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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
See Above

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet Defensive Cyber Operations	
Solicitation No. - N° de l'invitation W6369-17DE25/B	**Date** 2017-12-18
Client Reference No. - N° de référence du client W6369-17DE25	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-049-26594
File No. - N° de dossier 049qe.W6369-17DE25	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-06-05**	**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: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (819) 420-1757 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** See Herein	

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

PART I - INTRODUCTION 2
Background 2
Purpose of this RFI 2
Proposed Engagement and Procurement Process 3
Procurement Timeline 3
PART II - REQUEST FOR INFORMATION 5
1. INSTRUCTIONS FOR RESPONDING TO THIS REQUEST FOR INFORMATION 5
1.1. Nature of the Request for Information 5
1.2. Response Costs 5
1.3. Treatment of Responses 5
1.4. National Security Exception 5
1.5. Nature and Format of Responses Requested 6
1.6. Contents of the RFI 6
1.7. Solicitation Caveat 6
1.8. Format of Responses 6
1.9. Enquiries 7
1.10. Language of Response 7
1.11. Submission of Responses 7
1.12. Fairness Monitor 8
2. OBJECTIVES OF THIS REQUEST FOR INFORMATION 8
2.1. Purpose 8
2.2. Provision of Classified Information (Annex C and Classified Questions and Answers) 8
2.3. Provision of License to Canada Owned Intellectual Property 9
3. SECURITY 9
3.1 Security Requirements of Procurement and Engagement Activities 9
3.2 Security Clearance Sponsorship for Phases 1-3 10
3.3 Security Clearance Sponsorship for Phase 4 11
4. INDUSTRIAL AND TECHNOLOGICAL BENEFITS (ITB) POLICY 11
5. OFFICIAL LANGUAGES 11
6. ENGAGEMENT APPROACH 11
7. INFORMATION REQUESTED BY CANADA 13
7.1. Documents of Interest 13
7.2 Guidance and Registration 14
7.3 Invitation to Respond 14
7.4 Information Requested 14
ANNEX A: PROJECT BACKGROUND 18
ANNEX B: PRELIMINARY STATEMENT OF OPERATIONAL REQUIREMENTS 19
ANNEX C: CURRENT CONCEPT OF OPERATIONS AND IN-SERVICE CAPABILITIES - CLASSIFIED 20
ANNEX D: PRODUCT OFFERINGS AND PRICING INFORMATION RESPONSE TEMPLATE 21
ANNEX E: SECURITY REQUIREMENTS 22
ANNEX F: APPLICATION OF THE INDUSTRIAL AND TECHNOLOGICAL BENEFITS (ITB) POLICY 26
ANNEX G: RULES OF ENGAGEMENT 29
ANNEX H: UNCLASSIFIED INDUSTRY DAY DETAILS AND REGISTRATION 31
ANNEX I: CLASSIFIED ONE-ON-ONE MEETING AND GROUP FOLLOW-UP MEETING DETAILS AND REGISTRATION 33
ANNEX J: REQUEST FOR SECURITY SPONSORSHIP 37

PART I - INTRODUCTION

Background

The Department of National Defence / Canadian Armed Forces (DND/CAF) has invested heavily in technologies that have radically increased the speed and precision of modern military operations. Underpinning most of these incredible leaps in capability has been a reliance on an increasingly complex cyberspace. To deliver on its core responsibilities to defend Canada, defend North America and contribute to international peace and security the DND/CAF must be an effective, agile, responsive, well-trained and well-equipped, modern military force with the core capabilities and flexibility required to successfully address both conventional and asymmetric threats, including cyber-attacks. Therefore, in support of its command and control structure, DND/CAF requires the capability to monitor and control its cyberspace so it remains defensible. To this end, two of the projects within the DND/CAF cyber force development program focus on addressing these requirements: Cyber Security Awareness (CSA) and Defensive Cyber Operations – Decision Support (DCO-DS):

a. The CSA project will transform how DND/CAF manages the confidentiality, integrity and availability of the increasingly complex DND/CAF cyberspace. This will be accomplished by focusing on identifying and securing its cyberspace, providing an end-to-end situational awareness that enables commanders to make informed decisions concerning the security posture of their cyberspace.

b. The DCO-DS project will improve DND/CAF's ability to conduct Defensive Cyber Operations (DCO). This will be accomplished by providing a response capability against advanced threats, and enhancing DCO decision making, making the process more agile, responsive and effective in order to maintain Commanders' freedom of manoeuvre in cyberspace.

