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
Québec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Net C2 ISAC RFI/ITQ

Solicitation No. - N° de l'invitation	Date
W8474-18NT10/A	2018-07-26
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
W8474-18NT10	PW-$$QE-459-26920
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
459qe.W8474-18NT10	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2018-08-29

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Williamson, Ian	459qe
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 956-0185 ( )	( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Specified Herein
Précisé dans les présentes

Comments - Commentaires

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
Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Canada

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
Québec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet Net C2 ISAC RFI/ITQ	
Solicitation No. - N° de l'invitation W8474-18NT10/A	**Date** 2018-07-25
Client Reference No. - N° de référence du client W8474-18NT10	**GETS Ref. No. - N° de réf. de SEAG**
File No. - N° de dossier 459qe.W8474-18NT10	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2018-08-29**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Williamson, Ian R	**Buyer Id - Id de l'acheteur** 459qe
Telephone No. - N° de téléphone (819) 956-0185 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** DEPARTMENT OF NATIONAL DEFENCE 101 Colonel By Drive OTTAWA Ontario K1A 0K2 Canada	

Comments - Commentaires

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 See Herein	**Delivery Offered - Livraison proposée**
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
Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Canada

W8474-18NT10/A

INVITATION TO QUALIFY (ITQ)

FOR

NETWORK COMMAND AND CONTROL INTEGRATED SITUATIONAL AWARENESS CAPABILITY (NET C2 ISAC)

FOR

THE DEPARTMENT OF NATIONAL DEFENCE (DND)

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

1.1.1 This Request for Information / Invitation to Qualify (hereinafter referred to as ITQ) is neither a Request for Proposal (RFP) nor a solicitation of bids or tenders. No Contract will result from this ITQ. Canada reserves the right to cancel this procurement at any time during the ITQ phase or any other phase of the procurement process. Given that this ITQ may be cancelled by Canada, it may not result in any of the subsequent procurement processes described in this document. Suppliers may withdraw from the process at any time, as the ITQ is not a tender. Neither the Government of Canada nor its advisors shall be liable for any expense, cost, loss or damage incurred or suffered by any Respondent, any Respondent advisor or any Person connected with any one of them, as a result of any action taken by the Crown in respect of the ITQ Process or the RFP Process.

1.1.2 This ITQ is the first phase in the procurement process for the Network Command and Control Integrated Situational Awareness Capability (Net C2 ISAC) Project. The objective of this ITQ is to qualify responsive Suppliers to proceed to the subsequent phases of this procurement process. The responsive Suppliers will be hereinafter referred to as "ITQ Responsive Suppliers".

1.1.3 Only ITQ Responsive Suppliers will be permitted to receive the draft RFP and the final RFP.

1.1.4 ITQ Responsive Suppliers may choose not to bid on the final RFP.

1.1.5 This ITQ may be cancelled if less than two (2) responses are received or if less than two (2) Suppliers are qualified.

1.1.6 The ITQ is divided into the following parts:

Part 1: General Information: provides an overview of the Net C2 ISAC Solution requirements;

Part 2: Respondent Instructions: provides the instructions, clauses and conditions applicable to the ITQ;

Part 3: Response Preparation Instructions: provides Suppliers with instructions on how to prepare their response to the ITQ;

Part 4: Overview of the Procurement Process;

Part 5: Evaluation Procedures and Basis of Qualification: describes how the responses will

be evaluated and the basis of Qualification;

Part 6: Certifications: includes the certifications to be provided as part of the ITQ response;

Part 7: Security Requirement: describes specific security requirements;

Part 8: Anticipated RFP; and

Part 9: Subset of Anticipated Resulting Contract Clauses.

Refer to the Table of Contents for the list of annexes, attachments and forms.

1.2 Summary

1.2.1 The Department of National Defence (DND) has a requirement to implement a Net C2 ISAC solution to provide Operational and Strategic Commanders and their Staff (OSC&S) the knowledge of key elements in the Information Technology Infrastructure (ITI) necessary to make well-informed decisions regarding the command and control of their operations.

1.2.2 The Canadian Armed Forces (CAF) is becoming increasingly reliant upon communications and computer networks to perform every aspect of operational and planning activities (domestic, international, expeditionary and corporate services/administrative functions). More and more operations are being supported by strategic capabilities in Canada delivered through Information Technology (IT) Services. Thus, understanding the state of those IT Services has become increasingly important.

The overall requirement is to put in place a capability consisting of personnel, processes and tools to:

a. Generate and display Network Situational Awareness (Net SA);

b. Align processes and procedures to support the creation and dissemination of Net SA;

c. Support CAF/DND command and control as they relate to the ITI; and

d. Sustain the on-going efforts in the production of Net SA.

1.2.3 Canada has identified the following as components required for the production of the Net C2 ISAC solution:

a. Refined existing and/or new defined processes, that make use of appropriate ITI data sources, to establish reliable, relevant and meaningful situational awareness concerning the ITI that affects DND/CAF IT capabilities;

b. New software and computer tools brought into service to support the processes;

c. System integration services, programming, script writing, database support, interface development,

d. Training for strategic and operational commanders (and staffs);

e. Training for IT Technical personnel; and

f. One year of stabilization support to maintain and optimize the processes, the software and hardware tools, and the training of CAF/DND personnel.

1.2.3 Further details can be found in Annex A: High Level Requirements

1.2.4 The purpose of this ITQ is to invite all Suppliers capable of meeting the requirements of this ITQ to submit responses to Public Works and Government Services Canada (PWGSC) for evaluation in an attempt to become an ITQ Responsive Supplier. Only ITQ Responsive Suppliers will be invited to participate in the draft RFP process and bid on the final RFP. An overview of the procurement process can be found in Part 4: Overview of Procurement Process.

1.3 Procurement Overview

1.3.1 The Net C2 ISAC Project procurement will be fulfilled through a multi-phased collaborative procurement process. It is intended that a single contract resulting from any subsequent bid solicitation will be awarded by PWGSC to a single supplier to act as the Net C2 ISAC Prime Integrator.

1.3.2 ITQ: This ITQ is open to all Suppliers and will result in ITQ Qualified Suppliers being invited to participate in the draft RFP process. Respondents will be notified of the evaluation results once the ITQ evaluation process is completed.

1.3.3 Draft RFP: A draft RFP will be issued to ITQ Qualified Suppliers to further refine the requirement by addressing industry concerns and considering industry best practices. It is anticipated that ITQ Qualified Suppliers will be engaged to review preliminary RFP documents, provide feedback electronically, as well as attend industry day meetings and one-on-one meetings, to discuss specific issues relating to the content of the preliminary RFP documents. The RFP will be finalized following the draft RFP process.

1.3.4 Anticipated Final RFP: The RFP will be issued directly to ITQ Qualified Suppliers. Reference Part 8 for further details of the anticipated RFP.

1.4 Debriefings (ITQ)

1.4.1 Respondents may request a debriefing on the results of the ITQ. Respondents should make the request to the Contracting Authority within fifteen (15) calendar days of receipt of the results of the ITQ.

1.5 Conflict of Interest

1.5.1 Respondents are advised to refer to Conflict of Interest provisions at Article 18 of the Standard Acquisition Clauses and Conditions (SACC) 2003, Standard Instructions – Goods or Services – Competitive Requirements (dated 2018-05-22) and Conflict of Interest provisions of SACC 2030, General Condition – Higher Complexity – Goods (dated 2018-06-21) available on the PWGSC Website https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual

1.5.2 Without limiting in any way the provisions described in 1.5.1 above, Respondents are advised that Canada has engaged the assistance of the following private sector contractors and resources who have provided services including the preparation of this ITQ and/or who have had, or may have had, access to information related to this ITQ or other documents related to the Net C2 ISAC solicitation:

Contractors:

- Modis Canada
- P1 Consulting

Resources:

- Ken Polson
- Grant Brazier
- Neil MacAskill
- David Yeo
- Alan Walsh
- Sean Hoopey
- Abdallah Abi-Aad
- Brian Cheng;
- Oliver Grant, Fairness Monitor
- Louise Panneton, Fairness Monitor

1.6 Fairness Monitor

1.6.1 Canada has engaged the services of an organization to act as an independent third party Fairness Monitor (FM) for the Net C2 ISAC procurement process. The role of the FM is to provide an attestation of assurance on the fairness, openness and transparency of the monitored activities.

1.6.2 The FM will not be part of the evaluation team, but will be granted access to any response submitted in response to this ITQ and any related correspondence received by Canada pursuant to this ITQ. The FM will observe the evaluation of the ITQ responses with respect to Canada's adherence to the evaluation process described in this ITQ and will observe the response debriefings. The FM is under obligations pursuant to its contract with Canada to maintain the confidentiality of all information received as a result of its participation in this procurement process

1.7 Trade Agreements

1.7.1 This procurement is subject to national security exception and is, therefore, excluded from all of the obligations of trade agreements.

PART 2 – RESPONDENT INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

2.1.1 All instructions, clauses and conditions identified in the ITQ 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 PWGSC.

2.1.2 Respondents who submit a response agree to be bound by the instructions, clauses and conditions of the ITQ.

2.1.3 The 2003 (2018-05-22) Standard Instructions - Goods or Services – Competitive Requirements, are incorporated by reference into and form part of the ITQ, except that:

a. Wherever the term "bid solicitation" is used, it is substituted with "Invitation to Qualify";
b. Wherever the term "bid" is used, it is substituted with "response";
c. Wherever the term "Bidder(s)" is used, it is substituted with "Respondent(s)";
d. Wherever the terms "Contract (contract)" is used, it is substituted with "Qualification" or "ITQ Responsive Supplier" as applicable;
e. Subsection 5(4), which discusses a validity period, does not apply, given that this ITQ invites Respondents simply to qualify;
f. The title of Section 10 is amended to read "Legal Capacity and Ownership and Control Information", the first paragraph is numbered as 1 and the following is added:

2. The Respondent must provide, if requested by the Contracting Authority, the following information as well as any other requested information related to the ownership and control of the Respondent, its owners, its management and any related corporations and partnerships:

i. An organization chart for the Respondent showing all related corporations and partnerships;

ii. A list of all the Respondent's shareholders and/or partners, as applicable; if the Respondent is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner; and

iii. A list of all the Respondent's directors and officers, together with each individual's home address, date of birth, birthplace and citizenship(s); if the Respondent is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner.

In the case of a joint venture Respondent, this information must be

provided for each member of the joint venture. The Contracting Authority may also require that this information be provided in respect of any Subcontractors specified in a response.

3. For the purposes of this section, a corporation or partnership will be considered related to another party if:

i. they are "related persons" or "affiliated persons" according to the Canada Income Tax Act;

ii. the entities have now or in the two (2) years before the closing date had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

iii. 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.

g. Subsection 14 Price Justification does not apply as there is no financial component to the ITQ.

2.2 Composition of Core Team

2.2.1 Respondents submitting responses to the ITQ must indicate the relevant company and/ or organization names (including Core Team Members) that are jointly submitting the response in Form 1: ITQ Submission Form.

2.2.2 If a response is submitted by a joint venture, it must be in accordance with section 17 Joint Venture, of the SACC 2003 Standard Instructions (2018-05-22)

2.2.3 Only the capabilities and experience of the Core Team will be considered when evaluating the response submitted to this ITQ.

2.2.4 The Core Team may be comprised of a Respondent and any additional firms deemed necessary by the Respondent (Core Team Members). The structure can either be Prime (Respondent) and Subcontractors or a joint venture of two (2) or more of the members identified as the Core Team, if applicable.

2.2.5 Once a Respondent has identified itself as the Respondent, it must remain the Respondent and cannot switch roles with any member of its Core Team for the duration of Net C2 ISAC procurement process. For Respondents who qualify to proceed to the next phases of the procurement process, the Respondent must be the Bidder for the RFP.

2.2.6 A Respondent's Core Team for subsequent phases of the Net C2 ISAC Project procurement process must continue to consist of the Core Team identified in the response to this ITQ (Form 1). Beyond this period, changes to the Core Team may only be made following receipt of written approval from the Contracting Authority. Failure to maintain the Core Team throughout the procurement process (unless approved in writing by the Contracting Authority) may, at the discretion of Canada, result in the Respondent becoming ineligible for continued participation in the Net C2 ISAC procurement process.

2.2.7 Respondents must, in their ITQ Response, identify what role each member of their Core Team will play in delivery of the Net C2 ISAC Project services. Further, the Respondent must demonstrate that where a Core Team member's experience has been proposed to meet Qualifications listed in the Mandatory Requirements section of the ITQ, that Core Team member will carry out the same work under any resulting Contract. For example, where a Respondent has identified itself as the Core Team member with the experience required for Mandatory Requirement 1 (M1), the Respondent will deliver that service under any resulting Contract.

