Automation Protocol (SCAP) complaint configuration tests **or** implementing SCAP compliant configuration tests.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 22 points**	**Maximum Score: 31 points**		

C.5 Public Key Infrastructure (PKI) Specialist – Level 3
Specific Task Title: PKI

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.5 Public Key Infrastructure (PKI) Specialist – Level 3 Specific Task Title: PKI					
R1	The Contractor should demonstrate that the proposed resource has a minimum of one (1) year of experience within the past seven (7) years enabling PKI with one or more of the following technologies for an IM/IT project: 1) Firewall; 2) Email; 3) Webserver; and 4) Active Directory	1 point = minimum experience demonstrated for enabling PKI with one of the listed technologies for an IM/IT project. 2 points = minimum experience demonstrated for enabling PKI with two of the listed technologies for an IM/IT project. 3 points = minimum experience demonstrated for enabling PKI with three of the listed technologies for an IM/IT project. 4 points = minimum experience demonstrated for enabling PKI with four of the listed technologies for an IM/IT project.	4		
R2	The Contractor should demonstrate that the proposed resource has a minimum of one (1) year of experience within the past seven (7) years integrating smart card technology with PKI.	2 points = minimum experience demonstrated integrating one (1) smart card technology with PKI. 3 points = minimum experience demonstrated integrating two (2) or more smart card technologies with PKI.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource experience within the past seven (7) years integrating PKI with Virtual Private Network (VPN) (secure remote access) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience designing and deploying Microsoft Certificate Authority 2012 or more recent versions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years integrating PKI with an identity management solution (such as Oracle and/or Tivoli).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years developing and implementing a PKI system Disaster Recovery plan.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years developing both Certificate Policies (CP) and Certificate Practice Statements (CPS).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource has experience within the past seven (7) years developing audit programs and auditing PKI deployments.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 25 points**		

C.6 Information Technology Security Engineer – Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 Information Technology Security Engineer – Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto VM-series firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience working with VMWare.	1 point: 2 to 4 years of experience. 2 points: >4 to 6 years of experience. 3 points: >6 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience working with McAfee Web Gateway.	1 point: 6 months to 1 year of experience. 2 points: >1 year of experience.	2		
R5	The Contractor should demonstrate that the proposed resource has experience working with Imperva Web Application Firewalls (WAF) and/or Database Activity Monitoring (DAM).	1 point: 6 months to 1 year of combined experience. 2 points: >1 to 2 years of combined experience. 3 points: >2 years of combined experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has experience working with network proxies.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: >1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience implementing Microsoft security capabilities in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience implementing McAfee host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience evaluating various security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Contractor provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required for the project to be considered.	3		
R6	The Contractor should demonstrate that the proposed resource has combined experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and/or 9) Other Content Inspection systems. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); and/or 4) Global Information Assurance Certification (GIAC) certification. A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall solutions such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco networking technologies including Routers and/or Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto VM-series firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience working with Intrusion Detection Systems (IDS).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware solutions.	1 point: 2 to 4 years of experience. 2 points: >4 to 6 years of experience. 3 points: >6 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning F5 load balancers.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience working with inline network encryption technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 22 points**		

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Virtualization Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Virtualization Security					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Hyper-V technology.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Contractor should demonstrate that the proposed resource has experience working with a virtualized data centre.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R4	The Contractor should demonstrate that the proposed resource has experience designing virtual desktop infrastructure (VDI) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R5	The Contractor should demonstrate that the proposed resource has experience designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has experience providing security guidance for virtualized infrastructures.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R7	The Contractor should demonstrate that the proposed resource has experience integrating 3rd party security controls into virtualized infrastructures.	2 points = 1 project. 3 points = 2 projects. 4 points = 3 or more projects. A minimum of 6 months of experience per project is required for the project to be considered.	4		
R8	The Contractor should demonstrate that the proposed resource has experience performing analysis or preparation of Business Continuity (BC) and Disaster Recovery plans (DR)	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
	Total:	**Minimum Passing Score: 22 points**	**Maximum Score: 32 points**		

C.7 IT Security Design Specialist – Level 3
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 IT Security Design Specialist – Level 3 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)					
R1	The Contractor should demonstrate that the proposed resource has experience in architecting Stormshield Endpoint Security solution at an enterprise level of at least 15,000 users.	3 points: >4 to 5 years of experience. 4 points: >5 to 6 years of experience. 5 points: >6 years of experience.	5		
R2	The Contractor should demonstrate that the proposed resource has experience in architecting Symantec Enterprise Protection security solution at an enterprise level of at least 15,000 users.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 to 7 years of experience. 4 points: >7 years of experience.	4		
R3	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies to an enterprise level system of at least 15,000 users.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R4	The Contractor should demonstrate that the proposed resource has combined experience analyzing the following: 1) IT Security tools and techniques; 2) Security data, provision of advisories and related reports; and/or 3) IT Security statistics.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 to 7 years of experience. 4 points: >7 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has combined experience writing technical reports such as requirement analysis, options analysis, and/or technical architecture documents.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 to 7 years of experience. 4 points: >7 years of experience.	4		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.8 Network Security Analyst – Level 2
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 Network Security Analyst – Level 2 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)					
R1	The Contractor should demonstrate that the proposed resource has experience implementing centrally managed host-based firewall policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has more than one (1) year of experience providing technical support for at least one of the following host-based security technologies, on an enterprise level environment of at least 15,000 users: 1) Stormshield Endpoint Security; 2) Symantec Endpoint Protection; and 3) McAfee ePolicy Orchestrator.	3 points: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 4 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 5 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	5		
R3	The Contractor should demonstrate that the proposed resource has experience implementing and coding F5 Big-IP iRules.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 to 3 years of experience. 4 points: >3 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has experience implementing centrally managed host-based Intrusion Detection System (IDS) rules.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 to 3 years of experience. 4 points: >3 years of experience.	4		
R5	The Contractor should demonstrate that the proposed resource has a minimum of two (2) years of combined experience supporting and configuring: 1) Windows 7; 2) Windows Server 2008; and/or 3) Windows Server 2012.	2 points: for achieving the minimum combined experience demonstrated for 1 of the listed operating systems. 3 points: for achieving the minimum combined experience demonstrated for each of 2 of the listed operating systems. 4 points: for achieving the minimum combined experience demonstrated for each of the 3 listed operating systems.	4		
R6	The Contractor should demonstrate that the proposed resource has experience supporting Syslog servers.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R7	The Contractor should demonstrate that the proposed resource has experience maintaining MS SQL (Microsoft Structured Query Language) databases.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 to 3 years of experience. 4 points: >3 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
	Total:	**Minimum Passing Score: 20 points**	**Maximum Score: 29 points**		

C.8 Network Security Analyst – Level 2
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 Network Security Analyst – Level 2 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall solutions such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience designing and configuring application traffic distribution using F5 products (DNS, LTM and BIGIP technologies).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Cisco networking technologies including dynamic routing protocols (e.g. BGP, OSPF), network separation (e.g. VRF, VLAN) and Network Address Translation (NAT).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R8	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Contractor should demonstrate that the proposed resource has experience within the past ten (10) years performing network security monitoring and log analysis to detect malicious activity.	1 point: >1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and optimizing production Security Information and Event Management System (SIEM) and/or Full Packet Capture solutions (excluding lab environments) for a large enterprise organization.	1 point: Experience achieved in an environment of 500 to 5000 users. 2 points: Experience achieved in an environment of >5000 to 10,000 users. 3 points: Experience achieved in an environment of >10,000 users.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience providing IT security incident detection, analysis and handling services using automated Security Information and Event Management System (SIEM) tool(s).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience operating and configuring all aspects of: 1) a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting; and/or 2) a Full Packet Capture solution including monitoring & capture, collection & metadata production, and analysis.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R6	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of experience reviewing, developing and implementing incident handling and escalation process flows in an IM/IT project.	1 point = 1 project. 2 points = 2 projects. 3 points = 3 or more projects. A minimum of 6 months of experience per project is required for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource holds one or more of the following certifications: 1) International Information System Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA); and/or 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 14 points**	**Maximum Score: 20 points**		

APPENDIX C TO ANNEX A

RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLE

WORKSTREAM 2 – TOP SECRET

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

RESOURCE CRITERIA

MANDATORY CRITERIA

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Configuration Management

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT security solutions.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years performing security architecture design or engineering support in the area of IT security.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the last ten (10) years, planning, developing, implementing and integrating vulnerability assessment solutions.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last eight (8) years, developing and implementing a vulnerability management program for an organization of at least 5,000 users.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience applying Government IT Security policies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cyber Security Reference Architecture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the design, planning, and/or implementation of information technology services, such as web services, database services, directory services, user access services, virtualized environments, and/or virtual desktops.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the review, design, planning, and/or implementation of security services, or security architectures for IT systems supporting more than 100 users.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience authoring technical configuration or implementation documentation.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience developing, configuring and testing of network security controls and policies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience designing and delivering virtual desktop services.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience designing, configuring and implementing role and rule-based access control models.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M6	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing, configuring and implementing IPSec tunneling schemes.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Cross Domain Solution – Transfer