The intent is to create a sustainable, state-of-the-art defensive cyber security operations capability, comprised of DND/CAF personnel and professional services, enabled with appropriate governance and policy, and equipped with the right tools and processes.

Purpose of this RFI

Public Services and Procurement Canada (PSPC), on behalf of The Department of National Defence (DND) / Canadian Armed Forces (CAF), is releasing this Request for Information (RFI) to inform Industry and to seek input on the possible procurement and related costing for the Defensive Cyber Operations - Decision Support Project and Cyber Security Awareness (DCO-DS and CSA) Project. As the projects are closely linked they are currently both under this single RFI. This RFI will be continually amended to advise industry, on an on-going basis, of industry engagement activities and resulting feedback. To facilitate this process it is Canada's intention to keep the RFI open until such time as a final Request for Proposal is released, however responses to the RFI are requested by the date listed in Table 1 – Procurement / Engagement Activities and Related Dates.

The RFI and engagement process provides Industry with the opportunity to present their capabilities and considerations regarding Canada's requirements for the DCO-DS and CSA Project. Canada may use the information gathered to assist in the development of a Request for Proposal (RFP). The intent is to actively engage and consult Industry throughout the procurement process to ensure a successful project end-state.

Security Sponsorship: As the RFI contains a classified Annex and as the draft RFP, RFP as well as the resulting contract may contain classified information, one of the key purposes of this RFI is to provide direction and assistance to interested suppliers who do not meet the security requirements detailed in Annex E in obtaining those clearances. Please refer to Annex I – Request for Security Sponsorship for details on the sponsorship process. Only suppliers meeting the security requirements will be provided with the classified components of any resulting

RFP(s).

Proposed Engagement and Procurement Process

The proposed engagement and procurement process for both projects is explained in greater detailed in Part 1 of this RFI and consist of a multi-phased approach as detailed below. Please be advised the proposed procurement activities beyond this initial RFI are for discussion only and may be amended at any time. The decision to conduct any further procurement activities has not been taken.

Phase 1

Letter of Interest: A Letter of Interest (LOI) for both projects was issued in December of 2016 and closed January 2017 under Buyandsell.gc.ca solicitation numbers W6369-17DE25/A and W6369-17DE26/A. A total of 31 companies responded to the LOIs. The results of the LOI indicated the need for a more detailed Request for Information (RFI).

Request for Information: A RFI to provide more detailed information to industry and will act as a continuous single point of official project(s) communication. Chiefly it will solicit detailed industry feedback on operational and technical requirements, cost and schedule.

Unclassified Industry Day: To present an overview of the requirements and engagement process.

One-on-One Meetings: Classified one-on-one meetings to distribute, present and discuss the classified Annex of the RFI.

Group Follow-up Meeting: Classified group follow-up meeting to distribute classified questions and answers.

Phase 2

Request for Information: The RFI issued in Phase 1 will remain open in order to provide direction and assistance to suppliers in obtaining security clearances.

Draft Request for Proposal: A draft RFP for each project or a single combined project may be released to suppliers meeting the security requirements for their review and input.

Phase 3

Request for Proposal: The formal Request for Proposal for each project or a single combined project will be issued.

Evaluation: Bids will be evaluated in accordance with the terms of the RFP.

Phase 4

Contract Award: A contract(s) will be awarded to the winning bidder in accordance with the terms of the RFP.

Procurement Timeline

Canada is at the preliminary stage of a potential procurement process, however it is Canada’s intention that the engagement and procurement activities follow the timeline below. Suppliers are advised to note the dates for information requested by Canada and are asked to submit the information requested on or before that date.