2.3 Submission of Responses

2.3.1 Responses must be submitted only to the PWGSC Bid Receiving Unit by the date, time and place indicated on page 1 of the ITQ.

2.3.2 Due to the nature of the ITQ, transmission of responses by facsimile or e-mail to PWGSC will not be accepted.

2.4 Enquiries

2.4.1 All enquiries must be submitted in writing to the Contracting Authority, at the email address identified below, no later than ten (10) calendar days before the ITQ closing date. Enquiries received after that time may not be answered.

Ian R. Williamson

Contracting Authority – Net C2 ISAC Project
Public Services and Procurement Canada
Email address: Ian.Williamson@pwgsc.gc.ca

2.4.2 Respondents should reference as accurately as possible the numbered item of the ITQ to which the enquiry relates. Care should be taken by Respondents to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. 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 Respondents do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all Respondents. Enquiries not submitted in a form that can be distributed to all

Respondents may not be answered by Canada.

2.5 Applicable Laws

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

2.6 Improvement of Requirement during ITQ

2.6.1 Should Respondents consider that the requirements contained in the ITQ could be improved technically or technologically, Respondents are invited to make suggestions, in writing, to the Contracting Authority named in the ITQ. Respondents must clearly outline the suggested improvement as well as the reason for the suggestion. Only suggestions that do not restrict the level of competition nor favour a particular Respondent may be given consideration provided they are submitted to the Contracting Authority at least ten (10) calendar days before the ITQ closing date. Canada will have the right to accept or reject any or all suggestions.

2.7 Language

2.7.1 Respondents are requested to identify, in writing, in Form 1 - ITQ Submission Form which of Canada's two (2) official languages (English or French) will be used for future communications from Canada and, if successful in the ITQ evaluation, for the next steps of the procurement process.

2.8 Basis for Canada's Ownership of Intellectual Property

2.8.1 Canada has determined that any intellectual property arising from the performance of the Work under the Contract will belong to Canada, on the grounds of National Security.

Canada will own the foreground intellectual property rights to the Net C2 ISAC, the public key infrastructure solution, software/hardware solutions for all customized modules, custom Canadian consumables design and artwork, plates, dies and other custom tooling bearing Canadian designs used in the performance of work under the Contract. All other intellectual property rights, including background and other foreground, will be owned or licensed by the Contractor with appropriate licenses granted to Canada.

PART 3 - RESPONSE PREPARATION INSTRUCTIONS

3.1 Response Preparation Instructions

Canada requests that Respondents provide their response as follows:

Volume I: Technical Response
Hard copies - 6 copies
Soft copies – 3 soft copies on 3 separate USB memory sticks;

Volume II: Application of the Industrial and Technological Benefits (ITB) Policy
Hard copies – 3 copies
Soft copies – 2 copies on 2 separate USB memory sticks; and

Volume III: Certifications - two (2) hard copies.

If there is a discrepancy between the wording of the soft copy and the original hard copy, the wording of the original hard copy will have priority over the wording of the soft copy.

Pricing is not a requirement and should not be included in the response.

a. **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.
   v. Soft copies will be accepted in any of the following electronic formats:
      - Portable Document Format (.pdf) in a searchable format
      - Microsoft Word 97/2000 (.doc)
      - Microsoft Excel 97/2000 (.xls)

b. **Canada's Policy on Green Procurement:** The 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 (https://www.tpsgc-pwgsc.gc.ca/app-acq/ae-gp/paecoif-pgptts-eng.html). To assist Canada in reaching its objectives, bidders are encouraged to :

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

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

3.2 Contents of Each Volume

Volume I: Technical Response

In the response, Respondents are requested to explain and demonstrate how their response meets the ITQ technical requirements.

The Technical Response must include submission of:

1. Form 1: ITQ Submission Form;
2. Attachment 1 to Part 5: Mandatory Evaluation Criteria;
3. Form 2: Project Reference Check Form; and
4. Form 3: Non-Disclosure Agreement for Participation in Solicitation Process

Volume II: Application of the Industrial and Technological Benefits (ITB) Policy

Respondents must address the Application of the ITB Policy as detailed in Annex D

Volume III: Certifications

Respondents must submit the certifications required under Part 6.

PART 4 - OVERVIEW OF PROCUREMENT PROCESS

4.1 Overview

4.1.1 The Net C2 ISAC Project's Prime Integrator requirement will be fulfilled through a multi-phase collaborative procurement process. It is intended that a single contract resulting from any subsequent bid solicitation will be awarded by PWGSC to a single supplier to act as the Net C2 ISAC Prime Integrator This approach focuses on the engagement with industry in order to help define the requirements and the procurement approach. This approach will allow Canada to perform due diligence with respect to the requirements with ITQ Responsive Suppliers before issuing the bid solicitation. Figure 1 below depicts the major phases of the procurement approach.

4.1.2 The Qualification Phase is the first phase of the Net C2 ISAC multi-phase procurement process. Although the procurement process remains subject to change (and even to cancellation), Canada currently anticipates that the procurement process will be conducted as shown in Figure 1. Additional information on the Net C2 ISAC procurement process can be found in Annex B: Draft Net C2 ISAC Procurement Process.

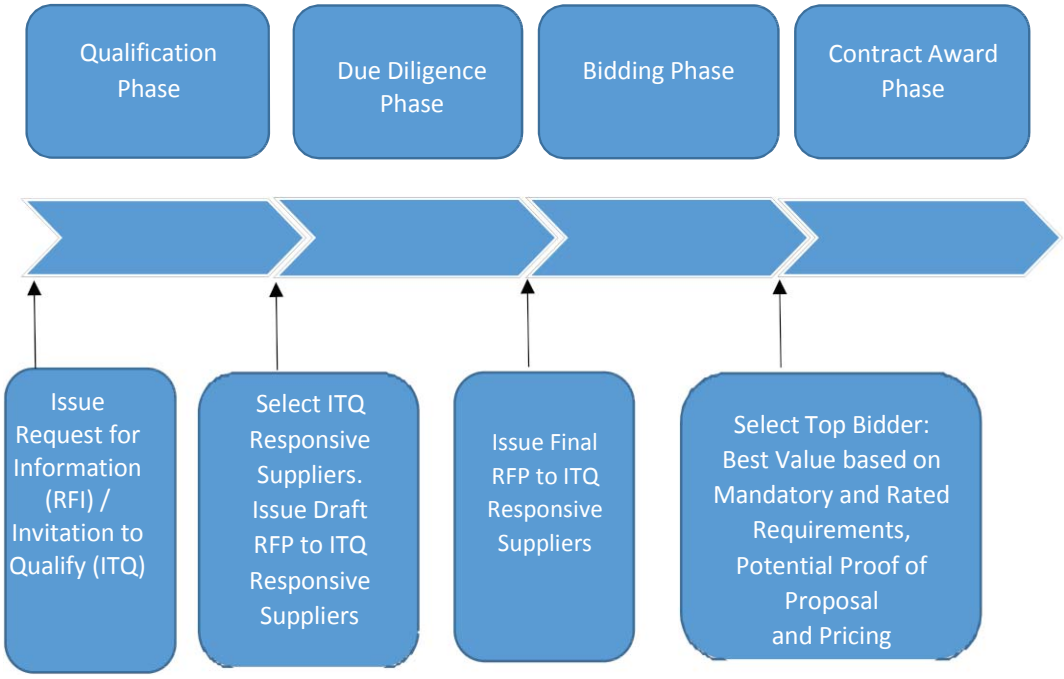
4.1.3 Qualification Phase: The ITQ defines the requirements for the Qualification Phase. The objective of the Qualification Phase is to qualify Respondents for further consideration in the Net C2 ISAC procurement process. Refer to Part 5 of the ITQ for a more detailed explanation of the ITQ Evaluation Procedures and Selection of ITQ Responsive Suppliers. This ITQ is open to all Suppliers and will result in ITQ Responsive Suppliers being invited to participate in the Due Diligence Phase. Respondents will be notified of the evaluation results once the ITQ evaluation process is completed.

4.1.4 Due Diligence Phase: The objective of the Due Diligence Phase is to further refine the Net C2 ISAC Prime Integrator requirement by obtaining industry feedback from ITQ Responsive Suppliers, addressing industry concerns and considering industry best practices. It is anticipated that ITQ Responsive Suppliers will be engaged to review preliminary RFP documents, including system information, the draft Statement of Work (SOW) and draft Evaluation Criteria, provide feedback electronically, as well as attend industry day meetings and one-on-one meetings, to discuss specific issues relating to the content of the preliminary RFP documents. Further details regarding the Due Diligence Phase will be provided to ITQ Responsive Suppliers. The RFP will be finalized following the draft RFP process. Only ITQ Responsive Suppliers will be permitted to participate in the Due Diligence Phase. Each ITQ Responsive Supplier will identify the individual(s) who will participate in the Due Diligence Phase on its behalf.

4.1.5 Bid Solicitation Phase: During this phase, Canada anticipates releasing the final RFP directly to ITQ Responsive Suppliers who have not withdrawn from the procurement process, and who remain responsive at the time the RFP is released. Reference Part 8 for further details of the anticipated RFP. A contract will only be awarded after completion of

the Bid Solicitation Phase and when all necessary approvals have been obtained.

Figure 1. Net C2 ISAC Procurement Approach



PART 5 - EVALUATION PROCEDURES AND BASIS OF QUALIFICATION

5.1 Evaluation Procedures

5.1.1 Responses will be assessed in accordance with the entire requirement of the ITQ, including the technical evaluation criteria.

5.1.2 An evaluation team composed of representatives of Canada and possibly independent consultants will evaluate the responses. Canada may hire any independent consultant, consulting firm or use any Government resources to evaluate any ITQ response. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation. By submitting a response, Respondents consent to the release of those responses to the third-party consultants retained by Canada, subject to Canada's obtaining confidentiality undertakings from these third-party consultants.

5.1.3 In addition to any other time periods established in the solicitation process:

a. Requests for Clarifications: If Canada seeks clarification or verification from the Respondent about its response, the Respondent will have two (2) calendar days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada; and

b. Extension of Time: If additional time is required by the Respondent, the Contracting Authority may grant an extension at his or her sole discretion.

5.2 Technical Evaluation

5.2.1 Each response will be reviewed for compliance with the mandatory requirements of this ITQ. Responses that do not comply with each and every mandatory requirement will be considered non-responsive and given no further consideration.

5.2.2 The Mandatory Evaluation Criteria, and Substantiation of Technical Compliance - Mandatory Evaluation Criteria, are described in Attachment 1 to Part 5.

5.2.3 Respondents should demonstrate their understanding of the requirements contained in this ITQ and address clearly and in sufficient depth the points that are subject to the evaluation. Simply repeating the statement contained in the ITQ is not sufficient.

5.2.4 In conducting its evaluation of the responses, Canada may, but will have no obligation to, do the following:

a. contact any or all references supplied by Respondents to verify and validate any information submitted by the Respondents; and

b. seek clarification or verification from Respondents regarding any or all information provided by them with respect to the ITQ.

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

5.2.6 Only referenced material included within the Respondent's response, or clarified upon request by the Contracting Authority, will be evaluated. Reference material outside of the Respondent's response will not be considered. It is the sole responsibility of the Respondent to provide sufficient information so that their responses can be adequately evaluated.

5.3 Reference Checks

5.3.1 The Respondent is requested to provide a third-party reference for each project in its response as requested in Attachment 1 to Part 5: Mandatory Evaluation Criteria, using Form 2: Project Reference Check Form. If information requested is not provided in the response, the Respondent must provide the information upon request by the Contracting Authority within the timeframe identified in the request. References from representatives of Canada will be accepted.

5.3.2 It is the responsibility of the Respondent to confirm in advance that their client contact for the project reference will be available to provide a response and is willing to provide a reference.

5.3.3 For the purpose of this evaluation, reference checks may be used to verify and validate the Respondent's response. If a reference check is performed, Canada will conduct the reference check in writing by e-mail. Canada will send the reference check request directly to the client contact for the project reference provided by the Respondent. The client contact will have five (5) calendar days (or a longer period otherwise specified in writing by the Contracting Authority) from the date that Canada's e-mail was sent, to respond to Canada.

5.3.4 The client contact will be required, within two (2) calendar days after Canada sends out the reference check request, to acknowledge the receipt of the reference check request and identify his or her willingness and availability to conduct such reference check. If Canada has not received the required response from the client contact, Canada will notify the Respondent by e-mail, to allow the Respondent to contact its client contact directly to ensure that he or she responds to Canada within the allotted time. The client contact's failure to respond to Canada's request in a timely manner will result in non-consideration of the Respondent's claimed project experience.