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating High Assurance Guard technologies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience configuring and integrating Firewall technologies.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience engineering, designing, configuring and integrating e-mail content filter (such as malware prevention) and data loss prevention (such as label checking and word checking) technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Engineer.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of combined experience composing and maintaining Security Information and Event Management (SIEM) and/or Full Packet Capture (FPC) technical and engineering documentation.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing and implementing network security monitoring use cases in an enterprise deployment.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last ten (10) years designing, deploying and integrating SIEM tools and/or Full Packet Capture (FPC) tools in a production environment.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Full Packet Capture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Full Packet Capture				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years, designing, deploying, administering and troubleshooting local and wide-area network communications infrastructure components.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years performing system administration with Linux or a Linux variant.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of combined experience, within the last seven (7) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include two (2) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience applying IT Security end-point protection policies in an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years developing security architecture design for a Government classified solution (SECRET and above).			
M3	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience using at least one (1) of the following architectural methods/frameworks within the past seven (7) years: • TOGAF; • US government FEAP; • Canadian government BTEP; • Zachman; and/or • SABSA Security Architecture Framework			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years conducting detailed ICAM solution requirements analysis, design and implementation.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Contractor must demonstrate that the proposed resource has a minimum of one (1) year of experience briefing senior managers (Director level and above) on IT security implications and recommended courses of action.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following security networking technologies: • Guards and Gateways; • Firewalls; • Border Protection Services; • Data Diodes; • Web proxies; and • Mail Transfer Agent. A minimum of two years of experience is required for each of the above technologies.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following IT products and infrastructure: • Microsoft Network Operating System; • IP Networks; • Applications Integration; and • Virtualization. A minimum of three years of experience is required for each of the above technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M3	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last six (6) years working with common classified networks at the Secret and/or Top Secret level.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Cross Domain Solution - Access				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT Security integration architectures.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of experience in the design, implementation and change management of network security controls and policies.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of virtual desktop services.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of role- and rule-based access control models.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of IPSec tunneling schemes.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Host Security				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience designing and implementing IT security solutions.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience, within the last eight (8) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include three (3) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years applying IT Security end-point protection policies to an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Contractor must demonstrate that the resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Contractor must demonstrate that the proposed resource has a minimum ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years configuring and integrating networking equipment.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last ten (10) years designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years configuring, integrating and troubleshooting Firewalls.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience, within the last fifteen (15) years, working as an IT Security Design Specialist.			
M2	The Contractor must demonstrate that the proposed resource has at least two (2) years of experience, within the last five (5) years developing and implementing an Enterprise Governance, Risk, and Compliance (eGRC) solution for an organization of at least 5,000 users.			
M3	The Contractor must demonstrate that the proposed resource has at least two (2) years of experience within the last five (5) years in the assessment of applied Security Controls, the evaluation of Threats and Risks to an IT system, or the interpretation and application of Information Technology Security Guidance (ITSG) 33 Annex A.			
M4	The Contractor must demonstrate that the proposed resource has at least two (2) years of experience within the last ten (10) years defining requirements, translating business process into workflow, and engineering solutions in the definition and implementation stages of an IT Security project.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analysing security log files from an enterprise network of at least 500 users.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience with the collection and analysis of malicious code from hosts and network traffic.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last eight (8) years monitoring, configuring and tuning Security Information and Event Management (SIEM) tools and/or Full Packet Capture tools in a production environment.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last five (5) years configuring and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analyzing security log files from an enterprise network of at least 500 users.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
	Compliant (Yes/No)?			

C.12 Incident Management Specialist – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.12 Incident Management Specialist – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an Incident Management Specialist.			
M2	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years implementing and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M4	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
M5	The Contractor must demonstrate that the proposed resource has a minimum of two (2) years of experience composing and maintaining SIEM documents or SIEM engineering deliverables.			
	Compliant (Yes/No)?			

RATED CRITERIA

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Configuration Management

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience performing options analysis of IT security tools and techniques.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Contractor should demonstrate that the proposed resource has experience planning, developing, implementing and integrating IT asset discovery or configuration management database (CMDB) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has experience in planning, developing, implementing and integrating automated configuration compliance auditing solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R5	The Contractor should demonstrate that the proposed resource has experience writing technical reports such as requirements analysis, options analysis, and technical architecture documents.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R6	The Contractor should demonstrate that the proposed resource has experience developing hardening guides for IT systems.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The proposed resource should hold one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 – Information Technology Security Engineer - Level 2
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 – Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cyber Security Reference Architecture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture					
R1	The Contractor should demonstrate that the proposed resource has at least 6 months experience designing, or co-designing one major scale IT (Information Technology) environment for a minimum of 100 users.	IT supporting users: 3 points: 100 to 300 users. 4 points: >300 to 1000 users. 5 points: >1000 or more users.	5		
R2	The Contractor should demonstrate that the proposed resource has experience working in the application of IT Security Risk Management processes or System Security Engineering processes.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience designing or implementing and configuring IT Intrusion Detection and Protection methodologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience working with the design or implementing and configuring System Monitoring for accesses, changes or operational status.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience designing or implementing and configuring IT Enterprise Services, including directory, single sign-on, email, backup, or distributed database for an IT system supporting at least 500 users.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience designing or implementing and configuring IT Defence in Depth principles. The Contractor should also demonstrate and provide a description of how the resource applied the principles.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience working with a recognized enterprise architecture framework.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R8	The Contractor should demonstrate that the proposed resource has experience writing technical documents using desktop office-class tools, for audience at the corporate level.	1 point: 1 to 2 years of experience. 2 points: >2 to 4 years of experience. 3 points: >4 to 6 years of experience 4 points: >6 years of experience.	4		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: Cross Domain Solution – Transfer

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning					
R1	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Red Hat Enterprise Linux (RHEL).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R8	The Contractor should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last ten (10) years engineering network security monitoring solutions using at least three (3) of the following security technologies: 1) Host-based security; 2) IDS/IPS (Intrusion Prevention System); 3) Firewalls/UTMs; 4) Full Packet Capture; 5) Proxies; 6) Load Balancers; and 7) Matrix Switches/Taps.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience within the last ten (10) years designing network security monitoring solutions for the Government based on IT Security Directive (ITSD) 02 or IT Security Guidance (ITSG) 22 at the Protected B level or higher.	1 point per project up to a maximum 3 projects*† *If a Contractor provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		
R4	The Contractor should demonstrate that the proposed resource has experience providing IT security engineering services to Government departments and agencies in the form of security architecture development, advice and guidance.	1 point: 3 to 5 years of experience. 2 points: >5 to 7 years of experience. 3 points: >7 to 9 years of experience. 4 points: >9 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate the proposed resource holds one or more of the following IT security certifications: 1) International Information Systems Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA) A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 16 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Full Packet Capture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Full Packet Capture					
R1	The Contractor should demonstrate the proposed resource has experience within the last seven (7) years designing, planning and implementing network infrastructure of complex and highly available* environments. *Complex and highly available environments are defined as environments spanning multiple cities or countries with zero-downtime.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

R2	The Contractor should demonstrate that the proposed resource has combined experience within the last ten (10) years performing one or more of the following IT-related tasks: 1. Writing technical reports such as requirement analysis, options analysis, engineering process artefacts and/or technical architecture documents; 2. Automating the administration of Linux systems through scripting and APIs such as (but not limited to) Ruby, PHP, Bash, Perl or Python; 3. Analysis of raw network traffic capture to support troubleshooting or network forensics; 4. Deployment and administration of network forensics or traffic monitoring devices such as (but not limited to) FireEye, Solera, Sourcefire/Cisco IDS/IPS, SNORT or Netwitness (RSA Security Analytics); 5. Review alerts and packet-level data from IDS sensors/ packet capture devices;	1 point: 6 to 9 months of experience. 2 points: >9 to 12 months of experience. 3 points: >12 to 15 months of experience. 4 points: >15 months of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R2	6. Malware analysis and sandboxing with applications like (but not limited to) Netwitness Spectrum/RSA Malware, WireShark, CaptureBAT or Cuckoo Sandbox and the ability to reverse engineer and debug malware samples using tools such as (but not limited to) IDA Pro, Responder Pro or OllyDbg, including defeating anti debugging, packing and obfuscation techniques; and/or 7. Management of SAN and NAS technologies – Fibre Channel, FCOE, iSCSI, NFS, CIFS, including but not limited to the provisioning of LUNs, cabling, troubleshooting and patching. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.				