Table 1 - Procurement / Engagement Activity and Related Dates

Procurement / Engagement Activity	Date
Security Clearance Sponsorship*	From RFI release to RFP release
Phase 1	
Letter of Interest	Completed January 2017
Request for Information (RFI), includes:	Present to Autumn 2019
Industry Day Registration deadline	February 16, 2018
Unclassified Industry Day	February 26, 2018
Classified One-on-one Meeting registration deadline	January 23, 2018
Classified One-on-one Meetings	February 26, 2018 – March 2, 2018
Classified Group Follow-up Meeting registration deadline	January 23, 2018
Classified Group Follow-up Meeting	TBD - Week of March 5, 2018
RFI Response Date	**March 23, 2018**
Phase 2	
Draft Request for Proposal	Autumn 2019
Phase 3	
Request for Proposal	Summer 2020
Evaluation	Autumn 2020
Phase 4	
Contract Award	Summer 2021

*Suppliers not meeting the security requirements of the RFI, RFP and potentially the contract will be sponsored for the required clearance by PSPC. Suppliers not meeting the security requirements will only have access to the information publically posted.

PART II - REQUEST FOR INFORMATION

1. INSTRUCTIONS FOR RESPONDING TO THIS REQUEST FOR INFORMATION

1.1. Nature of the Request for Information

Respondents are reminded that this is an RFI and not a Request for Proposals (RFP). As such, respondents are requested to provide their comments, concerns and recommendations regarding how the requirements or objectives described in this RFI could be satisfied. Respondents should explain any assumptions they make in their responses.

Responses will not be used for competitive or comparative evaluation purposes, and thus the response format is not as rigorously defined as would normally be for an RFP. However, for ease of use and in order for the greatest value be gained from responses, Canada requests that respondents follow the structure outlined in the Format of Responses.

Whether or not any potential supplier responds to this RFI will not preclude that supplier from participating in any future procurement. Also, the procurement of any of the goods and services described in this RFI will not necessarily follow this RFI.

1.2. Response Costs

Canada will not reimburse any organization for expenses incurred in responding to this RFI, including, but not limited to, expenses incurred for participating in the additional engagement activities or security sponsorship process.

1.3. Treatment of Responses

Use of Responses: Responses will not be evaluated. However, the responses received may be used by Canada to develop or modify the procurement approach. Canada will review all responses received. Canada may, at its discretion, review responses received after the RFI Response Request Date.

Review Team: A review team composed of representatives of the Department of National Defence and Public Services and Procurement Canada (PSPC) will review the responses. Canada reserves the right to hire any independent consultant or to use any Government of Canada (GOC) resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

Confidentiality: Respondents should mark any portions of their response that they consider proprietary or confidential. Responses will be handled in accordance with the provisions of various legislations including the *Access to Information Act* (R.S. 1985, c. A-1) the *Privacy Act* (R.S., 1985, c. P-21), and the Defence Production Act (R.S. 1985, c. D-1).

Clarifications: Canada may, at its discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response or for one-on-one meetings.

1.4. National Security Exception

To protect national security interests, Canada has invoked its right under national and international trade agreements to use a National Security Exception (NSE) for this procurement.

An NSE allows Canada to remove a procurement from some or all of the obligations of the relevant trade agreement where Canada considers it necessary to do so in order to protect its national security or other related interests specified in the text of the national security exceptions.

1.5. Nature and Format of Responses Requested

Respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements described in the RFI could be satisfied. Respondents are also invited to provide comments regarding the content, format and/or organization of any draft documents included in this RFI. Respondents should list and explain any assumptions that they make in their responses.

1.6. Contents of the RFI

The information contained in this document remains a work in progress and respondents should not assume that new requirements will not be added to any bid solicitation that is ultimately published by Canada. Nor should respondents assume that none of the requirements will be deleted or revised. Comments regarding any aspect of the requirement are welcome. This RFI also contains specific questions addressed to industry.

1.7. Solicitation Caveat

This RFI does not imply that Canada has made a final decision on any procurement possibilities. DND/CAF may not select any of the solutions or equipment identified in the responses. Canada shall not be liable under any circumstances to any supplier who has prepared a response to this RFI.