5.3.5 Notwithstanding section 5.3.3, the Respondents are requested to provide an alternate client contact for the same referenced project. The process as described in 5.3.3 is applicable for the reference check with the alternate client contact.

5.3.6 Wherever information provided by a client contact differs from the information supplied by

the Respondent, the Respondent will be asked to clarify project reference information provided in its ITQ response. Canada will assess the following information during the evaluation of the Respondent's response: the Respondent's original project reference information; any information provided by the Respondent in response to clarification request(s); and any information supplied by the client contact for the referenced project.

5.3.7 A Respondent will not meet the mandatory experience requirement if:
(1) the client contact fails to respond to Canada's request in a timely manner
(2) the client contact states he or she is unable or unwilling to provide the information requested;
(3) the information provided by the Respondent cannot be verified and validated by Canada; or
(4) the client is itself an affiliate or other entity that does not deal at arm's length with the Respondent.

5.4 Basis of Qualification

5.4.1 Selection of ITQ Responsive Suppliers

5.4.1.1 To be declared responsive, a response must:

a. comply with all the requirements of this ITQ; and
b. comply with all of the Mandatory Evaluation Criteria (Attachment 1 to Part 5).
c. hold the required security clearances prior to the start of the Due Diligence Phase.

If a response fails to meet the any of the above, it will be declared non-responsive and given no further consideration.

5.4.1.2 Respondents whose submissions are deemed responsive will be selected as ITQ Responsive Suppliers to participate in the remaining steps of the procurement process.

PART 6 – CERTIFICATIONS

Respondents must provide the required certifications and associated information to become an ITQ Responsive Supplier.

The certifications provided by Respondents to Canada are subject to verification by Canada at all times. Canada will declare a response non-responsive, if any certification made by the Respondent is found to be untrue whether made knowingly or unknowingly during the ITQ response evaluation period.

The Contracting Authority will have the right to ask for additional information to verify the Respondent's certifications. Canada has the right to terminate the Respondent status, if the Respondent fails to comply and to cooperate with any request or requirement imposed by the Contracting Authority.

6.1 Certifications Precedent to becoming an ITQ Responsive Supplier

The certifications listed below must be completed and submitted with the response. If any of these required certifications are not completed and submitted as requested, the Contracting Authority will inform the Respondent and provide it with a time frame within which to provide the information. Failure to comply with the request of the Contracting Authority and to provide the certifications within the time frame will render the response non-responsive.

6.1.1 Integrity Provisions – Required Documentation

In accordance with the Ineligibility and Suspension Policy (https://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html), the Respondent must provide the required documentation, as applicable, to be given further consideration in the procurement process.

6.1.2 Former Public Servant – Competitive Response

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, Respondents 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 responses is completed, Canada will inform the Respondents 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.

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:

a. an individual;

b. an individual who has incorporated;

c. a partnership made of former public servants; or

d. a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"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.

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Respondent a FPS in receipt of a pension? Yes ( ) No ( ) If so, the Respondent must provide the following information, for all FPSs in receipt of a pension, as applicable:

a. name of former public servant;

b. date of termination of employment or retirement from the Public Service.

By providing this information, Respondents agree that the successful Respondent'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.

Work Force Adjustment Directive

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

If so, the Respondent must provide the following information:

a. name of former public servant;

b. conditions of the lump sum payment incentive;

c. date of termination of employment;

d. amount of lump sum payment;

e. rate of pay on which lump sum payment is based;

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

g. 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.

6.1.3 Non-Disclosure Requirement.

The Respondent shall complete, and include with its response, Form 3: Non-Disclosure Agreement (NDA) for Participation in the Solicitation Process.

6.1.4 Certificate of Independent Bid Determination

The Respondent shall complete, and include with its response, a Certificate of Independent Bid Determination which can be found at:

http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/00599.html

6.1.5 Acknowledgement

By submitting a response, the Respondent represents that it has full authority to bind the company and individuals representing the company, to be bound by all the terms and conditions contained herein.

PART 7 - SECURITY REQUIREMENT

7.1 Security Requirement

7.1.1 Security Requirement at the Qualification Phase

There is a security requirement associated with the Qualification Phase: respondents must hold the appropriate security clearances prior to the commencement of the Due Diligence Phase. In order to be invited to the Bidder Conference (which is the commencement of the Due Diligence Phase), respondents must hold the appropriate security clearances as detailed below. When Canada is prepared to invite Respondents to the Bidder Conference (date to be determined), the PWGSC Contracting Authority will contact CISD to verify each Respondents' clearances. Those Respondents who do not hold the appropriate clearances at that time will be contacted and advised that they have been screened-out of the remaining Net C2 ISAC procurement process.

7.1.2 There will be security requirements for the RFP. Preliminary security requirements for the RFP and resulting Contract are outlined in Part 9 of this document to assist Suppliers in preparing for the RFP security requirements.

7.1.3 As there will be security requirements for the Due Diligence Phase, and the RFP and resulting Contract, Suppliers that do not currently have personnel and organization security clearances through the Canadian federal government or their respective domestic Industrial Security Program, or Suppliers that do not meet the anticipated security requirements outlined in Part 9, should begin the clearance process early by contacting the Industrial Security Program (ISP) of PWGSC (https://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html) website, or their respective domestic Industrial Security Program, as applicable.

7.2 Security Requirement at the Due Diligence Phase

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

7.2.2. 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 (Public Works and Government Services Canada (PWGSC).

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

7.2.4. The Contractor **MUST NOT** utilize its Information Technology systems to electronically process, produce or store any sensitive **CLASSIFIED / PROTECTED** information until CISD/PWGSC has is-sued written approval. After approval has been granted, these tasks may be performed at the level of **SECRET**.

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

7.2.6. The Contractor/Offeror must comply with the provisions of the:

a) Security Requirements Check List and security guide (if applicable), attached at Appendix 1 to Annex E

b) *Industrial Security Manual* (Latest Edition).

PART 8 - ANTICIPATED REQUEST FOR PROPOSAL (RFP)

8.1 Bid Solicitation Components

8.1.1 Canada will use the High Complexity (HC) bid solicitation template for the anticipated RFP.

8.1.2 A copy of the template can be found at:

https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-sacc-manual/standard-procurement-templates

8.1.3 The latest versions of the template and terms and conditions will be used in the anticipated RFP. The numbering of sections, annexes, attachments and forms may change in the final RFP.

8.1.4 At a minimum the anticipated RFP may contain the following:

a. security, database location, and privacy requirements;
b. financial capability (reference SACC A9033T);
c. a complete description of the Work to be performed;
d. 2003, Standard Instructions - Goods or Services - Competitive Requirements;
e. bid preparation instructions;
f. instructions for the submission of bids;
g. evaluation procedures and basis of selection;
h. terms and conditions of the resulting Contract; and
i. certifications.

8.1.5 It is anticipated that certifications, at time of bid submission, may include, but may not be limited to the following:
1) Integrity Provisions - Associated Information;
2) Former Public Servant – Competitive Bid (reference SACC A3025T);
3) Federal Contractors Program for Employment Equity – Bid Certification; and
4) Status and Availability of Subcontractors Providing Core Services.

8.1.6 Phased Bid Compliance Process

8.1.6.1 The Phased Bid Compliance Process (PBCP) will be applied to the RFP for this procurement. For more information on the PBCP, please visit the following link:

https://buyandsell.gc.ca/policy-and-guidelines/policy-notifications/PN-123

PART 9 - SUBSET OF ANTICIPATED RESULTING CONTRACT CLAUSES

9.1 General

9.1.1 The conditions of any Contract awarded as a result of the RFP will be in accordance with the relevant resulting Contract clauses of the HC template used for the RFP.

9.1.2 Only a subset of the anticipated resulting Contract clauses are included in this section in order to provide ITQ Responsive Suppliers advance notice, as well as to allow ITQ Responsive Suppliers time to consider the impact of said clauses and provide feedback to Canada as required.

9.2 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 PWGSC.

9.2.1 General Conditions

2030 (2018-06-21), General Conditions – Higher Complexity – Goods, apply to and form part of the Contract.

9.3 Anticipated Security Requirements

Only a subset of the anticipated RFP security clearance requirements are included in this section in order to provide ITQ Responsive Suppliers advance notice of said requirements. It is anticipated the security clearance requirements will be expanded in the RFP. It is also anticipated that the personnel and facility(ies) proposed by the ITQ Responsive Supplier must hold the required security clearances at the closing date of the RFP.

For information purposes, ITQ Responsive Suppliers are hereby informed that the amount of time to obtain required security clearance levels may be lengthy and is contingent upon the specific clearance levels required. ITQ Responsive Suppliers are solely responsible for obtaining such clearances.

A. ANTICIPATED SECURITY REQUIREMENT FOR CANADIAN SUPPLIERS:

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Facility Security Clearance at the level of **SECRET**, with approved Document Safeguarding at the level of **SECRET**, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC) as well as Communications-Electronic Security (COMSEC) account at the level of **SECRET**, issued by the Communications Security Establishment Canada (CSEC).

2. 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 (Public Works and Government Services Canada (PWGSC).

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

4. The Contractor personnel requiring access to **COMSEC** information/assets **must be citizens of Canada and/or United States and must EACH** hold a valid security clearance commensurate with the information/assets that will be accessed, have a need-to-know and have undergone a COMSEC briefing and signed a COMSEC Briefing certificate. Access by foreign nationals or resident aliens must be approved by the Head IT Security Client Services at CSEC on a case-by-case basis.

5. The Contractor **MUST NOT** utilize its Information Technology systems to electronically process, produce or store any sensitive **CLASSIFIED / PROTECTED** information until CISD/PWGSC has issued written approval. After approval has been granted, these tasks may be performed at the level of **SECRET** and an IT Link at the level of **SECRET**.

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

7. 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 **COMSEC** 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"*.

8. 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.*

9. 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.

10. The Contractor/Offeror must comply with the provisions of the:

    (a) Security Requirements Check List and security guide (if applicable), attached at Appendix 2 to Annex E
    (b) *Industrial Security Manual* (latest edition) and the *IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06A).

NOTE: Keying material and associated devices bearing (or intended to bear) the caveat, "CRYPTO", are subject to special safeguards at all times, whether: in bulk storage; in custody at user locations; in current use; or awaiting destruction. Keying Material must be stored in a locked, approved security container, in an area protected by security guards or by an intrusion- detection system when left unattended by COMSEC account personnel or authorized users.

B. ANTICIPATED SECURITY REQUIREMENT FOR UNITED STATES OF AMERICA SUPPLIERS:

All **CANADA PROTECTED / CLASSIFIED** information/assets, furnished to the Foreign recipient **Contractor / Offeror / Subcontractor** or produced by the Foreign recipient **Contractor / Offeror / Subcontractor**, shall be safeguarded as follows:

1. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of the **Contract / Standing Offer / Subcontract**, hold a valid Facility Security Clearance (FSC), issued by the National Security Authority (NSA) or Designated Security Authority (DSA) of **the UNITED STATES OF AMERICA**, at the equivalent level of **SECRET**, and hold an approved Document Safeguarding Capability Clearance at the level of **SECRET**, issued by the National Security Authority (NSA) or Designated Security Authority (DSA) for industrial security of **the UNITED STATES OF AMERICA** in accordance with the national policies of **the UNITED STATES OF AMERICA**.

2. All **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated under this **Contract / Standing Offer / Subcontract** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Contract / Standing Offer / Subcontract**, in accordance with the national policies of **the UNITED STATES OF AMERICA.**

3. The Foreign recipient **Contractor / Offeror / Subcontractor** shall provide the **CANADA PROTECTED / CLASSIFIED** information/assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the national policies, National Security legislation and regulations and as prescribed by the National Security

Authority (NSA) or Designated Security Authority (DSA) of **the UNITED STATES OF AMERICA**.

4. All **CANADA PROTECTED / CLASSIFIED** information/assets provided to the Foreign recipient **Contractor / Offeror / Subcontractor** pursuant to this **Contract / Standing Offer / Subcontract** by the Government of Canada, shall be marked by the Foreign recipient **Contractor / Offeror / Subcontractor** with the equivalent security classification utilized by **the UNITED STATES OF AMERICA** and in accordance with the national policies of **the UNITED STATES OF AMERICA**.

5. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of this **Contract / Standing Offer / Subcontract**, ensure the transfer of **CANADA PROTECTED / CLASSIFIED** information/assets be facilitated in accordance with the national policies of **the UNITED STATES OF AMERICA**, and in compliance with the provisions of the Bilateral Industrial Security Instrument between **the UNITED STATES OF AMERICA** and Canada.