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has one or more of the following IT security certifications: 1) RSA Security Analytics Certified Administrator; 2) Any Cisco Associate level certification; 3) Any Cisco Professional level certification; 4) Any Cisco Expert level certification; 5) Any SANS GIAC certification in the Security Administration category; 6) Any Redhat Certified System Administrator, Engineer and/or architect certification; A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 8 points**	**Maximum Score: 12 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Host Security					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience implementing McAfee, Symantec or Trend-Micro host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, in an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Contractor should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Contractor should demonstrate that the proposed resource has experience evaluating various IT security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Contractor provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds at least one of the following IT security certifications: 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); and/or 4) Global Information Assurance Certification (GIAC) certification (any). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 26 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)					
R1	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years developing Standard Operating Procedures (SOP) on projects.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying PKI technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying Identity, Credential and Access Management (ICAM) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months experience designing IT solutions requiring interoperability with: • one or more GoC departments; and/or • one or more of the following International partners: US, UK, AUS, NZ.	1 point: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with GoC department(s). 2 points: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with International partner(s) (US, UK, AUS, NZ)	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years designing process mapping for a security architecture design.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall technologies, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions), Active Directory and Domain Name System in large (at least 1,000 users) IT networks.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has combined experience performing at least three (3) the following IT Security tasks: 1) Analysis of IT Security tools and techniques; 2) Analysis of security data and provision of advisories and reports; 3) Writing technical reports including requirements analysis, options analysis, technical architecture documents and mathematical risk modeling; 4) Security architecture design and engineering support; and 5) Data security classification studies. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions) Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience in design, implementation and change management of VMWare technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Contractor should demonstrate that the proposed resource holds one or more of the following architecture certifications: 1) Certification in The Open Group Architecture Framework (TOGAF); 2) Certification in Information Technology Service Management (ITSM); 3) Certification in Enterprise Architecture Center of Excellence (EACOE); 4) Certification in Microsoft Certified Architect (MCA); and/or 5) Certification in VMWare Certified Design Expert (VCDX). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Host Security					
R1	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience implementing McAfee host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Contractor should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, on an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Contractor should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Contractor should demonstrate that the proposed resource has experience evaluating various security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Contractor provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Contractor should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience working with Intrusion Detection Systems (IDS).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience working with VMWare.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has experience configuring, integrating and provisioning F5 load balancers.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience working with inline network encryption technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 25 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)					
R1	The Contractor should demonstrate that the proposed resource holds one or more of the following administrating IT GRC or eGRC application certifications: 1) RSA Archer Certified Administrator 2) IBM OpenPages Administrator 3) MetricStream GRC Certified Administrator A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R2	The Contractor should demonstrate that the proposed resource has combined experience within the last five (5) years authoring XML data transformation and/or translation scripts.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience with IT Security Design projects within an eGRC implementation environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years writing technical reports such as options analysis, and/or implementation plans.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has combined experience within the last five (5) years accrediting an IT system using the Security Assessment and Authorization (SA&A) process and/or the Certification and Accreditation (C&A) program.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years developing network security architectures (Level II or higher) based on IT Security Directives (ITSD) and /or IT Security Guidance (ITSG).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications	3		
	Total:	**Minimum Passing Score: 16 points**	**Maximum Score: 23 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last ten (10) years performing network security monitoring and log analysis to detect malicious activity.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and optimizing production Security Information and Event Management System (SIEM) and/or Full Packet Capture solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience providing IT security incident detection, analysis and handling services using automated Security Information and Event Management System (SIEM) tool(s).	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R4	The Contractor should demonstrate that the proposed resource has experience operating and configuring all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of experience reviewing, developing and implementing incident handling and escalation process flows in an IM/IT project.	1 point = 1 project. 2 points = 2 projects. 3 points = 3 or more projects. A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) International Information System Security Certification Consortium (ISC)2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE); A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 14 points**	**Maximum Score: 20 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		
R4	The Contractor should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		
R7	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		

C.12 – Incident Management Specialist - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.12 – Incident Management Specialist - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Contractor should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Contractor should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		
R4	The Contractor should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Contractor should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Contractor should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Contractor should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-17-P5LL S1 - Amendment 2
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
DND	DGIMTSP / DIMEI
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Professional services using the Task-Based Informatics Professional Services (TBIPS) supply arrangement on an as-required basis.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non ☐	Yes / Oui ☑
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	No / Non ☐	Yes / Oui ☑
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non ☐	Yes / Oui ☑
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	No / Non ☑	Yes / Oui ☐
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	No / Non ☑	Yes / Oui ☐

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

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

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☑	NATO SECRET / NATO SECRET ☑	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☑	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

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

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

☐ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☐ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☑ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted? — ☐ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

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

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — ☑ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

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

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-17-P5LL S2 - Amendment 2
Security Classification / Classification de sécurité UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine **DND**	2. Branch or Directorate / Direction générale ou Direction DGIMTSP / DIMEI
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

Professional services using the Task-Based Informatics Professional Services (TBIPS) supply arrangement on an as-required basis.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☐ No / Non	☑ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☐ No / Non	☑ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	**NATO / OTAN** ☑	**Foreign / Étranger** ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion ☐	All NATO countries Tous les pays de l'OTAN ☐	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☑		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☑	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays : Canada	Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☑	NATO SECRET / NATO SECRET ☑	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☑	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☑		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☑		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

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

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

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

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

☐ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☐ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☑ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☑ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? ☐ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

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

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? ☑ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

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

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S1

Part A - Multiple Release Restrictions: Security Guide

To be completed in addition to SRCL question 7.b) when release restrictions are therein identified. Indicate to which levels of information release restrictions apply. Make note in the chart if a level of information bears multiple restrictions (e.g. a portion of the SECRET information bears the caveat Canadian Eyes Only while the remainder of the SECRET information has no release restrictions.)

Canadian Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions	X	X					
Not Releasable							
Restricted to: Canada and USA				X	X		
Permanent Residents Included*							

NATO Information

Citizenship Restriction	NATO UNCLASSIFIED	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
All NATO Countries					
Restricted to: Canada and USA				X	
Permanent Residents Included*					

Foreign Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions							
Restricted to :							
Permanent Residents Included*							

COMSEC Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
Not Releasable							
Restricted to:							

***When release restrictions are indicated, specify if permanent residents are allowed to be included.**

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S1

Part B - Multiple Levels of Personnel Screening: Security Classification Guide **To be completed in addition to SRCL question 10.a) when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work/access involved in the contract.**			
Level of Personnel Clearance (e.g. Reliability Status, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
NATO SECRET	IT Security Methodology, Policy and Procedures Analyst (Level 2)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	PKI Specialist (Level 3)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	IT Security Engineer (Level 3)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	IT Security Design Specialist (Level 2 and 3)	Up to and including NATO Secret	Canadian or US citizen
NATO SECRET	Network Security Analyst (Level 2 and 3)	Up to and including NATO Secret	Canadian or US citizen

Part C – Safeguards / Information Technology (IT) Media – 11d = yes
IT security requirements must be specified in a separate technical document and submitted with the SRCL

OTHER SECURITY INTRUCTIONS

Insert instructions

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S2

Part A - Multiple Release Restrictions: Security Guide

To be completed in addition to SRCL question 7.b) when release restrictions are therein identified. Indicate to which levels of information release restrictions apply. Make note in the chart if a level of information bears multiple restrictions (e.g. a portion of the SECRET information bears the caveat Canadian Eyes Only while the remainder of the SECRET information has no release restrictions.)

Canadian Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions	X	X					
Not Releasable				X	X	X	X
Restricted to:							
Permanent Residents Included*							

NATO Information

Citizenship Restriction	NATO UNCLASSIFIED	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET
All NATO Countries					
Restricted to: Canada				X	
Permanent Residents Included*					

Foreign Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
No Release Restrictions							
Restricted to :							
Permanent Residents Included*							

COMSEC Information

Citizenship Restriction	PROTECTED			CLASSFIED			
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	TOP SECRET (SIGINT)
Not Releasable							
Restricted to:							

***When release restrictions are indicated, specify if permanent residents are allowed to be included.**

Security Requirement Checklist (SRCL) Supplemental Security Guide

W6369-17-P5LL S2

Part B - Multiple Levels of Personnel Screening: Security Classification Guide **To be completed in addition to SRCL question 10.a) when multiple levels of personnel screening are therein identified. Indicate which personnel screening levels are required for which portions of the work/access involved in the contract.**			
Level of Personnel Clearance (e.g. Reliability Status, Secret)	Position / Description/Task	Access to sites and/or information. Levels of Information to be accessed.	Citizenship Restriction (if any)
NATO Secret and Top Secret-SIGINT	IT Security Engineer (Level 2 and 3)	Up to and including Top Secret-SIGINT	Canadian citizen
NATO Secret and Top Secret-SIGINT	IT Security Design Specialist (Level 2 and 3)	Up to and including Top Secret-SIGINT	Canadian citizen
NATO Secret and Top Secret-SIGINT	Network Security Analyst (Level 3)	Up to and including Top Secret-SIGINT	Canadian citizen
NATO Secret and Top Secret-SIGINT	Incident Management Specialist (Level 3)	Up to and including Top Secret-SIGINT	Canadian citizen

Part C – Safeguards / Information Technology (IT) Media – 11d = yes
IT security requirements must be specified in a separate technical document and submitted with the SRCL

<u>OTHER SECURITY INTRUCTIONS</u>

Insert instructions

ATTACHMENT 4.1

BID EVALUATION CRITERIA

WORKSTREAM 1 - SECRET

1. The evaluation criteria contained in this attachment will be used to evaluate bids during the solicitation and to facilitate resource assessment after contract award.

2. The Bidder must provide a qualifying résumé for each of the Resource Categories requested for evaluation (the Bidder must not propose the same resource more than once in response to this solicitation).

3. The Bidder must complete an evaluation grid for each of the résumés being provided as described in Table 1 below. For each criterion the Bidder must indicate the section in the résumé where compliance with the criteria is described. Failure to provide a qualifying résumé for each Resource Category results in a non-responsive bid.