1.8. Format of Responses

Industry is invited to respond to this RFI and provide the following information no later than the specified response request date . Respondents are asked to consider the following in preparing their response:

Cover Page: If the response includes multiple volumes, respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the respondent.

Title Page: The first page after the cover page should be the title page, which should contain the following information:

1) the title of the respondent’s response and the volume number;
2) the name and address of the respondent;
3) the name, address and telephone number of the respondent’s contact;
4) the date, and
5) the RFI’s Solicitation Number.

General Layout and File Format: Use the written format of respondent`s choice, but should use the Product Offerings and Pricing Information Response Template provided at Annex D and keep the same section numbering to facilitate Canada’s review and analysis of all responses. Responses should be provided electronically in MS Word, MS Excel, and/or PDF format. The layout of the submission should follow this proposed format:

1) Section 1: Executive Summary – 1 to 2 pages, summarizing the submission in total,
2) Section 2: Corporate Profile,
3) Section 3: Proposed Concept of Solution, and
4) Section 4: General Comments and Advice;

Number of Copies: Canada requests that respondents submit a copy of their response in unprotected (i.e. no password) MS Word, MS Excel, and/or PDF format by email, if the size of the document is less than 5MB, to: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Alternatively, Canada requests that respondents save a copy of their PDF (2003 or later) document onto each of four USB memory drives and mail them to the prime contracting authority below.

1.9. Enquiries

All enquiries and other communications related to this RFI shall be directed exclusively to the PSPC Contracting Authority. Since this is not a bid solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all respondents; however, respondents with questions regarding this RFI may direct their enquiries to:

Primary Contracting Authority:

Patti Wight
Public Services and Procurement Canada
Place du Portage III, 8C2
11 Laurier Street Gatineau, Quebec K1A 0S5
819-420-1757

Secondary Contracting Authority:

Jessica Strangemore
Public Services and Procurement Canada
Place du Portage III, 8C2
11 Laurier Street Gatineau, Quebec K1A 0S5
819-420-1771

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

The use of email to communicate is preferred.

Suppliers are encouraged to submit questions and provide feedback even if they choose not to participate in Industry day and/or one-on-one meetings.

Enquiries Containing Classified Information: Suppliers **must not email** any enquiries which contain SECRET classified information. This includes references to details in Annex C. Suppliers are advised to indicate simply the page or line etc. of Annex C which their enquiry is referencing. If the enquiry must contain classified information suppliers must contact the PSPC Contracting Authority and wait for direction as the question(s) must be hand delivered to the Contracting Authority

1.10. Language of Response

Responses may be submitted in French or English, at the preference of the respondent.

1.11. Submission of Responses

Time and Place for Submission of Responses: Canada request suppliers submit responses in accordance with the RFI Response Request Date listed in Table 1 - Procurement / Engagement Activity and Related Dates. The RFI closing date listed on page 1 of the RFI is not the deadline for comments or input. Suppliers interested in providing a response should deliver it by email to the Contracting Authority identified above by the time and date indicated.

Responses Containing Classified Information: Suppliers must not email any responses which contain SECRET classified information. This includes references to details in Annex C. Suppliers are advised to indicate simply the page or line etc. of Annex C which their response is referencing. If the response must contain classified information suppliers must contact the PSPC Contracting Authority and wait for direction as the response must be hand

delivered to the Contracting Authority

Identification of Response: Each respondent should ensure that its name, return address, the solicitation number appear legibly on the outside of the response.

Return of Response: Responses to this RFI will not be returned.

Comments and input will be accepted any time up to the time when/if a follow-on solicitation is published.

1.12. Fairness Monitor

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

The Fairness Monitor's duties include, but will not be limited to the following:

a. observing all or part of the procurement process (including, but not limited to, the engagement and contemplated RFP processes);
b. providing feedback to Canada on fairness issues; and
c. attesting to the fairness of the procurement process.