6. Upon completion of the work, the Foreign recipient **Contractor / Offeror / Subcontractor** shall return to the Government of Canada, via government-to-government channels, all **CANADA PROTECTED / CLASSIFIED** information/assets furnished or produced pursuant to this **Contract / Standing Offer / Subcontract**, including all **CANADA PROTECTED / CLASSIFIED** information/assets released to and/or produced by its subcontractors.

7. Throughout the duration of this **Contract / Standing Offer / Subcontract**, the Foreign recipient **Contractor / Offeror / Subcontractor** shall adhere to its respective national policies pertaining to the examination, possession and / or transfer of Canadian Controlled Goods and shall immediately report to its responsible National Security Authority (NSA) all cases in which it is known or there is reason to suspect that Canadian Controlled Good, furnished or generated pursuant to this **Contract / Standing Offer / Subcontract** have been lost or disclosed to unauthorized persons, including but not limited to a third party government, person, firm, or representative thereof. Canadian Controlled Goods which are lost or compromised while handled outside of Canada, should be immediately reported to the Canadian Government Authority owner of the Canadian Controlled Goods, for example the Canadian Department that issued the Canadian Controlled Goods to the Foreign recipient **Contractor / Offeror / Subcontractor**, as part of this **Contract / Standing Offer / Subcontract**. The *Defence Production Act* defines Canadian Controlled Goods (S.35).

8. Such **CANADA PROTECTED / CLASSIFIED** information/assets shall be released only to foreign recipient **Contractor / Offeror / Subcontractor** personnel who have a need to know for the performance of the **Contract / Standing Offer / Subcontract**, must be a citizen of **the United States of America** ***and / or a Canadian citizen and/ or a Permanent Resident of Canada***, and must each hold a valid personnel security screening at the level of **SECRET**, as required, granted or approved by their respective country National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the national policies of **the UNITED STATES OF AMERICA.**

9. **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated pursuant to this **Contract / Standing Offer / Subcontract** shall not be further provided to a third party Foreign recipient Subcontractor unless:
    a. written assurance is obtained from the third-party Foreign recipient's National Security Authority (NSA) or Designated Security Authority (DSA) to the effect that the third-party Foreign recipient Subcontractor has been approved for access to **CANADA PROTECTED / CLASSIFIED** information/assets by the third-party Foreign recipient's NSA/DSA; and
    b. written consent is obtained from the NSA/DSA of **the UNITED STATES OF AMERICA**, if the third-party Foreign recipient Subcontractor is located in a third country.

10. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of their respective National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the national policies of **the UNITED STATES OF AMERICA.**

11. A Communications-Electronic Security (COMSEC) account at the **SECRET** level must be issued and confirmed by the National Communication Security Authority (NCSA) of **the UNITED STATES OF AMERICA**. The Foreign recipient **Contractor / Offeror / Subcontractor** requiring access to accountable COMSEC material (ACM) and/or COMSEC information/assets must be citizens of **the United States of America *and / or a Canadian citizen and/ or a Permanent Resident of Canada***, hold a valid Personnel security clearance commensurate with the information/assets that will be accessed, have a need to know, have undergone a COMSEC briefing and signed a COMSEC Briefing Certificate. Access by Foreign Nationals or "Resident Aliens" must be approved by the NCSA of **the United States of America *and / or a Canadian citizen and/ or a Permanent Resident of Canada***, on a case by case basis. Such approvals must be communicated in writing to the Canadian Designated Security Authority (DSA).

12. The Foreign recipient **Contractor / Offeror / Subcontractor** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA CLASSIFIED** information/assets until the National Security Authority (NSA) or Designated Security Authority (DSA) of **the UNITED STATES OF AMERICA** has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Contractor / Offeror / Subcontractor**, these tasks may be performed up to the level of **SECRET.**

13. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not use the **CANADA PROTECTED / CLASSIFIED** information/assets for any purpose other than for the performance of the **Contract / Standing Offer / Subcontract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

14. The Foreign recipient **Contractor / Offeror / Subcontractor** visiting Canadian Government or industrial facilities, under this contract, will submit a Request for Visit form to Canada's Designated Security Authority (DSA) through their respective National Security Authority (NSA) or Designated Security Authority (DSA).

15. The Foreign recipient **Contractor / Offeror / Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED / CLASSIFIED** information/assets pursuant to this **Contract / Standing Offer / Subcontract** has been compromised.

16. The Foreign recipient **Contractor / Offeror / Subcontractor** shall immediately report to its respective National Security Authority (NSA) or Designated Security Authority (DSA) all cases in which it is known or there is reason to suspect that **CANADA PROTECTED / CLASSIFIED** information/assets accessed by the Foreign recipient **Contractor / Offeror / Subcontractor**, pursuant this **Contract / Standing Offer / Subcontract**, have been lost or disclosed to unauthorized persons.

17. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not disclose **CANADA PROTECTED / CLASSIFIED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent shall be sought through the recipient's National Security Authority/ Designated Security Authority (NSA/DSA).

18. The Foreign recipient **Contractor / Offeror / Subcontractor** shall comply with the provisions of the International bilateral industrial security instrument between **the UNITED STATES OF AMERICA** and Canada, in relation to equivalencies.

19. The Foreign recipient **Contractor / Offeror / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Appendix 2 to Annex E.

20. The Foreign recipient **Contractor / Offeror / Subcontractor** must use the below table of equivalency in conjunction with the above paragraphs, in accordance with the national policies of **the UNITED STATES OF AMERICA**, and in accordance with the provisions of the International bilateral industrial security instrument between **the UNITED STATES OF AMERICA** and Canada, in relation to the equivalencies of **CANADA PROTECTED A and/or CLASSIFIED CONFIDENTIAL AND SECRET** information/assets.

UNITED STATES of AMERICA & CANADA TABLE OF EQUIVALENCY	
CANADA	**UNITED STATES of AMERICA**
CONFIDENTIAL	CONFIDENTIAL
SECRET	SECRET

C. SUPPLY CHAIN INTEGRITY AND SECURITY

1. References:
a) https://www.cse-cst.gc.ca/en/page/technology-supply-chain-guidance
b) https://www.cse-cst.gc.ca/en/node/300/html/25733
c) https://www.cse-cst.gc.ca/en/node/299/html/25729

2. The Communications Security Establishment Canada (CSEC) offers IT Security advice and

guidance to the GC on supply chain threats and vulnerabilities, as well as prevention and mitigation guidance.

3. The guidelines for Contracting Clauses for Telecommunications Equipment and Services (TSCG-01\G) provides security clauses that can be included in Public Works and Government Services Canada (PWGSC) contracts with the aim of preventing or mitigating supply chain risks to GC communications networks and information technology (IT) infrastructure, often referred to as Supply Chain Integrity.

4. The clauses are based on a "managed telecommunications services" scenario, whereby a contractor is given responsibility for selecting, implementing, operating and maintaining the telecommunications infrastructure and services for GC clients. Some of the clauses are also relevant for IT solution or hardware/equipment procurement. The guidelines identify a process to select and tailor specific clauses, including the cost, schedule and requirements considerations.

5. The Contracting Clauses for Telecommunications Equipment and Services Leaflet (TSCG-01\L) describes the purpose and provides an overview of the clause groupings.

Annex A – High Level Requirements

1.1 Project Background

The Canadian Armed Forces (CAF) is becoming increasingly reliant upon communications and computer networks to perform every aspect of operational and planning activities. Information Technology (IT) Applications such as Email, Chat, Web Services, File Servers, Database Applications, Mobile Phone, Text Messaging, and others are critical to the success of operations, be they domestic, international, expeditionary or corporate services/administrative functions.

The challenge is that for every IT Service there is a vast network of IT Assets that form part of delivery of the IT Service. If one or more of the dependant IT Assets fail or lose some functionality, the associated IT Services can fail or have degraded functionality.

At present, no coherent IT Service status monitoring and alert capability exists in the CAF to effectively support the Operational and Strategic Commanders and their Staff (OSC&S) in their missions. Status information regarding IT Services is produced through a process that is largely manual and involves analyzing various data feeds from IT Assets along with trouble reports from users of the IT Services. Reports on the availability of some IT Assets can be produced within a few minutes following the report of a failure but there is no automatic connection to the specific IT Services that may be affected by the failed IT Assets. Thus, the OSC&S are missing some of the essential information necessary to make well-informed decisions regarding the command and control of their operations.

Figure 1 is a pictorial of the current Situation Awareness process provided to OSC&S. The process is largely reactive (problem occurs and assistance is requested) rather than proactive (data indicates IT Service issues resulting in notifications).

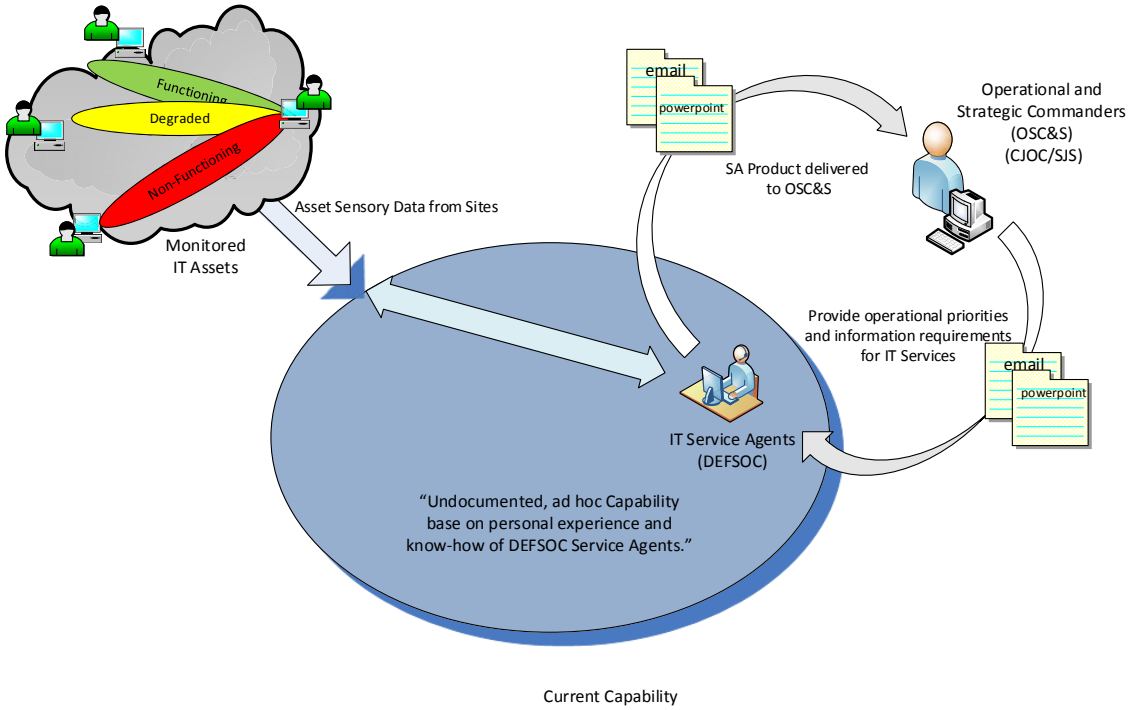


Figure 1 – Current Capability

1.2 Capability Deficiency

Situational Awareness (SA) is defined as the *"knowledge of the elements in the operational environment necessary to make well-informed decisions."*[1]

Department of National Defence / Canadian Armed Forces (DND/CAF) current IT Service SA is provided in an ad-hoc, mostly manual approach putting OSC&S largely into reactive roles, preventing any planning activities.

When the capability is delivered, the IT Service SA provided will be able to deal in part or in whole with the below operational decision-making scenarios:

1.2.1 Operational Readiness.
Is the ITI working and if not, what alternatives are available so as to not jeopardize mission success? SA must be near real time and accurate;

1.2.2 Operational Priority Planning to conduct Defence Cyber Operations.
What Operations, in order of priority, are affected if or when, one or more elements of the Information Technology Infrastructure (ITI) fail? Personnel responsible to conduct Defence Cyber Operations require operational priorities to be provided so that they can carry out

[1] Defence Terminology Bank, Record 41441

Defence Cyber Operations; and

1.2.3 Operational Priority Planning for ITI Improvement/Investment.
What Operations, in order of priority, can be better supported through ITI improvement and investment? Planned investments and improvements can lead to mitigating or minimizing risk to ITI.