Table 1: Bidders must submit the following number of résumés per resource category in response to this evaluation. The actual numbers of resources required are listed in Part 1, 1.2 Summary, of the bid solicitation;

Resource Category with Specific Task Title	Level	Number of Résumés
C.2 IT Security Methodology, Policy and Procedures Analyst Specific Task Title: Security Technical Implementation Guide	2	1
C.5 PKI Specialist Specific Task Title: PKI	3	1
C.6 IT Security Engineer Specific Task Title: Network Security – Content Inspection	3	1
C.7 IT Security Design Specialist Specific Task Title: Host Security	2	1
C.7 IT Security Design Specialist Specific Task Title: Information Exchange Gateway (IEG)	3	1
C.7 IT Security Design Specialist Specific Task Title: Network Security – Content Inspection	3	1
C.7 IT Security Design Specialist Specific Task Title: Virtualization Security	3	1
C.7 IT Security Design Specialist Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)	3	1

C.8 Network Security Analyst Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)	2	1
C.8 Network Security Analyst Specific Task Title: Information Exchange Gateway (IEG)	2	1
C.8 Network Security Analyst Specific Task Title: Network Security Monitoring (NSM)	3	1

1. CORPORATE REQUIREMENTS

1.1. Corporate Mandatory Requirements

MANDATORY REQUIREMENTS – CORPORATE CRITERIA			
Item	**Mandatory Corporate Criteria**	**MET (Yes/No)**	**Page number(s) in bid**
M1	The Bidder must have been awarded at least 2 Government* informatics professional service† contracts. For each contract identified: 1. The value must be at least $5,000,000.00 ($5M) excluding applicable taxes; 2. The duration must be at least two (2) years within the last eight (8) years from the closing date of this solicitation and cannot include option periods that have not been exercised; 3. The Bidder must have provided at least five (5) resources simultaneously for a period of at least twelve (12) consecutive months; and Each contract used must also demonstrate that the Bidder has provided services to an organization with the following environment: • At least 100 workstations on a classified network or secret network; • Microsoft Windows workstation operating system (Windows XP, Windows Vista, Windows 7 and/or Windows 10); and • Centralized software distribution and patch management. The Bidder must provide one reference for each contract. The references must include the name of the organization, the unique contract identification number, a short description of the services provided, the name, title, email address and telephone number of the organization's responsible manager, the number of resources provided, as well as the award date, expiry date and dollar value of each contract. It is the Bidder's responsibility to ensure that any information divulged has the permission of the references provided. The Bidder must have been the prime contractor, rather than a subcontractor. This means that the Bidder contracted directly with the customer of the work. If the Bidder's contract was to perform work which another entity had itself first contracted to perform, the Bidder will not be considered the prime contractor. For example, Z (customer) contracted with Y for services. Y, in turn, entered into a contract with X to provide all or part of these services to Z. In this example, Y is a prime contractor and X is a subcontractor.		

	Bidders are reminded that a Supply Arrangement or Standing Offer is not a contract and therefore any reference to this type of document will not be accepted for the purpose of evaluating contract experience. For example if the Bidder references it's TBIPS SA number such as EN578-055605/XXX/EL for the purpose of demonstrating experience under the evaluation criteria, Canada will disregard this experience because it does not relate to a specific contract. * Government client may include a Federal, Provincial or Municipal Department/Agency or Crown Corporation. † Informatics Professional Services are professional services provided by the Bidder in support of an information technology or information management project or contract.		

RESOURCE CRITERIA

MANDATORY CRITERIA

C.2 - Information Technology Security Methodology, Policy and Procedures Analyst - Level 2
Specific Task Title: Security Technical Implementation Guide

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.2 - Information Technology Security Methodology, Policy and Procedures Analyst - Level 2 Specific Task Title: Security Technical Implementation Guide				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the past ten (10) years authoring security policy and/or requirements documentation.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the past ten (10) years authoring technical configuration and/or implementation documentation.			
	Compliant (Yes/No)?			

C.5 Public Key Infrastructure (PKI) Specialist – Level 3
Specific Task Title: PKI

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.5 Public Key Infrastructure (PKI) Specialist – Level 3 Specific Task Title: PKI				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience within the past fifteen (15) years designing and delivering PKI solutions.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years developing System Engineering documentation (e.g. Options Analysis, Design, Build, Test and Implementation)			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of combined experience within the past five (5) years integrating PKI solutions with enterprise services including: • Active Directory; • X.500 directory services; • Malicious code and host-based protection; and • Firewall services.			
	Compliant (Yes/No)?			

C.6 Information Technology Security Engineer – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as an IT Security Engineer.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of combined experience within the past eight (8) years configuring, integrating and troubleshooting Firewalls.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years configuring and integrating networking equipment.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the past ten (10) years engineering secure environments while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of combined experience within the past seven (7) years designing, engineering, installing, configuring, and testing endpoint protection security capabilities in an enterprise IT environment. Endpoint protection security capabilities experience must include two (2) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME).			
M3	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience applying IT Security end-point protection policies in an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following security networking equipment: • Guards and Gateways; • Firewalls; • Border Protection Services; • Data Diodes; • Web proxies; and • Mail Transfer Agent. A minimum of two years of experience is required for each of the above technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following IT products and infrastructure: • Microsoft Network Operating System; • IP Networks; • Applications Integration; and • Virtualization. A minimum of three years of experience is required for each of the above technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the past six (6) years working with common classified networks at the Secret and/or Top Secret level.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years configuring and integrating networking equipment.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the past eight (8) years configuring, integrating and troubleshooting Firewalls.			
M5	The Bidder must demonstrate that the resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Virtualization Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Virtualization Security				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of eight (8) years of experience working with virtualization technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as an Information Technology Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience within the past eight (8) years in the architectural design, build, test, implementation, and in-service support of Stormshield Endpoint Security Software to an enterprise wide environment of at least 15,000 users.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 2
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 2 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)				
M1	The Contractor must demonstrate that the proposed resource has a minimum of five (5) years of experience within the past ten (10) years working as a Network Security Analyst.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience within the past five (5) years maintaining Symantec Endpoint Protection security software in an enterprise environment of at least 15,000 users.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience within the past five (5) years maintaining McAfee ePolicy Orchestrator software in an enterprise environment of at least 15,000 users.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience within the past five (5) years maintaining Stormshield Endpoint Security software in an enterprise environment of at least 15,000 users.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 2
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 2 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating network technologies.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the past fifteen (15) years working as a Network Security Analyst.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the past ten (10) years monitoring and analyzing security log files from an enterprise network of at least 500 users.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the past eight (8) years monitoring, configuring and tuning Security Information and Event Management (SIEM) tools and/or Full Packet Capture tools in a production environment.			
	Compliant (Yes/No)?			

RATED CRITERIA

C.2 - Information Technology Security Methodology, Policy and Procedures Analyst - Level 2
Specific Task Title: Security Technical Implementation Guide

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.2 - Information Technology Security Methodology, Policy And Procedures Analyst - Level 2 Specific Task Title: Security Technical Implementation Guide					
R1	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years performing security architecture design.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on or implementing security hardening of hypervisors and operating systems (e.g. VMware vSphere, Microsoft Hyper-V, Microsoft Windows, Unix/Linux, etc.).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on or implementing the security hardening of client or server applications (e.g. web browsers, document viewers/editors, database servers, email servers, web servers, etc.).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on implementing the security hardening of networking devices (e.g. routers, switches, load balancers, proxies, etc.).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R5	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years implementing test automation and automated configuration validation.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R6	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years developing or implementing baseline technical security configurations.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R7	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years providing guidance on Security Content Automation Protocol (SCAP) complaint configuration tests **or** implementing SCAP compliant configuration tests.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Bidder should demonstrate that the proposed resource holds one or more of the following certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 22 points**	**Maximum Score: 31 points**		

C.5 Public Key Infrastructure (PKI) Specialist – Level 3
Specific Task Title: PKI

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.5 Public Key Infrastructure (PKI) Specialist – Level 3 Specific Task Title: PKI					
R1	The Bidder should demonstrate that the proposed resource has a minimum of one (1) year of experience within the past seven (7) years enabling PKI with one or more of the following technologies for an IM/IT project: 1) Firewall; 2) Email; 3) Webserver; and 4) Active Directory	1 point = minimum experience demonstrated for enabling PKI with one of the listed technologies for an IM/IT project. 2 points = minimum experience demonstrated for enabling PKI with two of the listed technologies for an IM/IT project. 3 points = minimum experience demonstrated for enabling PKI with three of the listed technologies for an IM/IT project. 4 points = minimum experience demonstrated for enabling PKI with four of the listed technologies for an IM/IT project.	4		
R2	The Bidder should demonstrate that the proposed resource has a minimum of one (1) year of experience within the past seven (7) years integrating smart card technology with PKI.	2 points = minimum experience demonstrated integrating one (1) smart card technology with PKI. 3 points = minimum experience demonstrated integrating two (2) or more smart card technologies with PKI.	3		
R3	The Bidder should demonstrate that the proposed resource experience within the past seven (7) years integrating PKI with Virtual Private Network (VPN) (secure remote access) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience designing and deploying Microsoft Certificate Authority 2012 or more recent versions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years integrating PKI with an identity management solution (such as Oracle and/or Tivoli).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years developing and implementing a PKI system Disaster Recovery plan.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years developing both Certificate Policies (CP) and Certificate Practice Statements (CPS).	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R8	The Bidder should demonstrate that the proposed resource has experience within the past seven (7) years developing audit programs and auditing PKI deployments.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 25 points**		

C.6 Information Technology Security Engineer – Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 Information Technology Security Engineer – Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto VM-series firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience working with VMWare.	1 point: 2 to 4 years of experience. 2 points: >4 to 6 years of experience. 3 points: >6 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience working with McAfee Web Gateway.	1 point: 6 months to 1 year of experience. 2 points: >1 year of experience.	2		
R5	The Bidder should demonstrate that the proposed resource has experience working with Imperva Web Application Firewalls (WAF) and/or Database Activity Monitoring (DAM).	1 point: 6 months to 1 year of combined experience. 2 points: >1 to 2 years of combined experience. 3 points: >2 years of combined experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Bidder should demonstrate that the proposed resource has experience working with network proxies.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R8	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: >1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience implementing Microsoft security capabilities in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience implementing McAfee host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience evaluating various security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Bidder provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required for the project to be considered.	3		
R6	The Bidder should demonstrate that the proposed resource has combined experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and/or 9) Other Content Inspection systems. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); and/or 4) Global Information Assurance Certification (GIAC) certification. A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall solutions such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco networking technologies including Routers and/or Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto VM-series firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience working with Intrusion Detection Systems (IDS).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware solutions.	1 point: 2 to 4 years of experience. 2 points: >4 to 6 years of experience. 3 points: >6 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning F5 load balancers.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience working with inline network encryption technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 22 points**		

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Virtualization Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Virtualization Security					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Hyper-V technology.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Bidder should demonstrate that the proposed resource has experience working with a virtualized data centre.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R4	The Bidder should demonstrate that the proposed resource has experience designing virtual desktop infrastructure (VDI) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R5	The Bidder should demonstrate that the proposed resource has experience designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Bidder should demonstrate that the proposed resource has experience providing security guidance for virtualized infrastructures.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R7	The Bidder should demonstrate that the proposed resource has experience integrating 3rd party security controls into virtualized infrastructures.	2 points = 1 project. 3 points = 2 projects. 4 points = 3 or more projects. A minimum of 6 months of experience per project is required for the project to be considered.	4		
R8	The Bidder should demonstrate that the proposed resource has experience performing analysis or preparation of Business Continuity (BC) and Disaster Recovery plans (DR)	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
	Total:	**Minimum Passing Score: 22 points**	**Maximum Score: 32 points**		

C.7 IT Security Design Specialist – Level 3
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 IT Security Design Specialist – Level 3 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)					
R1	The Bidder should demonstrate that the proposed resource has experience in architecting Stormshield Endpoint Security solution at an enterprise level of at least 15,000 users.	3 points: >4 to 5 years of experience. 4 points: >5 to 6 years of experience. 5 points: >6 years of experience.	5		
R2	The Bidder should demonstrate that the proposed resource has experience in architecting Symantec Enterprise Protection security solution at an enterprise level of at least 15,000 users.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 to 7 years of experience. 4 points: >7 years of experience.	4		
R3	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies to an enterprise level system of at least 15,000 users.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R4	The Bidder should demonstrate that the proposed resource has combined experience analyzing the following: 1) IT Security tools and techniques; 2) Security data, provision of advisories and related reports; and/or 3) IT Security statistics.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 to 7 years of experience. 4 points: >7 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has combined experience writing technical reports such as requirement analysis, options analysis, and/or technical architecture documents.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 to 7 years of experience. 4 points: >7 years of experience.	4		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.8 Network Security Analyst – Level 2
Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 Network Security Analyst – Level 2 Specific Task Title: National Endpoint Protection System In-Service Support (NEPS ISS)					
R1	The Bidder should demonstrate that the proposed resource has experience implementing centrally managed host-based firewall policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has more than one (1) year of experience providing technical support for at least one of the following host-based security technologies, on an enterprise level environment of at least 15,000 users: 1) Stormshield Endpoint Security; 2) Symantec Endpoint Protection; and 3) McAfee ePolicy Orchestrator.	3 points: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 4 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 5 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	5		
R3	The Bidder should demonstrate that the proposed resource has experience implementing and coding F5 Big-IP iRules.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 to 3 years of experience. 4 points: >3 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience implementing centrally managed host-based Intrusion Detection System (IDS) rules.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 to 3 years of experience. 4 points: >3 years of experience.	4		
R5	The Bidder should demonstrate that the proposed resource has a minimum of two (2) years of combined experience supporting and configuring: 1) Windows 7; 2) Windows Server 2008; and/or 3) Windows Server 2012.	2 points: for achieving the minimum combined experience demonstrated for 1 of the listed operating systems. 3 points: for achieving the minimum combined experience demonstrated for each of 2 of the listed operating systems. 4 points: for achieving the minimum combined experience demonstrated for each of the 3 listed operating systems.	4		
R6	The Bidder should demonstrate that the proposed resource has experience supporting Syslog servers.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R7	The Bidder should demonstrate that the proposed resource has experience maintaining MS SQL (Microsoft Structured Query Language) databases.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 to 3 years of experience. 4 points: >3 years of experience.	4		
	Total:	**Minimum Passing Score: 20 points**	**Maximum Score: 29 points**		

C.8 Network Security Analyst – Level 2
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 Network Security Analyst – Level 2 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall solutions such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience designing and configuring application traffic distribution using F5 products (DNS, LTM and BIGIP technologies).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Cisco networking technologies including dynamic routing protocols (e.g. BGP, OSPF), network separation (e.g. VRF, VLAN) and Network Address Translation (NAT).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R8	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Bidder should demonstrate that the proposed resource has experience within the past ten (10) years performing network security monitoring and log analysis to detect malicious activity.	1 point: >1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and optimizing production Security Information and Event Management System (SIEM) and/or Full Packet Capture solutions (excluding lab environments) for a large enterprise organization.	1 point: Experience achieved in an environment of 500 to 5000 users. 2 points: Experience achieved in an environment of >5000 to 10,000 users. 3 points: Experience achieved in an environment of >10,000 users.	3		
R3	The Bidder should demonstrate that the proposed resource has experience providing IT security incident detection, analysis and handling services using automated Security Information and Event Management System (SIEM) tool(s).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience operating and configuring all aspects of: 1) a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting; and/or 2) a Full Packet Capture solution including monitoring & capture, collection & metadata production, and analysis.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R6	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of experience reviewing, developing and implementing incident handling and escalation process flows in an IM/IT project.	1 point = 1 project. 2 points = 2 projects. 3 points = 3 or more projects. A minimum of 6 months of experience per project is required for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource holds one or more of the following certifications: 1) International Information System Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA); and/or 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx)	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 14 points**	**Maximum Score: 20 points**		

ATTACHMENT 4.1

BID EVALUATION CRITERIA

WORKSTREAM 2 – TOP SECRET

1. The evaluation criteria contained in this attachment will be used to evaluate bids during the solicitation and to facilitate resource assessment after contract award.

2. The Bidder must provide a qualifying résumé for each of the Resource Categories requested for evaluation (the Bidder must not propose the same resource more than once in response to this solicitation).

3. The Bidder must complete an evaluation grid for each of the résumés being provided as described in Table 1 below. For each criterion the Bidder must indicate the section in the résumé where compliance with the criteria is described. Failure to provide a qualifying résumé for each Resource Category results in a non-responsive bid.

Table 1: Bidders must submit the following number of résumés per resource category in response to this evaluation. The actual numbers of resources required are listed in Part 1, 1.2 Summary, of the bid solicitation;

Resource Category with Specific Task Title	Level	Number of Résumés
C.6 IT Security Engineer Specific Task Title: Configuration Management	3	1
C.6 IT Security Engineer Specific Task Title: Information Exchange Gateway (IEG)	2	1
C.6 IT Security Engineer Specific Task Title: Cyber Security Reference Architecture	3	1
C.6 IT Security Engineer Specific Task Title: Cross Domain Solution - Access	3	1
C.6 IT Security Engineer Specific Task Title: Cross Domain Solution - Transfer	2	1
C.6 IT Security Engineer Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning	2	1
C.6 IT Security Engineer Specific Task Title: Network Security Monitoring (NSM)	3	1
C.7 IT Security Design Specialist	2	1

Specific Task Title: Full Packet Capture		
C.7 IT Security Design Specialist Specific Task Title: Host Security	2	1
C.7 IT Security Design Specialist Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)	3	1
C.7 IT Security Design Specialist Specific Task Title: Information Exchange Gateway (IEG)	3	1
C.7 IT Security Design Specialist Specific Task Title: Cross Domain Solution - Access	3	1
C.7 IT Security Design Specialist Specific Task Title: Host Security	3	1
C.7 IT Security Design Specialist Specific Task Title: Network Security – Content Inspection	3	1
C.7 IT Security Design Specialist Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)	3	1
C.8 Network Security Analyst Specific Task Title: Network Security Monitoring (NSM)	3	1
C.8 Network Security Analyst Specific Task Title: Security Information and Event Management (SIEM)	3	1
C.12 Incident Management Specialist Specific Task Title: Security Information and Event Management (SIEM)	3	1