1.3 Project Overview

The Net C2 ISAC project will deliver a cyberspace SA capability that achieves the operational requirement of mapping IT services to priority defence operations and missions, and implement a stabilization period for in-service support for the capability as a whole. The intent of the Network Command and Control Integrated Situational Awareness Capability (Net C2 ISAC) is to provide OSC&S the knowledge of key elements in the ITI necessary to make well-informed decisions regarding the command, control, and conduct of their operations in and through the cyber environment. In general, this will be accomplished by:

(a) Reducing, to the furthest extent possible, the manual, reactive nature in which Network Situational Awareness (Net SA) is produced and disseminated;

(b) Providing a reliable and robust means to map IT Assets and IT Services; and

(c) Providing OSCS with the knowledge of IT Services required to allow well-informed decisions regarding missions and CAF operations.

Net C2 ISAC will provide network command and control situational awareness on the SECRET domain (Consolidated Secret Network Infrastructure (CSNI) and Environmental Chiefs of Staff extensions, where appropriate) as well as the Deployed Designated Domain (also known as the Defence Wide Area Network (DWAN)), to support decision-making for command, control, and conduct of operations in and through the cyber domain. When pieced together, IT Alerts, IT Service status reports, IT Service maps, IT Asset technical information, and priority mission mapping will allow commanders, their staffs, and IT Service Agents operators, to develop situational awareness related to IT networks and IT services.

1.4 DND/CAF Capital Project Governance

The project life cycle for DND projects is governed by the department's Project Approval Directive. The DND project lifecycle is normally as follows: Problem Identification, Options Analysis, Definition, Implementation and Close Out phases. The Net C2 ISAC project has completed its Options Analysis phase.

Definition Part 1 is the current phase of the project that largely consists of work to further refine the Statement of Operational Requirements and to establish project cost estimates to seek Expenditure Authority (EA) for the subsequent project phase. It includes conducting the Qualification Phase of the Net C2 ISAC procurement process, performing engagement with Invitation to Qualify (ITQ) Responsive Suppliers on the draft RFP, issuing the final bid solicitation to ITQ Responsive Suppliers and obtaining costing data of sufficient confidence to substantiate EA for Definition Part 2.

Definition Part 2 is the next phase of the project that is primarily designing and prototyping. It includes awarding the Prime Integrator contract for the RFP that was published during Definition Part 1. The Prime Integrator will conduct all the necessary work to design the required solution. Key deliverables will include a detailed system design, prototyping, initial testing to confirm solution acceptance, an implementation plan, and cost estimates for the implementation of the solution. Following this, the DND/CAF project team will proceed to EA for Implementation.

Implementation is the final phase of the project that includes implementing the design created in Definition Part 2, and also includes integrated logistics support elements such as business process improvements, training, support plans, spares, etc. After the capability is launched, the Prime Integrator will stabilize the capability by performing the support function for a year.

Project Close Out will be completed by the Project Management Office, including transition to In-Service Support (i.e. the Prime Integrator is not involved in this phase).

See Figure 2 for a pictorial representation of the project phases and a high level anticipated timeline associated with the project.

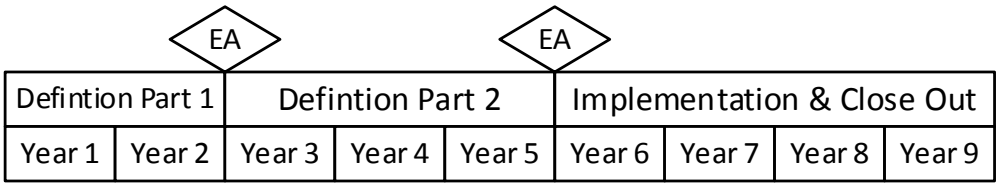


Figure 2 – Net C2 ISAC Project Lifecycle Representation

1.5 Prime Integrator Contractor Responsibilities

1.5.1 General

This ITQ is being conducted in anticipation of a Request for Proposal (RFP) to acquire a Prime Integrator to provide professional services to create the Net C2 ISAC solution for DND/CAF.

The overall responsibilities will include:

a. capability design & prototype services and all other definition work required to launch the DND/CAF capability; and

b. implementation services to deliver and deploy the capability and a one year stabilization support of the implemented capability.

The Net C2 ISAC solution shall provide SA on the ITI, which is principally achieved by:

i. determining what IT Services are essential to missions, operations and tasks defined by the OSC&S;

ii. determining how IT Assets relate to IT Services and then monitoring the appropriate IT

Assets in the most appropriate manner (should another viable method be available, with DND's permission it may be used in place of this one);

iii. creating Alerts and Status Reports on IT Services when required; and

iv. disseminating these Alerts and Status Reports as required by the OSC&S.

1.5.2 SA Products

Based on the operational priorities defined by the OSC&S, Net C2 ISAC shall monitor key assets, process the data collected from various sensors within the ITI, and prepare the following SA Products outlined in the sub-sections below.

1.5.2.1 IT Service Maps

IT Service Maps are fundamentally text and graphic descriptions of the Cyber Terrain, as it relates to missions, operations and tasks, much the way street maps or topographic maps describe physical terrain. The goal is to help OSC&S visualize the key aspects of the ITI in a manner that allows their understanding of the physical situation.

IT Service Maps are a listing of monitored IT Assets that support the effective functioning of an IT Service. The IT Service Map shows the functional relationship and dependency of monitored IT Assets in a connectivity and interdependency hierarchy as it relates to the function of an IT Service and a mission, operation or task.

The IT Service Map is the initial output of the creation of an IT Service Monitoring Task. It defines all necessary IT Assets required to report on the status of the IT Service. This map will likely be classified as it will contain information vital to the success of some missions, operations or tasks.

For each IT Service being monitored, IT Service Maps shall list:

a. the date and time that the IT Service Map was last confirmed;

b. the name, title or description of the mission, operation, or task using the IT Service;

c. the key command or staff personnel involved in managing the success of the mission, operation or task and depend upon the IT Service;

d. the IT Service Locale(s) in which the key command or staff personnel will be located and from where they will access the IT Service;

e. all the IT Assets that are required to generate the IT Service status alerts; and

f. the owner and where possible the geographic location of the IT Asset including any other existing meta-data associated with the IT Asset.

IT Service Maps shall be produced in a manner that best permits integration with the Joint Battleship Management Capability (JBMC), including a geographic referenced format similar to that used by Command View, that shows the specific locations of the IT Assets where possible, their interconnectivity and inter-dependency using custom icons and connecting lines.

1.5.2.2 IT Alerts

IT Alerts are notifications that are disseminated as soon as possible to selected OSC&S. These notifications describe:

a. the date and time that a change in functioning status of an IT Service was detected;

b. the name, title or description of the mission, operation, or task using the IT Service; and

c. the nature of the change to IT Service functionality.

1.5.2.3 IT Status Reports

IT Status Reports are summary descriptions of the functioning status of one or more IT Services. These IT Status reports are disseminated on demand or on some pre-defined schedule to selected OSC&S and describe:

a. the date and time that the status was last confirmed;

b. the name, title or description of the mission, operation, or task using the IT Service;

c. the status of the IT Service functionality (Functioning, Not Functioning, Degraded (See Note)); and

d. IT Assets (if known) causing the service to not function or have degraded functionality.

Note: *The measure of Degraded Functionality will be dependent upon the nature of the IT Service being monitored. Examples of Degraded Functionality include: limited bandwidth, a thrashing state of a router may allow some data to pass but not all, or a failed DNS may not affect connectivity to all users as some host devices may have a cache of IP addresses and therefore not need DNS. Full description of Degraded Functionality will be defined during the definition phase of the project.*

Table 1: Glossary of Terms

Operational and Strategic Commanders and their Staff (OSC&S)	Commanders and Staff with responsibility for planning, coordinating and managing Canadian Missions, Operations and Tasks. This is principally restricted to Strategic Joint Staff (SJS), Canadian Joint Operations Command (CJOC) and Canadian Special Operations Forces Command (CANSOFCOM), but all Level 0 and Level 1 organizations in DND may fill this role under specific circumstances.
IT Assets	IT Asset is defined as “any elements of software and/or hardware that are part of Information Technology” IT Assets of interest may be gateways, switches, routers, firewalls and servers.
IT Asset Data	IT Asset Data (i.e. SNMP, Syslog, Net Flow, Windows Security Events, Windows Events, etc) will be collected from the IT Assets identified for monitoring at the sites.

IT Service	An IT application or function between two or more sites that supports a Command and Control process (e.g. email between users on Her Majesty's Canadian Ship (HMCS) Regina to users at Esquimalt).
IT Service Maps	IT Service Map is a map with the key IT Assets identified for a specific IT Service i.e. IT Service Maps are a listing of monitored IT Assets that support the effective functioning of an IT Service. An IT Service map shows relationships between a business service and its IT components.
Information Technology Infrastructure (ITI)	The set of computers, communications, systems software, utility programmes, and management tools which support the automation of information management throughout an organization. Infrastructure does not include applications and their associated databases.
Joint Battlespace Management Capability (JBMC)	A Joint Information and Intelligence Fusion Capability project deliverable which will allow for access to the dynamic visualizations and permission-controlled Battlespace Management functionality. JBMC is the interface for the inputs/outputs to/from the Net C2 ISAC system. Canadian JBMC System will be employed at the Operational/Strategic Level as opposed to the tactical level and on static level II (two eyes) network across Canada (CSNI). Primary users are the Canadian Joint Operations Command (CJOC) staff Central Headquarters in Ottawa, and Six (6) Regional Operational Head Quarters. SJS is the Operational Authority.
Key Cyber Terrain	Those elements of cyberspace that enable mission essential activities, operations or functions. It comprises any area (physical, logical, and social) whose seizure, retention or disruption affords a marked advantage to either combatant.
Mission	An activity assigned to an individual, unit or force by an authority who has full command, operational command or operational control. Note: Mission differs from Operation in that an Operational Commander may have forces in support, in location or otherwise involved in the Operation that they do not command or control
Operation	A combination of activities with a common purpose or unifying theme. (e.g. Op Medusa) Note: Mission differs from Operation in that an Operational Commander may have forces in support, in location or otherwise involved in the Operation that they do not command or control.
Situational Awareness (SA)	Situational Awareness is defined as the "knowledge of the elements in the operational environment necessary to make well-informed decisions." For the Net C2 ISAC project, the knowledge of interest and importance relates to

	the Information Technology Infrastructure of the cyber environment and how it affects DND/CAF operations.
Task	An activity that contributes to the achievement of a mission. (e.g. Canadian Army will generate an Infantry Heavy Battle Group for Operation XYZ)

Annex B – Draft Net C2 ISAC Procurement Process

1. OVERVIEW

(a) The latest draft of the Network Command and Control Integrated Situational Awareness Capability (Net C2 ISAC) procurement process is described in this Annex. It will remain a draft until the final RFP is issued to the Invitation to Qualify (ITQ) Responsive Suppliers. The Net C2 ISAC procurement approach will use a multi-phase process, as shown below. This approach will allow Canada to conduct due diligence of Net C2 ISAC requirements with ITQ Responsive Suppliers before issuing the bid solicitation. Since the post Qualification Phases of the Net C2 ISAC procurement may be very labour-intensive and time-consuming for both Respondents and Canada, Public Works and Services Canada (PWGSC) will only be conducting this phase with the ITQ Responsive Suppliers as determined in the Qualification Phase. PWGSC's intention, in conducting the Due Diligence Phase prior to issuing the final bid solicitation, is to ensure that the ITQ Responsive Suppliers have an opportunity for a detailed review of the draft Net C2 ISAC solicitation prior to Canada's distribution of the final Request for Proposal (RFP).

Steps in the Procurement Process	Phase	Components
1. Issue ITQ	Qualification Phase	• Mandatory Requirements (Pass/Fail) • Select ITQ Responsive Suppliers
2. Distribute Draft RFP to ITQ Responsive Suppliers	Due Diligence	• ITQ Responsive Supplier review of Draft RFP and Security Profile Protection Table • ITQ Responsive Supplier recommendations and questions based on review of Draft RFP • Finalize RFP
3. Issue Final RFP to ITQ Responsive Suppliers	Bidding Phase	• Mandatory Requirements (Pass/Fail) • Rated Requirements (Score) • Proof of Proposal Demonstration (Score) • Financial (Score) • Select Winning Bidder
4. Issue Contract to Winning Bidder	Contract Award Phase	• Award Contract

(b) Once the ITQ Responsive Suppliers have been selected and have been notified that they have qualified for the next phase of the procurement process, Canada intends to proceed with the Due Diligence Phase and will invite ITQ Responsive Suppliers to a Classified Industry Day to be briefed by PWGSC, the Department of National Defence (DND) and Innovation, Science and Economic Development Canada (ISED), and to receive the draft RFP (including Classified Annex F). Attendees must be cleared and equipped to accept any Classified documents and to carry them to, and safeguard them at, their facilities. Only ITQ Responsive Suppliers who have the required security clearance will be invited to the Classified Industry Day.

(c) ITQ Responsive Suppliers qualified at the ITQ step may withdraw from the process by providing written notification to the Contracting Authority.

(d) At any point, Canada may, at its sole discretion (but with no obligation to do so) choose to extend the time period for any post Qualification phase of this procurement.

2. DUE DILIGENCE

(a) It is the responsibility of each of ITQ Responsive Supplier to take advantage of the Due Diligence process by asking any questions that are necessary for it to prepare a complete response to the final bid solicitation.

(b) The objectives of the Due Diligence Phase include:

(i) Ensuring that the ITQ Responsive Suppliers have an opportunity to conduct a thorough review of the draft Net C2 ISAC RFP;

(ii) Obtaining recommendations for improvements to the draft Net C2 ISAC RFP which are advantageous for Canada; and

(iii) Modifying the draft Net C2 ISAC RFP to incorporate changes approved by Canada.

(c) The approach for the Due Diligence Phase is as follows:

(i) During the Due Diligence Phase, ITQ Responsive Suppliers will have 20 working days to submit questions on the draft Net C2 ISAC RFP. Canada will respond to the questions and provide copies of the responses to each ITQ Responsive Supplier. All questions and answers will be provided to all ITQ Responsive Suppliers.

(ii) Questions 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 ITQ Responsive Suppliers do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all ITQ Responsive Suppliers. Questions not submitted in a form that can be distributed to all ITQ Responsive Suppliers may not be answered by Canada.

3. BIDDING PHASE

(a) The objectives of the Bidding Phase include:

(i) Issuing the Final Net C2 ISAC RFP to the ITQ Responsive Suppliers (now referred to as Bidders);

(ii) Obtaining the bids from the Bidders;

(iii) Evaluating the bids; and

(iv) Selecting the successful Bidder.

(b) The approach for the Bidding Phase may be as follows:

(i) The RFP will include both mandatory and rated requirements. The rated requirements evaluation will include the rated requirements provided in the RFP and, if applicable, the details of a scripted Proof of Proposal (PoP) test (the decision to include a PoP test will be made prior to the release of the draft RFP).

(ii) The PoP test would be conducted at no cost to Canada, at a location in Canada proposed by the Bidder and agreed to by Canada. Canada will confirm the location of the PoP test at least 30 days in advance. Each responsive Bidder would perform the PoP test in accordance with a timeframe, schedule, and agenda defined by the Government of Canada (GOC). Bidders will be notified of the date, and time of their PoP test no later than 15 working days prior to the PoP test. The responsive Bidders will be responsible for ensuring that the location is equipped with all the equipment necessary to conduct the PoP.

(iii) The PoP test content will be based on the proposed Net C2 ISAC functionality testing and conformance to the proposed Technology Blueprint submitted in response to the RFP.

(iv) It is at the Bidder's discretion to determine the appropriate team members to participate in the PoP. It is recommended that the team members include:

(A) Program Executive: The Bidder’s senior executive with ongoing accountability and responsibility for the Net C2 ISAC program and the individual who represents the Supplier’s Chief Executive Officer in all matters;

(B) Program Manager: The Bidder’s senior manager with on-going operational responsibility for delivery of the Net C2 ISAC services; and

(C) Technical Architect: A senior technical representative who has responsibility for technical architecture and design of Net C2 ISAC services.

(v) On the day of the PoP each Bidder must provide (quantities to be determined):

(A) softcopy and hardcopy of the presentation;

(B) softcopy and hardcopy of documentation that is required to support the Bidder's presentation; and

(C) Client references that the Bidder is using to support the presentation, if applicable.

(vi) The Phased Bid Compliance Process (PBCP) will be applied to the RFP for this procurement. For more information on the PBCP, please visit the following link:

https://buyandsell.gc.ca/policy-and-guidelines/policy-notifications/PN-123

4. CONTRACTOR SELECTION

(a) The details of the Contractor Selection process will be provided in the Net C2 ISAC RFP.

(b) Canada has not yet finalized the Contractor Selection methodology for the final RFP but it is anticipated that the bids received from Qualified Suppliers in response to the final RFP will be evaluated on the basis of:

- Compliance with mandatory requirements / security profile protection table;
- Rated technical experience, with a minimum pass mark;
- Rated PoP demonstration (testing of solution performance, usability and conformance to technical bid); and
- Rated financial proposal.
- Rated Industrial and Technological Benefits (ITB) / Value Proposition proposal (see Annex D for more details).

After complying with mandatory requirements, the Technical Proposal, PoP demonstration (if applicable), Financial Proposal and ITB / Value Proposition proposal will each be scored separately.

ANNEX C: ABBREVIATIONS AND ACRONYMS

The table below provides all the abbreviations and acronyms found in this ITQ document.

Table 1 – Abbreviations and Acronyms

Abbreviation/ Acronym	Description
CAF	Canadian Armed Forces
CANSOFCOM	Canadian Special Operations Forces Command
CJOC	Canadian Joint Operations Command
CSNI	Consolidated Secret Network Infrastructure
DEFSOC	Defence Service Operations Centre
DND	Department of National Defence
DNS	Domain Name Service
DWAN	Defence Wide Area Network
EA	Expenditure Authority
FM	Fairness Monitor
FPS	Former Public Servants
HC	High Complexity
IP	Internet Protocol
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITB	Industrial and Technological Benefits
ITI	Information Technology Infrastructure
ITQ	Invitation to Qualify
JBMC	Joint Battleship Management Capability
Net C2 ISAC	Network Command and Control Integrated Situational Awareness Capability

Net SA	Network Situational Awareness
NDA	Non-Disclosure Agreement
OA	Operational Authority
OSC&S	Operational and Strategic Commanders and their Staff
PSSA	Public Service Superannuation Act
PWGSC	Public Works and Government Services Canada
R&D	Research and Development
RFI	Request for Information
RFP	Request for Proposal
SACC	Standard Acquisition Clauses and Conditions
SA	Situational Awareness
SJS	Strategic Joint Staff
SMB	Small and Medium-sized Businesses

Application of the Industrial and Technological Benefits (ITB) Policy

The Industrial and Technological Benefits (ITB) Policy may be applied on the **Network Command and Control Integrated Situational Awareness Capability (Net C2 ISAC)** project. Engagement with industry through the Request for Information (RFI) will help determine the application of the ITB Policy and how Canada could leverage opportunities for economic benefit through this procurement.

The ITB Policy, including Value Proposition

The ITB Policy is a powerful investment attraction tool and companies awarded defence procurement contracts are required to undertake business activities in Canada equal to the value of the contract. The ITB Policy encourages companies to establish or grow their presence in Canada, strengthen Canadian supply chains, and develop Canada's industrial capabilities.

The goal of the ITB Policy is to support the long-term sustainability and growth of Canada's defence sector, enhance the competitiveness and growth of Canadian-based suppliers, including small and medium-sized businesses, support skills development and training, enhance innovation through research and development (R&D) in Canada, and increase the export potential of Canadian-based firms. The ITB Policy includes the Value Proposition, which requires bidders to compete on the basis of the economic benefits to Canada associated with its bid. Winning bidders are selected on the basis of price, technical merit and their Value Proposition. Value Proposition commitments made by the winning bidder become contractual obligations in the ensuing contract.

For details regarding the ITB Policy, visit www.canada.ca/itb

Key Industrial Capabilities:

To maximize the economic impact that can be leveraged through the Value Proposition, Canada may use the ITB Policy to motivate defence contractors to invest in **Key Industrial Capabilities (KICs)**. KICs align with Canada's defence policy, *Strong, Secure, Engaged* and the *Innovation and Skills Plan* by supporting the development of skills and fostering innovation in Canada. KICs represent technological areas of emerging growth, established capabilities where Canada is globally competitive, as well as areas where domestic capacity is essential to national security.

The Government has identified this procurement as requiring capability in the areas of both **Cyber Resilience** and **Artificial Intelligence**. As emerging technologies, these KICs are areas with the potential for rapid growth and innovation. As a result, Canada will be seeking to foster opportunities in these emerging technologies by motivating partnerships and investments with industry and post-secondary institutions that promote skills development and research and development.

The definitions for KICs relevant to this project are:

Cyber Resilience

Cyber resilience spans every element of the domestic commercial, civil and national security sectors and addresses the vulnerabilities created by the expansion of information technology and the knowledge economy. Activities in this segment include design, integration and implementation of solutions that secure information and communications networks. These and other technologies should focus on achieving effective development of the following cyber capabilities:

Information security

The practice of defending electronic and digital data and information from unauthorized access/intrusion, use, disclosure, disruption, modification, perusal, inspection, recording or destruction;

IT security

Secure content and threat management (endpoint, messaging, network, web, cloud), security, vulnerability and risk management, identity and access management and other products (e.g. encryption/tokenization toolkits and security product verification testing), and education, training services and situational awareness;

Operational technology (OT) security

Monitoring, measuring and protecting industrial automation, industrial process control and related systems. Cyber resilience may involve the development of tools and the integration of systems and processes that permit hardening of tactical systems or broader networks, encryption, cyber forensics, incident response, and others. Capabilities developed in this domain may increasingly draw on AI as an enabling technology; for example, networks may autonomously and dynamically defend against intrusions and repair themselves if disrupted.

Artificial Intelligence

Artificial Intelligence (AI) spans a range of technologies that allow machines to execute tasks that normally require human intelligence, such as pattern and speech recognition, translation, visual perception, and decision-making. AI develops or draws on disciplines such as search and mathematical optimization, machine learning, deep learning, self-learning, and neural networks. AI can reduce operator workload and automate easily repeatable tasks that otherwise require significant human involvement. AI promises enhanced efficiency in the use of trained personnel, less exposure of humans to dangerous environments, and more rapid responses to changes in the military operating environment. It can also permit the analysis of large volumes of data in support of intelligence analysis, mission planning and rehearsal, logistics and business management, cyber security and resilience, and many other activities. AI is relevant across a broad set of both defence and non-defence domains.

ITB/Value Proposition Industry Engagement Questions

Defence Sector

The ITB Policy seeks to promote economic development and long-term sustainment of Canadian businesses engaged in the manufacturing and delivery of products and services for use in government defence and security applications.

1. Based on the technical specifications put forward by the Department of National Defence, describe what Direct Work activities, in the KICs identified above, your company would foresee undertaking in Canada for the design, production and maintenance of the Net C2 ISAC solution?

Supplier Development, including Small and Medium-sized Businesses

The ITB Policy seeks to improve the competitiveness of Canadian industry by encouraging Canadian industrial participation and the scaling up of Canadian Companies including small and medium-sized businesses (SMB).

2. The ITB Policy requires that at least 15 percent of the contractor's ITB obligation (equal to the value of the contract) be represented by work with Canadian SMB with less than 250 employees. To what extent can you commit to a SMB requirement of over 15 percent in order to nurture the development of Canadian SMB within the cybersecurity sector (includes both direct work on this procurement and work in other business areas)?

3. Apart from this procurement, in what other areas of production and service-provision do you see opportunities to assist SMBs that have capabilities within the KICs identified above, to scale up, in order to respond to domestic and global demand?

Skills Development and Training

The ITB Policy fosters the development and sustainment of a diverse, talented, and innovative Canadian workforce through access to training, education opportunities and programs.

4. What types of skills development and training investments would produce maximum benefit to Canada, in either the defence or commercial sectors?
    a. Examples:
        i. Work integrated learning programs (e.g., co-operative education; work placements);
        ii. Apprenticeship programs;
        iii. A new or existing skills development program at or through a post-secondary institution (e.g.: coding and programming, network engineering, and software development and integration);
        iv. Support for security certifications (e.g.: Top Secret, ITAR) or cybersecurity compliance certifications for Canadian Companies, especially small and medium-sized businesses;

Research and Development (R&D)

The ITB Policy promotes scientific investigation that explores the development of new goods and services, new inputs into production, new methods of producing goods and services, or new ways of operating and managing organizations.

5. Are there opportunities to partner with Canadian post-secondary or publicly-funded research institutions to perform Direct Work on the Net C2 ISAC project?

6. Is there potential to develop research consortia or centres of excellence in partnership with Canadian post-secondary or publicly-funded research institutions in the KICS identified above? If so, what research areas might your organization pursue?

    a. If not, what other research or development partnerships could be formed to support technological development in the KICs identified above?