1. CORPORATE REQUIREMENTS

1.1. Corporate Mandatory Requirements

MANDATORY REQUIREMENTS – CORPORATE CRITERIA			
Item	**Mandatory Corporate Criteria**	**MET (Yes/No)**	**Page number(s) in bid**
M1	The Bidder must have been awarded at least 2 Government* informatics professional service† contracts. For each contract identified: 1. The value must be at least $5,000,000.00 ($5M) excluding applicable taxes; 2. The duration must be at least two (2) years within the last eight (8) years from the closing date of this solicitation and cannot include option periods that have not been exercised; 3. The Bidder must have provided at least five (5) resources simultaneously for a period of at least twelve (12) consecutive months; and Each contract used must also demonstrate that the Bidder has provided services to an organization with the following environment: • At least 100 workstations on a classified network or secret network; • Microsoft Windows workstation operating system (Windows XP, Windows Vista, Windows 7 and/or Windows 10); and • Centralized software distribution and patch management. The Bidder must provide one reference for each contract. The references must include the name of the organization, the unique contract identification number, a short description of the services provided, the name, title, email address and telephone number of the organization's responsible manager, the number of resources provided, as well as the award date, expiry date and dollar value of each contract. It is the Bidder's responsibility to ensure that any information divulged has the permission of the references provided. The Bidder must have been the prime contractor, rather than a subcontractor. This means that the Bidder contracted directly with the customer of the work. If the Bidder's contract was to perform work which another entity had itself first contracted to perform, the Bidder will not be considered the prime contractor. For example, Z (customer) contracted with Y for services. Y, in turn, entered into a contract with X to provide all or part of these services		

	to Z. In this example, Y is a prime contractor and X is a subcontractor. Bidders are reminded that a Supply Arrangement or Standing Offer is not a contract and therefore any reference to this type of document will not be accepted for the purpose of evaluating contract experience. For example if the Bidder references it's TBIPS SA number such as EN578-055605/XXX/EL for the purpose of demonstrating experience under the evaluation criteria, Canada will disregard this experience because it does not relate to a specific contract. * Government client may include a Federal, Provincial or Municipal Department/Agency or Crown Corporation. † Informatics Professional Services are professional services provided by the Bidder in support of an information technology or information management project or contract.		

RESOURCE CRITERIA

MANDATORY CRITERIA

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Configuration Management

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT security solutions.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years performing security architecture design or engineering support in the area of IT security.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience within the last ten (10) years, planning, developing, implementing and integrating vulnerability assessment solutions.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last eight (8) years, developing and implementing a vulnerability management program for an organization of at least 5,000 users.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience applying Government IT Security policies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cyber Security Reference Architecture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience in the design, planning, and/or implementation of information technology services, such as web services, database services, directory services, user access services, virtualized environments, and/or virtual desktops.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the review, design, planning, and/or implementation of security services, or security architectures for IT systems supporting more than 100 users.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience authoring technical configuration or implementation documentation.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience developing, configuring and testing of network security controls and policies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience designing and delivering virtual desktop services.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience designing, configuring and implementing role and rule-based access control models.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M6	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing, configuring and implementing IPSec tunneling schemes.			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: Cross Domain Solution – Transfer

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating High Assurance Guard technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience configuring and integrating Firewall technologies.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience engineering, designing, configuring and integrating e-mail content filter (such as malware prevention) and data loss prevention (such as label checking and word checking) technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating Firewall technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating web proxy technologies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience configuring and integrating mail transfer agent (MTA) technologies.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience engineering, designing, configuring and integrating Border Protection Service solutions.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.6 - Information Technology Security Engineer Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.6 Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Engineer.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of combined experience composing and maintaining Security Information and Event Management (SIEM) and/or Full Packet Capture (FPC) technical and engineering documentation.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in designing and implementing network security monitoring use cases in an enterprise deployment.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last ten (10) years designing, deploying and integrating SIEM tools and/or Full Packet Capture (FPC) tools in a production environment.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Full Packet Capture

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Full Packet Capture				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years, designing, deploying, administering and troubleshooting local and wide-area network communications infrastructure components.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years performing system administration with Linux or a Linux variant.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 2
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 2 Specific Task Title: Host Security				
M1	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years, working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of combined experience, within the last seven (7) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include two (2) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience applying IT Security end-point protection policies in an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years developing security architecture design for a Government classified solution (SECRET and above).			
M3	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience using at least one (1) of the following architectural methods/frameworks within the past seven (7) years: • TOGAF; • US government FEAP; • Canadian government BTEP; • Zachman; and/or • SABSA Security Architecture Framework			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last seven (7) years conducting detailed ICAM solution requirements analysis, design and implementation.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M5	The Bidder must demonstrate that the proposed resource has a minimum of one (1) year of experience briefing senior managers (Director level and above) on IT security implications and recommended courses of action.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Information Exchange Gateway (IEG)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Information Exchange Gateway (IEG)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following security networking technologies: • Guards and Gateways; • Firewalls; • Border Protection Services; • Data Diodes; • Web proxies; and • Mail Transfer Agent. A minimum of two years of experience is required for each of the above technologies.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of combined experience designing, engineering, installing, configuring, testing, troubleshooting, and maintaining the following IT products and infrastructure: • Microsoft Network Operating System; • IP Networks; • Applications Integration; and • Virtualization. A minimum of three years of experience is required for each of the above technologies.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M3	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last six (6) years working with common classified networks at the Secret and/or Top Secret level.			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Cross Domain Solution – Access

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Cross Domain Solution - Access				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience planning and implementing IT Security integration architectures.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of experience in the design, implementation and change management of network security controls and policies.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of virtual desktop services.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of role- and rule-based access control models.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design, implementation and change management of IPSec tunneling schemes.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M6	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Host Security

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Host Security				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience designing and implementing IT security solutions.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience, within the last eight (8) years, designing, engineering, installing, configuring, and testing endpoint protection security software in an enterprise IT environment. Endpoint protection security software experience must include three (3) of the following: Anti-Virus, Data Loss Prevention (DLP), Data Labeling, Enterprise Data Rights Management (EDRM), Endpoint Detection and Response (EDR), Host Firewall, Malware Analysis/Reverse Engineering, Application Control, Host Intrusion Prevention, Data labeling and protection, User and Entity Behaviour Analytics (UEBA), Full Disk Encryption (FDE) and Removable Media Encryption (RME)			
M3	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years applying IT Security end-point protection policies to an enterprise IT environment.			

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
M4	The Bidder must demonstrate that the resource has a minimum of five (5) years of combined experience in the development of at least three (3) of the following types of System Engineering Documentation: • System Design Specifications; • Build / Configuration documents; • Concept of Operations (ConOps); • System Implementation Plans; • Test Plans/Test Reports; and • Life Cycle Support Plans			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Network Security – Content Inspection

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Network Security – Content Inspection				
M1	The Bidder must demonstrate that the proposed resource has a minimum ten (10) years of experience within the last fifteen (15) years working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience within the last ten (10) years configuring and integrating networking equipment.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience within the last ten (10) years designing secure architectures while following Communications Security Establishment (CSE)'s Information Technology Security Guidance (ITSG) 22, 33 and 38 guidelines.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of three (3) years of experience in the last eight (8) years configuring, integrating and troubleshooting Firewalls.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of five (5) years of experience integrating IT security solution Proof of Concepts (POCs).			
	Compliant (Yes/No)?			

C.7 Information Technology Security Design Specialist – Level 3
Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.7 Information Technology Security Design Specialist – Level 3 Specific Task Title: Enterprise Governance, Risk and Compliance (eGRC)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience, within the last fifteen (15) years, working as an IT Security Design Specialist.			
M2	The Bidder must demonstrate that the proposed resource has at least two (2) years of experience, within the last five (5) years developing and implementing an Enterprise Governance, Risk, and Compliance (eGRC) solution for an organization of at least 5,000 users.			
M3	The Bidder must demonstrate that the proposed resource has at least two (2) years of experience within the last five (5) years in the assessment of applied Security Controls, the evaluation of Threats and Risks to an IT system, or the interpretation and application of Information Technology Security Guidance (ITSG) 33 Annex A.			
M4	The Bidder must demonstrate that the proposed resource has at least two (2) years of experience within the last ten (10) years defining requirements, translating business process into workflow, and engineering solutions in the definition and implementation stages of an IT Security project.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Network Security Monitoring (NSM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Network Security Monitoring (NSM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analysing security log files from an enterprise network of at least 500 users.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience with the collection and analysis of malicious code from hosts and network traffic.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of four (4) years of combined experience within the last eight (8) years monitoring, configuring and tuning Security Information and Event Management (SIEM) tools and/or Full Packet Capture tools in a production environment.			
	Compliant (Yes/No)?			

C.8 Network Security Analyst – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.8 Network Security Analyst – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as a Network Security Analyst			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last five (5) years configuring and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience monitoring and analyzing security log files from an enterprise network of at least 500 users.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
	Compliant (Yes/No)?			