7. Is there potential to invest in R&D partnerships with Canadian cyber sector SMBs and start-up companies, including funding for late-stage R&D and commercialization of innovative products or services?

8. What should the minimum R&D requirement be (as a percentage of anticipated bid price) in order to motivate bidders to invest in high-value innovation within Canada's KICs?

Export:

The ITB Policy promotes the ability of Canadian companies, including SMBs, to successfully tap into export markets, thereby increasing their productivity, and competitiveness in the global market.

9. Please describe any export opportunities from Canada directly related to this procurement.

10. Is it feasible to secure sufficient intellectual property rights and an exclusive global product mandate to export from your Canadian-based operations, including subsidiaries and supply chain partners?

11. Please describe any other high value export opportunities from Canada related to the KICs identified above, whether commercial or defence, that can be leveraged as a result of this procurement.

Other Questions:

12. Are there other relevant KICs which align with the work to be conducted for the Net C2 ISAC project? If yes, please indicate which KICs should be considered and why. As part of your response, please describe how the proposed KICs would enhance the opportunities that could be leveraged through the Value Proposition for Canadian industry.

13. In comparison to price and technical merit, Value Proposition typically has a weight of no less than 10% of the overall bid evaluation. What is your view on the weighting of the Value Proposition for the Net C2 ISAC project?

14. Within the Value Proposition, what are your recommended minimum percentages of weighting for each of the Value Proposition pillars (Defence Sector, Supplier Development, Skills and Training, R&D, Exports, and other—if applicable)?

Please provide your written feedback to these questions and any other comments regarding Industrial and Technological Benefits/Value Proposition or KICs to the PWGSC Contracting Authority as part of your RFI/ITQ Response package.

ANNEX E: SECURITY REQUIREMENTS CHECK LISTS (SRCLs)

The purpose of this Annex is to present the following SRCLs:

Appendix 1 to Annex E: SRCL for ITQ

Appendix 2 to Annex E: SRCL for RFP and Resulting Contract

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8474-18-NT10 AMD3
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: Department of National Defence

2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD

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

This SRCL is for the Due Diligence phase of the procurement process for the Network Command and Control Integrated Situational Awareness Capability (NET C2 ISAC) Prime Integrator project

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: ☐

5. 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 : CAN/US	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	PROTECTED 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)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8474-18-NT10 AMD3
Security Classification / Classification de sécurité
UNCLASSIFIED

PART A (continued) / PARTIE A (suite)

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8474-18-NT10 AMD3
Security Classification / Classification de sécurité
UNCLASSIFIED

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
W8474-18-NT10 AMD3

Security Classification / Classification de sécurité
UNCLASSIFIED

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
LLoyd Gregan	Project Manager, NET C2 ISAC	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-995-4952		llyod.gregan@forces.gc.ca	

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Sasa Medjovic DDSO	Industrial Security Senior Security Analyst	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
Tel: 613-996-0286		E-mail: sasa.medjovic@forces.gc.ca	2018-Aug 30

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? / Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? — No / Non — Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Denis Lecompte	Contract Security Officer	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
			May 14/2018

DEC 20 2017

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8474-18-NT10-
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: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD
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
Network Command and Control Integrated Situational Awareness Capability (Net C2 ISAC) Project.

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 : CAN/US	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information					
PROTECTED A / PROTÉGÉ A	☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ	☐	PROTECTED 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)	☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8474-18-NT10
Security Classification / Classification de sécurité
UNCLASSIFIED

PART A (continued) / PARTIE A (suite)

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

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?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W8474-18-NT10-
Security Classification / Classification de sécurité
UNCLASSIFIED

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 / TRÉS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRES SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens					✓										✓	
Production																
IT Media / Support TI					✓											
IT Link / Lien électronique					✓											

SM

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
W8474-18-NT10
Security Classification / Classification de sécurité
UNCLASSIFIED

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Lloyd Gregan	Project Manager, Net C2 ISAC	L. Gregan	
Telephone No. - N° de téléphone: 613-995-4952	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel: Lloyd.Gregan@forces.gc.ca	Date

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Sasa Medjovic - DDSO - Industrial Security Senior Security Analyst Tel: 613-996-0286 E-mail: sasa.medjovic@forces.gc.ca			
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date: 2017-Dec 20

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☐ No / Non ☒ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Denis Lecompte	Contract Security officer	D Lecompte	
Telephone No. - N° de téléphone: 613 952 7907	Facsimile No. - N° de télécopieur: 613 948 1712	E-mail address - Adresse courriel	Date: Jan 8/2018

ANNEX F: Current Concept of Operations and In-Services Capabilities – CLASSIFIED

Annex F is classified: Suppliers who wish to review or obtain a copy of Annex F must pass the ITQ phase.

A hard copy only of the document will be provided in person to suppliers who pass the ITQ phase at a date to be determined.

Annex F is also considered controlled goods: As Annex F will require the production of or access to controlled goods that are subject to the *Defence Production Act, R.S. 1985, c. D-1*, suppliers are advised that within Canada only persons who are registered, exempt or excluded under the Controlled Goods Program (CGP) are lawfully entitled to examine, possess or transfer controlled goods (Annex F). Details on how to register under the CGP are available at: http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html

Attachment 1 to ITQ Part 5 – Mandatory Evaluation Criteria

Respondents must meet all of the mandatory requirements in this attachment. In accordance with Part 5 - Evaluation Procedures and Basis of Qualification of the ITQ, Canada may contact the client contact for the referenced project(s) to validate Respondents' responses.

1.1 Substantiation of Technical Compliance – Mandatory Evaluation Criteria

1.1.1 Respondents must respond to the corresponding mandatory requirements (Table 1) by providing a description explaining, demonstrating, substantiating and justifying their Qualifications. Respondents are requested to utilize the unique number and associated title of each mandatory requirement in their responses. Respondents are requested to indicate where their mandatory requirement is met by entering the location (e.g. volume/binder number, page number, etc.) in the "Cross Reference to Response" column. Respondent's responses to the mandatory requirements will be evaluated as either "Met" or "Not Met". A "Not Met" will result in the response being deemed non-responsive.

1.1.2 Respondents are requested to submit "Form 2 – Project Reference Check Form", for each project claimed in response to corresponding mandatory requirement(s).

1.1.3 Respondents should only provide the required reference project(s) as indicated in each mandatory requirement. If more than the required number of reference project(s) is provided, the Respondents will be required to clarify which reference project(s) apply to corresponding mandatory requirement(s).

1.1.4 Each reference project(s) must include, at minimum, the name of the project, the client name(s) and contact information, the project value in Canadian dollars, the team member names.

1.1.5 Please refer to Annex C – "Abbreviations and Acronyms" to assist with responding to the mandatory requirements.

Table 1 Mandatory Requirements

Req #	Mandatory Requirement	Cross Reference to Response
M1	The Respondent must have previous experience successfully implementing classified (Secret or above) projects for the Government of Canada within the past five (5) years. Respondents must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team have successfully implemented a classified project for the Government of Canada within the past five (5) years; and Where the Reference Project provided to demonstrate compliance with criterion M1 is that of a member of the Respondent's Core Team, in addition to the requirements above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M2	The Respondent must have previous experience developing, integrating, delivering and providing stabilization support* for Information Technology (IT) systems similar in size to the Consolidated Secret Network Infrastructure (CSNI) network (8000+ users). * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the IT capability to, at a minimum, when the IT capability was fully implemented. Respondents must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team have developed, integrated, delivered and provided stabilization support* for Information Technology (IT) systems similar in size to the Consolidated Secret Network Infrastructure (CSNI) network (8000+ users). Where the Reference Project provided to demonstrate compliance with criterion M2 is that of a member of the Respondent's Core Team, in addition to the requirements above, the Respondent must provide evidence of a contractual relationship between the Supplier and the Core Team member covering the period of any potential Contract resulting from this procurement process.	
M3	The Respondent must have previous experience developing, integrating, delivering and providing stabilization support* for high reliability Command and Control (C2) systems. * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the IT capability to, at a minimum, when the IT capability was fully implemented. Respondents must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent 's Core Team have developed, integrated, delivered and provided stabilization support* for high reliability Command and Control (C2) systems. Where the Reference Project provided to demonstrate compliance with criterion M3 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M4	The Respondent must have provided 3rd line technical support in English and in French for a period of at least 12 contiguous months in the last 5 years where technical support met or exceeded each of the following: a) operated 5 days per week; b) 8 hours per day; and, c) 52 weeks per year Respondents must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team provided 3rd line technical support in English and in French for a period of at least 12 contiguous months in the last 5 years where technical support met or exceeded the parameters detailed above. Where the Reference Project provided to demonstrate compliance with criterion M4 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M5	Respondents must have previous experience developing, integrating, delivering and providing stabilization support* for solutions utilizing the following: a) Modern Security Incident Event Management (SIEM) systems; and, b) Situational Awareness (SA) or IT Health Monitoring system in which both (a) and (b) systems have over ten (10) separate operating nodes each. * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the SIEM and SA or IT Health Monitoring systems to, at a minimum, when these systems were fully implemented. Respondents must demonstrate compliance with this requirement by: (a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team developed, integrated, delivered and provided stabilization support* for solutions utilizing the systems detailed above. Where the Reference Project provided to demonstrate compliance with criterion M5 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M6	Respondents must have previous experience developing, integrating, delivering and providing stabilization support* for a geographically dispersed SA or IT Health Monitoring system with a minimum of ten separate operating nodes, interconnected with high speed (100 Mbps or above). * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the SA or IT Health Monitoring systems to, at a minimum, when these systems were fully implemented. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team developed, integrated, delivered and provided stabilization support* for the systems detailed above. Where the Reference Project provided to demonstrate compliance with criterion M6 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M7	Respondents must have previous experience developing, integrating, delivering and providing stabilization support* for a geographically dispersed SA or IT Health Monitoring system with a minimum of five separate operating nodes, interconnected at disadvantaged speed (less than 1.544 Mbps links) remoted in austere environments to a High speed (100Mbps or above) central network. * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the SA or IT Health Monitoring systems to, at a minimum, when these systems were fully implemented. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team developed, integrated, delivered and provided stabilization support* for the systems detailed above. Where the Reference Project provided to demonstrate compliance with criterion M7 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M8	Respondents must have previous experience developing, integrating, delivering and providing stabilization support* for SA or IT Health Monitoring system that integrate data feeds from multiple sources, including, but not limited to Windows Event logs, Syslog data, Common Event Format (CEF) data, Packet Capture (PCAP) data, Simple Network Management Protocol (SNMP) events and Netflow data. * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the SA or IT Health Monitoring systems to, at a minimum, when these systems were fully implemented. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team developed, integrated, delivered and provided long term support* for the systems detailed above. Where the Reference Project provided to demonstrate compliance with criterion M8 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M9	Respondents must have previous experience developing, integrating, delivering and providing stabilization support* for SA or IT Health Monitoring systems that feature Graphical User Interfaces (GUI) and relational databases at the Regional and National Service Management Centers (SMC). * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the SA or IT Health Monitoring systems to, at a minimum, when these systems were fully implemented. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team developed, integrated, delivered and provided long term support* for the systems detailed above. Where the Reference Project provided to demonstrate compliance with criterion M9 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	
M10	Respondents must have previous experience developing, integrating, delivering and providing stabilization support* for systems that incorporate at least five Commercial-off-the-shelf (COTS) or Government-off-the-shelf (GOTS) products. * stabilization support is defined as continuous support for at least six (6) months duration from when the client group(s) began using the IT system to, at a minimum, when these systems were fully implemented. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team developed, integrated, delivered and provided long term support* for the systems detailed above. Where the Reference Project provided to demonstrate compliance with criterion M10 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M11	Respondents must have previous experience developing, integrating, delivering and providing stabilization support* for systems incorporating multi-level security environments and a cross domain gateway between them. * stabilization support is defined as support for at least six (6) months duration from when the client group(s) began using the IT system to, at a minimum, when these systems were fully implemented. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Respondent's Core Team developed, integrated, delivered and provided long term support* for the systems detailed above. Where the Reference Project provided to demonstrate compliance with criterion M11 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	
M12	Respondents must have previous experience developing and delivering IT training solutions for operators of IT equipment (hardware & software). This must include the development of operational and support scenarios which can be created, modified, maintained, and executed by the IT Service Agents using existing workstations and systems within an exercise/training environment. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team developed and delivered the training solutions described above. b) Providing a detailed description of the training developed and delivered. Where the Reference Project provided to demonstrate compliance with criterion M12 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

M13	Respondents must have previous experience performing analysis of IT Configuration Management (CM) processes and developing and implementing Configuration Management solutions based on the findings for a Customer in the IT Industry. Respondents must demonstrate compliance with this requirement by: a) Providing a minimum of one Reference Project in the last five (5) years for which they or a member of the Supplier's Core Team performed the CM process analysis and developed and delivered the CM solutions described above. b) Providing a detailed description of what work was performed along with any new CM processes that were implemented. Where the Reference Project provided to demonstrate compliance with criterion M13 is that of a member of the Respondent's Core Team, in addition to the requirement above, the Respondent must provide evidence of a contractual relationship between the Respondent and the Core Team member covering the period of any potential Contract resulting from this procurement process.	