C.12 Incident Management Specialist – Level 3
Specific Task Title: Security Information and Event Management (SIEM)

	REQUIREMENT	MET	NOT MET	COMMENTS (I.E. LOCATION IN PROPOSAL, CRITERIA NOT MET, ETC)
C.12 Incident Management Specialist – Level 3 Specific Task Title: Security Information and Event Management (SIEM)				
M1	The Bidder must demonstrate that the proposed resource has a minimum of ten (10) years of experience within the last fifteen (15) years working as an Incident Management Specialist.			
M2	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience within the last six (6) years implementing and providing technical support for the Security Information and Event Management (SIEM) tool ArcSight in a production environment.			
M3	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience in the design and implementation of SIEM use cases for both servers and workstations in an enterprise deployment.			
M4	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience building, configuring, and troubleshooting Linux servers.			
M5	The Bidder must demonstrate that the proposed resource has a minimum of two (2) years of experience composing and maintaining SIEM documents or SIEM engineering deliverables.			
	Compliant (Yes/No)?			

RATED CRITERIA

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Configuration Management

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Configuration Management					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience performing options analysis of IT security tools and techniques.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R3	The Bidder should demonstrate that the proposed resource has experience planning, developing, implementing and integrating IT asset discovery or configuration management database (CMDB) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R4	The Bidder should demonstrate that the proposed resource has experience in planning, developing, implementing and integrating automated configuration compliance auditing solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience writing technical reports such as requirements analysis, options analysis, and technical architecture documents.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
R6	The Bidder should demonstrate that the proposed resource has experience developing hardening guides for IT systems.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The proposed resource should hold one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 – Information Technology Security Engineer - Level 2
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 – Information Technology Security Engineer - Level 2 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cyber Security Reference Architecture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cyber Security Reference Architecture					
R1	The Bidder should demonstrate that the proposed resource has at least 6 months experience designing, or co-designing one major scale IT (Information Technology) environment for a minimum of 100 users.	IT supporting users: 3 points: 100 to 300 users. 4 points: >300 to 1000 users. 5 points: >1000 or more users.	5		
R2	The Bidder should demonstrate that the proposed resource has experience working in the application of IT Security Risk Management processes or System Security Engineering processes.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience designing or implementing and configuring IT Intrusion Detection and Protection methodologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience working with the design or implementing and configuring System Monitoring for accesses, changes or operational status.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience designing or implementing and configuring IT Enterprise Services, including directory, single sign-on, email, backup, or distributed database for an IT system supporting at least 500 users.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience designing or implementing and configuring IT Defence in Depth principles. The Bidder should also demonstrate and provide a description of how the resource applied the principles.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience working with a recognized enterprise architecture framework.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R8	The Bidder should demonstrate that the proposed resource has experience writing technical documents using desktop office-class tools, for audience at the corporate level.	1 point: 1 to 2 years of experience. 2 points: >2 to 4 years of experience. 3 points: >4 to 6 years of experience 4 points: >6 years of experience.	4		
	Total:	**Minimum Passing Score: 19 points**	**Maximum Score: 27 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: Cross Domain Solution – Transfer

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: Cross Domain Solution – Transfer					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.6 - Information Technology Security Engineer - Level 2
Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 2 Specific Task Title: TS Information Exchange Gateway (IEG) and TS Zoning					
R1	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Firewall solutions, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing proxy solutions, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing VMware solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Windows Server 2008 (or more recent version), Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and implementing Red Hat Enterprise Linux (RHEL).	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R8	The Bidder should demonstrate that the proposed resource has experience engineering, configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 17 points**	**Maximum Score: 24 points**		

C.6 - Information Technology Security Engineer - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.6 - Information Technology Security Engineer - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last ten (10) years engineering network security monitoring solutions using at least three (3) of the following security technologies: 1) Host-based security; 2) IDS/IPS (Intrusion Prevention System); 3) Firewalls/UTMs; 4) Full Packet Capture; 5) Proxies; 6) Load Balancers; and 7) Matrix Switches/Taps.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Bidder should demonstrate that the proposed resource has experience within the last ten (10) years designing network security monitoring solutions for the Government based on IT Security Directive (ITSD) 02 or IT Security Guidance (ITSG) 22 at the Protected B level or higher.	1 point per project up to a maximum 3 projects*† *If a Bidder provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		
R4	The Bidder should demonstrate that the proposed resource has experience providing IT security engineering services to Government departments and agencies in the form of security architecture development, advice and guidance.	1 point: 3 to 5 years of experience. 2 points: >5 to 7 years of experience. 3 points: >7 to 9 years of experience. 4 points: >9 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate the proposed resource holds one or more of the following IT security certifications: 1) International Information Systems Security Certification Consortium $(ISC)^2$ CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified Intrusion Analyst (GCIA) A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 16 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Full Packet Capture

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Full Packet Capture					
R1	The Bidder should demonstrate the proposed resource has experience within the last seven (7) years designing, planning and implementing network infrastructure of complex and highly available* environments. *Complex and highly available environments are defined as environments spanning multiple cities or countries with zero-downtime.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R2	The Bidder should demonstrate that the proposed resource has combined experience within the last ten (10) years performing one or more of the following IT-related tasks: 1. Writing technical reports such as requirement analysis, options analysis, engineering process artefacts and/or technical architecture documents; 2. Automating the administration of Linux systems through scripting and APIs such as (but not limited to) Ruby, PHP, Bash, Perl or Python; 3. Analysis of raw network traffic capture to support troubleshooting or network forensics; 4. Deployment and administration of network forensics or traffic monitoring devices such as (but not limited to) FireEye, Solera, Sourcefire/Cisco IDS/IPS, SNORT or Netwitness (RSA Security Analytics); 5. Review alerts and packet-level data from IDS sensors/ packet capture devices;	1 point: 6 to 9 months of experience. 2 points: >9 to 12 months of experience. 3 points: >12 to 15 months of experience. 4 points: >15 months of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R2	6. Malware analysis and sandboxing with applications like (but not limited to) Netwitness Spectrum/RSA Malware, WireShark, CaptureBAT or Cuckoo Sandbox and the ability to reverse engineer and debug malware samples using tools such as (but not limited to) IDA Pro, Responder Pro or OllyDbg, including defeating anti debugging, packing and obfuscation techniques; and/or 7. Management of SAN and NAS technologies – Fibre Channel, FCOE, iSCSI, NFS, CIFS, including but not limited to the provisioning of LUNs, cabling, troubleshooting and patching. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.				

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Bidder should demonstrate that the proposed resource has one or more of the following IT security certifications: 1) RSA Security Analytics Certified Administrator; 2) Any Cisco Associate level certification; 3) Any Cisco Professional level certification; 4) Any Cisco Expert level certification; 5) Any SANS GIAC certification in the Security Administration category; 6) Any Redhat Certified System Administrator, Engineer and/or architect certification; A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 8 points**	**Maximum Score: 12 points**		

C.7 - Information Technology Security Design Specialist - Level 2
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 2 Specific Task Title: Host Security					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience implementing McAfee, Symantec or Trend-Micro host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, in an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Bidder should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Bidder should demonstrate that the proposed resource has experience evaluating various IT security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Bidder provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of three (3) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Bidder should demonstrate that the proposed resource holds at least one of the following IT security certifications: 1) ISC2 Certified Information System Security Professional (CISSP); 2) ISC2 Certified Cloud Security Professional (CCSP); 3) ISC2 Systems Security Certified Professional (SSCP); and/or 4) Global Information Assurance Certification (GIAC) certification (any). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	3 points = 1 certification. 4 points = 2 certifications. 5 points = 3 or more certifications.	5		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 26 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Identity, Credential and Access Management (ICAM) and Public Key Infrastructure (PKI)					
R1	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years developing Standard Operating Procedures (SOP) on projects.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying PKI technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years designing and deploying Identity, Credential and Access Management (ICAM) solutions.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months experience designing IT solutions requiring interoperability with: • one or more GoC departments; and/or • one or more of the following International partners: US, UK, AUS, NZ.	1 point: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with GoC department(s). 2 points: demonstrated at least six (6) months of experience designing IT solutions requiring interoperability with International partner(s) (US, UK, AUS, NZ)	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years designing process mapping for a security architecture design.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Information Exchange Gateway (IEG)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Information Exchange Gateway (IEG)					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Firewall technologies, such as McAfee, Palo Alto, or F5.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing proxy technologies, such as McAfee Web Gateway, F5, or Blue Coat.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Trustwave MailMarshall Secure Email Gateway mail transfer agent (MTA) solutions.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing SSL, HTTPS, HTTP, IPSec and SMTP technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing VMware technology.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions), Active Directory and Domain Name System in large (at least 1,000 users) IT networks.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco networking technologies including Routers and Switches.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Cross Domain Solution – Access

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Cross Domain Solution – Access					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has combined experience performing at least three (3) the following IT Security tasks: 1) Analysis of IT Security tools and techniques; 2) Analysis of security data and provision of advisories and reports; 3) Writing technical reports including requirements analysis, options analysis, technical architecture documents and mathematical risk modeling; 4) Security architecture design and engineering support; and 5) Data security classification studies. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R3	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and implementing Windows Server 2008 (or more recent versions) Active Directory and Domain Name System.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience in design, implementation and change management of VMWare Technologies.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R5	The Bidder should demonstrate that the proposed resource holds one or more of the following architecture certifications: 1) Certification in The Open Group Architecture Framework (TOGAF); 2) Certification in Information Technology Service Management (ITSM); 3) Certification in Enterprise Architecture Center of Excellence (EACOE); 4) Certification in Microsoft Certified Architect (MCA); and/or 5) Certification in VMWare Certified Design Expert (VCDX). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 11 points**	**Maximum Score: 15 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Host Security

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Host Security					
R1	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security end-point protection policies in an enterprise IT environment.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has experience implementing centrally managed host-based endpoint security policies in an enterprise IT environment.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience implementing McAfee host-based endpoint security policies in an enterprise IT environment.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has a minimum one (1) year each of experience engineering and implementing the following host-based security technologies, on an enterprise IT environment: 1) Symantec Endpoint Protection; 2) McAfee ePolicy Orchestrator; or 3) Trend-Micro Control Manager.	1 point: for achieving the minimum experience demonstrated for 1 of the listed host-based security technologies. 2 points: for achieving the minimum experience demonstrated for each of 2 of the listed host-based security technologies. 3 points: for achieving the minimum experience demonstrated for each of the 3 listed host-based security technologies.	3		
R5	The Bidder should demonstrate that the proposed resource has experience engineering, integrating or supporting McAfee, Symantec, or Trend-Micro Management for Optimized Virtual Environments in a production environment.	1 point: 1 to 2 years of experience. 2 points: >2 years of experience.	2		
R6	The Bidder should demonstrate that the proposed resource has experience evaluating various security technologies and documenting an analysis for management decision.	1 point per project up to a maximum 3 projects*† *If a Bidder provides more than 3 projects in response to this criterion, only the first 3 projects in order of appearance in the Bid will be evaluated. †A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource has experience engineering and implementing network security solutions using at least three (3) of the following network security technologies: 1) IDS/IPS; 2) Firewalls/UTMs; 3) Full Packet Capture; 4) Proxies; 5) Load Balancers; 6) Matrix Switches/Taps; 7) Database Activity Monitoring; 8) Network Access Control (802.1x); and 9) Other Content Inspection systems. A minimum of six (6) months experience is required in any given area claimed for the experience to be considered.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 to 4 years of experience. 4 points: >4 years of experience.	4		
	Total:	**Minimum Passing Score: 15 points**	**Maximum Score: 21 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Network Security – Content Inspection

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Network Security – Content Inspection					
R1	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning Cisco technologies including Routers, and/or Nexus and Catalyst Series Switches.	1 point: 5 to 6 years of experience. 2 points: >6 to 7 years of experience. 3 points: >7 to 8 years of experience. 4 points: >8 years of experience.	4		
R2	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and troubleshooting Palo Alto firewalls.	1 point: 3 to 4 years of experience. 2 points: >4 to 5 years of experience. 3 points: >5 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience working with application aware traffic generators.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R4	The Bidder should demonstrate that the proposed resource has experience working with Intrusion Detection Systems (IDS).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience working with VMWare.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R6	The Bidder should demonstrate that the proposed resource has experience configuring, integrating and provisioning F5 load balancers.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience working with inline network encryption technologies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 18 points**	**Maximum Score: 25 points**		

C.7 - Information Technology Security Design Specialist - Level 3
Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.7 - Information Technology Security Design Specialist - Level 3 Specific Task Title: Enterprise Governance, Risk, and Compliance (eGRC)					
R1	The Bidder should demonstrate that the proposed resource holds one or more of the following administrating IT GRC or eGRC application certifications: 1) RSA Archer Certified Administrator 2) IBM OpenPages Administrator 3) MetricStream GRC Certified Administrator A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R2	The Bidder should demonstrate that the proposed resource has combined experience within the last five (5) years authoring XML data transformation and/or translation scripts.	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		
R3	The Bidder should demonstrate that the proposed resource has experience with IT Security Design projects within an eGRC implementation environment.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years writing technical reports such as options analysis, and/or implementation plans.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience applying Government IT Security policies.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has combined experience within the last five (5) years accrediting an IT system using the Security Assessment and Authorization (SA&A) process and/or the Certification and Accreditation (C&A) program.	1 point: 1 to 2 years of experience. 2 points: >2 to 3 years of experience. 3 points: >3 years of experience.	3		
R7	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years developing network security architectures (Level II or higher) based on IT Security Directives (ITSD) and /or IT Security Guidance (ITSG).	1 point: 6 months to 1 year of experience. 2 points: >1 to 2 years of experience. 3 points: >2 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R8	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) Certified Information System Security Professional (CISSP); 2) Systems Security Certified Practitioner (SSCP); 3) GIAC Security Essentials (GSEC); 4) Microsoft Certified Solutions Expert (MCSE); and/or 5) Cisco Certified Network Associate (CCNA). A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications	3		
	Total:	**Minimum Passing Score: 16 points**	**Maximum Score: 23 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Network Security Monitoring (NSM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Network Security Monitoring (NSM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last ten (10) years performing network security monitoring and log analysis to detect malicious activity.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and optimizing production Security Information and Event Management System (SIEM) and/or Full Packet Capture solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		
R3	The Bidder should demonstrate that the proposed resource has experience providing IT security incident detection, analysis and handling services using automated Security Information and Event Management System (SIEM) tool(s).	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience operating and configuring all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: >2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or RSA Netwitness specific training and/or holds a current certification for ArcSight Technology or RSA Netwitness technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
R6	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of experience reviewing, developing and implementing incident handling and escalation process flows in an IM/IT project.	1 point = 1 project. 2 points = 2 projects. 3 points = 3 or more projects. A minimum of 6 months of experience per project is required in order for the project to be considered.	3		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R7	The Bidder should demonstrate that the proposed resource holds one or more of the following IT security certifications: 1) International Information System Security Certification Consortium (ISC)2 CISSP; 2) Global Information Assurance Certification (GIAC) – GIAC Certified Incident Handler (GCIH); 3) Global Information Assurance Certification (GIAC) – GIAC Certified 4) Global Information Assurance Certification (GIAC) – GIAC Security Expert (GSE); A copy of the resource's valid Certification(s) (or certification ID with web link to verify) must be submitted with the Bid. The Certification must be obtained from an accredited institution, recognized by the Canadian Information Centre for International Credentials (http://www.cicic.ca/en/index.aspx).	1 point = 1 certification. 2 points = 2 certifications. 3 points = 3 or more certifications.	3		
	Total:	**Minimum Passing Score: 14 points**	**Maximum Score: 20 points**		

C.8 – Network Security Analyst - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.8 – Network Security Analyst - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 2 to 3 years of experience. 2 points: >3 to 4 years of experience. 3 points: >4 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		
R3	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		
R7	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		

C.12 – Incident Management Specialist - Level 3
Specific Task Title: Security Information and Event Management (SIEM)

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
C.12 – Incident Management Specialist - Level 3 Specific Task Title: Security Information and Event Management (SIEM)					
R1	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years performing network security monitoring and log analysis to detect malicious activity.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R2	The Bidder should demonstrate that the proposed resource has a minimum of six (6) months of continuous experience in one project configuring, tuning and maintaining production SIEM solutions (excluding lab environments) for a large enterprise organization.	1 point = experience achieved supporting 500 to 5000 users. 2 points = experience achieved supporting >5000 to 10,000 users. 3 points = experience achieved supporting over 10,000 users.	3		
R3	The Bidder should demonstrate that the proposed resource has experience within the last seven (7) years providing technical support to at least three (3) of the following network security technologies: 1) Host-based security 2) IDS/IPS (Intrusion Prevention System) 3) Firewalls/UTMs 4) Proxies 5) Load Balancers 6) Matrix Switches/Taps	1 point: 2 to 5 months of experience. 2 points: >5 months of experience.	2		

#	CRITERIA	SCORING GUIDELINES	MAX POINTS	SCORE	CROSS REFERENCE TO PROPOSAL (PAGE AND PARA)
R4	The Bidder should demonstrate that the proposed resource has experience deploying and operating all aspects of a SIEM solution including: data normalization, log forwarding, log aggregation, log and event storage, log and event correlation, and reporting and alerting.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R5	The Bidder should demonstrate that the proposed resource has experience tuning and configuring SIEM components to improve efficiency, accuracy, and performance.	1 point: 1 to 3 years of experience. 2 points: >3 to 5 years of experience. 3 points: >5 years of experience.	3		
R6	The Bidder should demonstrate that the proposed resource has experience in the last seven (7) years working in an in-service support/helpdesk environment.	1 point: 1 to 6 months of experience. 2 points: >6 months of experience.	2		
R7	The Bidder should demonstrate that the proposed resource completed ArcSight specific training and/or holds a current certification for ArcSight Technology. A copy of the resource's valid Certification (or certification ID with web link to verify) must be submitted with the Bid.	1 point = 1 certification. 2 points = 2 or more certifications.	2		
	Total:	**Minimum Passing Score: 13 points**	**Maximum Score: 18 points**		