FORM 1: ITQ SUBMISSION FORM

Supplier's (Core Team Member 1) full legal name	
(a)	
Supplier's Procurement Business Number	
(b)	
Authorized Representative of Supplier for evaluation purposes (e.g. clarifications)	
(c)	Name:
	Title:
	Address:
	Telephone #:
	Email:
If submitting a response to the ITQ as a joint venture, the Supplier must provide the joint venture member's full legal name and address [Supplier to add more rows if more than two (2) joint venture members]	
(d)	Joint venture member full legal name:
	Joint venture member address:
(e)	Joint venture member full legal name:
	Joint venture member address:
Canada's Official Language in which the Supplier will communicate with Canada during the procurement process – indicate either English or French	
English ☐	French ☐

Core Team Members

Core Team Member 2 full legal name:
Address:

Core Team Member 3 full legal name:
Address:

Core Team Member 4 full legal name:
Address:
ITQ Submission Requirements
It is the Suppliers sole responsibility to ensure their response addresses all requirements outlined in the ITQ.
Supplier Authorization
Name:
Address:
Email:
Signature of authorized representative of Supplier
Telephone #:
Date:
If submitting a response to the ITQ as a joint venture, the Supplier must complete section (f) below.
[Supplier to add more rows if more than two (2) joint venture members]
(f) Name:
Address:
Email:
Signature of authorized representative of Supplier
Telephone #:
Date:

FORM 2: PROJECT REFERENCE CHECK FORM

Instructions to Suppliers:

(a) Suppliers are requested to submit a Project Reference Check Form for each project referenced in response to each mandatory requirement in Attachment 1 to Part 5 of the ITQ.

(b) If the information requested in this form is not provided with the Suppliers' ITQ response it must be provided upon request by the Contracting Authority within the timeframe identified in the request.

(c) Canada may contact the client contact, provided for the referenced project, to validate the information provided.

#	Response		
(a)	Mandatory Requirement Number (from Attachment 1 to Part 5)		
(b)	Supplier Full Legal Name (if the Supplier is a joint venture, the full legal name of the joint venture member for the referenced project)		
(c)	Description and project value in Canadian dollars of the referenced project		
(d)	Name of client organization for the referenced project		
(e)	Name of client contact for the referenced project		
(f)	Client organization and client contact affiliation with the Supplier (or joint venture member)		
	Please indicate accordingly	Are Not Affiliated	Are Affiliated
(g)	Name of organization the client contact is currently working for (if the client contact is no longer working for the client organization identified for the referenced project)		
(h)	Title of client contact (while working on the referenced project)		
(i)	Current telephone number of client contact		
(j)	Current e-mail address of the client contact		
(k)	Role of the client contact in the referenced project		

Form 3 - NDA

CORPORATE

NON-DISCLOSURE AGREEMENT FOR PARTICIPATION IN SOLICITATION PROCESS

PWGSC FILE # W8474-18NT10/A – RFI/ITQ Phase

The above noted solicitation process (the "**Solicitation Process**"), including the Request for Information ("**RFI**") component, may require the disclosure of Information and Controlled Information (each as defined below) by or on behalf of Canada to Recipient. In consideration of Canada providing such disclosures, Recipient acknowledges and agrees that:

1. Information

(a) During the Solicitation Process, Canada may disclose certain information to Recipient: (i) that is not Controlled Information (as defined below); or (ii) that is information that is not otherwise made publicly available by Canada without obligations of confidentiality or non-disclosure (collectively, the "**Information**").

(b) Canada is disclosing the Information to Recipient for the sole and exclusive purpose of enabling Recipient to participate in the Solicitation Process, and, should Recipient determine it wishes to do so, to prepare and submit an offer to Canada, should Canada seek such offers (the "**Purpose**").

(c) Recipient shall keep confidential the Information provided to Recipient by or on behalf of Canada in connection with the Solicitation Process.

(d) Any disclosure of the Information shall be on a "need to know" basis solely to Recipient's employees or to its legal or financial advisors, provided they have executed, in advance, the Individual Non-Disclosure Agreement at Attachment 1 to Form 3. Recipient shall not disclose any Information to any other person including to its contractors or subcontractors without Canada's prior written consent nor shall Recipient make or permit any public disclosure or release whatsoever of the Purpose or the Information, in whole or in part. Recipient shall not alter, remove or obstruct any confidentiality or other notices provided on or in the Information, and shall reproduce, in full, all such notices and markings in or on any copies, extracts or other documentation which may contain any Information.

(e) Recipient may disclose Information where required to do so by law or order of a court of competent jurisdiction, but only to the extent necessary to comply with such law or order and provided that Recipient has first provided advance written notice to Canada so that Canada, at its sole discretion, may obtain any protective order or its equivalent. Recipient shall notify the relevant person or entity to whom the Information is to be disclosed of the confidential nature of such information and request confidential treatment. Without prejudice to the foregoing, Recipient shall comply with all reasonable requests of Canada relating to such disclosure.

(f) Unless otherwise permitted under paragraph (g), Recipient shall, on the earlier of Canada's written request or the completion or termination of the Purpose or any solicitation process with respect thereto, return or destroy (as Canada may direct) all of the Information disclosed by or on behalf of Canada in its possession or under its control, and procure the return or destruction (as Canada may direct) of any such Information in the possession or under the control of any person to whom such Information may have been disclosed, save that Recipient's legal advisors may each retain one copy of the Information to the extent required to satisfy their professional duties or requirements. For the purposes of this paragraph, "destruction" shall include expunging any Information held on computer or other electronic systems.

(g) Should Recipient be awarded a contract as a result of the Solicitation Process, Recipient is entitled to retain the Information, subject to its continued compliance with this Agreement and those provisions of the awarded contract with respect thereto.

2. **Controlled Information**

(a) Controlled Information means: (i) any information or materials that are a controlled good as defined in the *Schedule (Controlled Goods List)* of the *Defence Production Act*; or (ii) any information that is subject to Canada's Industrial or Contract Security Program, including PROTECTED/CLASSIFIED information or materials; or (iii) information or materials that are both a controlled good as defined in the *Defence Production Act* and subject to Canada's Industrial or Contract Security Program.

(b) Recipient acknowledges and agrees that any and all use of Controlled Information, including without limitation, all access, copying, distribution, disclosure, transmission, retransmission, export, re-export, transfer, re-transfer, storage and destruction (or prohibitions on destruction) of Controlled Information, shall be on a "need to know" basis solely and exclusively for the Purpose and shall be subject to and in compliance with, as applicable: (i) the *Controlled Goods Regulations* and the requirements of the Controlled Goods Program (including registration, compliance, or exemption); and (ii) Canada's Industrial or Contract Security Program including any Security Agreement or other requirements of such Program(s), including those Security Requirements as set forth in Annex E (as applicable) to this Agreement. Nothing contained in this Agreement limits or otherwise derogates from Recipient's obligations under either of the foregoing Programs.

(c) Recipient acknowledges that (i) Canada may disclose Controlled Information during the Solicitation Process to Recipient, to the extent Recipient is authorized to receive such Controlled Information; and (ii) Recipient may not be authorized to receive all Controlled Information otherwise made available by Canada during the Solicitation Process. Recipient remains solely responsible for maintaining all requisite authorizations and permissions at all times.

(d) Without limiting the foregoing, Recipient shall return or destroy (at Canada's sole and exclusive direction) any Controlled Information. Recipient acknowledges that such direction may be provided by Canada in its sole and exclusive discretion, whether or not the Solicitation Process has been completed or terminated or Recipient has completed the Purpose.

3. General

(a) Recipient is liable for any damages, costs, losses and expenses arising from a breach of this Agreement by Recipient, its employees, representatives and/or any other party to whom Recipient discloses the Information or Controlled Information. The provisions of this Agreement shall survive termination of this Agreement and/or any return or destruction of Information or Controlled Information, and/or termination or completion of the Purpose or the Solicitation Process. This Agreement and any dispute or claim arising out of or in connection with it shall be governed by and construed in accordance with the laws of the Province of Ontario.

Recipient Name: _____

[Insert full corporate (legal) name]

I have authority to bind Recipient

Per: _____

Name (print): _____

Date: _____

Recipient Security Officer

Per: _____

Name (print): _____

Date: _____

Attachment 1 to Form 3

INDIVIDUAL

NON-DISCLOSURE AGREEMENT FOR PARTICIPATION IN SOLICITATION PROCESS

PWGSC FILE # W8474-18NT10/A – RFI/ITQ Phase

The above noted solicitation process (the "**Solicitation Process**"), including the Request for Information ("**RFI**") component, may require the disclosure of Information and Controlled Information (each as defined below) to Recipient by or on behalf of Canada or by Recipient's employer as identified below (the "**Company**"). Recipient acknowledges and agrees that:

1. Information

(a) During the Solicitation Process certain information may be disclosed to Recipient by the Company or by or on behalf of Canada: (i) that is not Controlled Information (as defined below); or (ii) that is information that is not otherwise made publicly available by Canada without obligations of confidentiality or non-disclosure (collectively, the "**Information**").

(b) Disclosure of Information to Recipient is for the sole and exclusive purpose of enabling Recipient, on behalf of and under the direction of Company, to participate in the Solicitation Process (the "**Purpose**").

(c) Recipient shall keep confidential all Information provided to Recipient. Any disclosure of the Information shall be on a "need to know" basis solely to Company's employees who have been identified by Company as being authorized to receive such Information. Recipient shall not disclose any Information to any other person including to Company's contractors or subcontractors without Company's prior written direction nor shall Recipient make or permit any public disclosure or release whatsoever of the Purpose or the Information, in whole or in part. Recipient shall not alter, remove or obstruct any confidentiality or other notices provided on or in the Information, and shall reproduce, in full, all such notices and markings in any copies, extracts or other documentation which may contain any Information.

(d) Recipient may disclose Information where Company has confirmed that Company is required to do so by law or order of a court of competent jurisdiction, but only to the extent necessary to comply with such law or order and provided that, without prejudice to the foregoing, Recipient has complied with any direction of Company with respect to such disclosure.

(e) Recipient shall, immediately, upon direction from Company, return or destroy all of the Information in Recipient's possession or under Recipient's control. For the purposes of this paragraph, "destruction" shall include expunging any Information held on computer or other electronic systems.

2. Controlled Information

(a) Controlled Information means: (i) any information or materials that are a controlled good as defined in *Schedule (Controlled Goods List)* of the *Defence Production Act*, or (ii) any information that is subject to Canada's Industrial or Contract Security Program, including PROTECTED/CLASSIFIED information or materials; or (iii) information or materials that are both a controlled good as defined in the *Defence Production Act* and subject to Canada's Industrial or Contract Security Program.

(b) Any and all use of Controlled Information, including without limitation, all access, copying, distribution, disclosure, transmission, retransmission, export, re-export, transfer, re-transfer, storage and destruction (or prohibitions on destruction) of Controlled Information, shall be on a "need to know" basis solely and exclusively for the Purpose and shall be subject to and in compliance with, as applicable: (i) the *Controlled Goods Regulations* and the requirements of the Controlled Goods Program (including registration, compliance, or exemption); and (ii) Canada's Industrial or Contract Security Program including any Security Agreement or other requirements of such Program(s), including those Security Requirements as set forth in Annex E (as applicable) to this Agreement. Nothing contained in this Agreement limits or otherwise derogates from Recipient's obligations under either of the foregoing Programs.

(c) Without limiting the foregoing, Recipient shall immediately, at Company's direction, return or destroy any Controlled Information in Recipient's possession or under Recipient's control.

3. General

(a) Recipient shall immediately notify Company of any breach of this Agreement. The provisions of this Agreement shall survive termination of this Agreement and/or any return or destruction of Information or Controlled Information, and/or termination or completion of the Purpose or the Solicitation Process. This Agreement and any dispute or claim arising out of or in connection with it shall be governed by and construed in accordance with the laws of the Province of Ontario.

Company (print): _____	**Company Security Officer (print):** _____
Recipient: (print name): _____	Signature: _____
Signature: _____	Date: _____
Date: _____	