Please note that, for the purpose of carrying out its Fairness Monitor related obligations, the Fairness Monitor will be granted access to industry responses and related correspondence received by Canada as a result of this RFI and may act as an observer at potential follow-up engagement or contracting activities.

2. OBJECTIVES OF THIS REQUEST FOR INFORMATION

2.1. Purpose

This RFI is being issued with the key objectives of:

- Soliciting indicative pricing and scheduling information for the acquisition and in-service support for key requirements of the CSA and DCO-DS projects.
- Soliciting feedback on industry capabilities to assist in the development of the Industrial and Technological Benefits (ITB) Value Proposition.
- Collaborating with industry on the ITB and Value Proposition strategy.
- Serving as a continuous point of contact for Canada and Industry throughout the engagement and procurement process.
- Outlining the engagement approach and proposed procurement process.
- Providing schedule and procurement updates.
- Advising industry of key dates within the RFI process.
- Soliciting detailed industry feedback on the procurement process, operational and technical requirements, cost and schedule.
- Advising suppliers of the security requirements of the RFI, Draft RFP, RFP and resulting contract.
- Provide direction and assistance to non-cleared suppliers in obtaining security clearances.

2.2. Provision of Classified Information (Annex C and Classified Questions and Answers)

Respondents who meet the security requirements for receipt of Annex C of the RFI and the one-on-one meetings, upon their request to the Contract Authority, will be:

a. Invited to attend a one-on-one meeting that will be conducted within a classified environment.
b. Provided with the classified Annex C at the one-on-one meeting.
c. Invited to attend a follow-up group meeting to be provided with hard copies of any classified questions and answers.

Annex C will only be provided in hard copy and in person during the one-on-one meeting or the group follow-up meeting. It will not be issued outside of these two events. The classified annex provides additional details that may assist suppliers in preparing their response. Suppliers are advised however that although it provides more granularity with respect to the current operations and in-service capabilities at DND it is not required to provide a fulsome response to this RFI.

2.3. Provision of License to Canada Owned Intellectual Property

This RFI shall also advise industry that Canada developed and owned intellectual property (IP) exists under a Defence Research and Development Canada (DRDC) project for an automated computer network defence tool – ARMOUR. If a supplier is interested in investigating this IP they are advised to email the Prime or Secondary Contracting Authority at section 1.9 who will then pass on the request to DRDC. Please be advised DRDC is wholly responsible for any inquiries or licensing process pertaining to this IP.

3. SECURITY

There are Security Requirements associated with this RFI. For more information on personnel and organization security screening or security clauses, suppliers should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

One of the key purposes of this RFI is to advise suppliers of these mandatory security requirements associated with the various procurement and engagement activities and allow non-cleared suppliers to request security clearance sponsorship by PSPC in order that they may participate. It is Canada's intention to keep this RFI open until such time as a final RFP is released to advise suppliers of the security requirements and sponsor suppliers to the Canadian Industrial Security Directorate (CISD) so they may obtain the required clearance. PSPC will cease to sponsor security clearances upon the release of the final RFP. Canada will not delay the release or closing of a RFP while suppliers obtain the required security clearance.

3.1 Security Requirements of Procurement and Engagement Activities

The RFI, draft RFP, RFP and resulting contract each contain specific mandatory security requirements as detailed in section 4.3 below and Annex E – Security Requirements. The following chart, however, summarizes the security requirements by procurement / engagement activity. Security clearance(s) must be issued by PSPC's Canadian Industrial Security Directorate (CISD). The security clearance of foreign suppliers will be confirmed through the International Industrial Security Directorate (IISD) with their own domestic industrial security programs.

Table 2 - Procurement / Engagement Activity and Associated Security Requirements

Procurement / Engagement Activity	Security Clearance Required
Phase 1	
Request for Information (RFI):	
Unclassified Industry Day	None
View Annex C	Facility Security Clearance: SECRET, CAN, US, UK, AU Personnel Viewing: SECRET CAN, US, UK, AU
Obtain a hard copy of Annex C Obtain a hard copy of any Classified Questions and Answers	Facility Security Clearance: SECRET, CAN, US, UK, AU Personnel Transporting Document: SECRET, CAN, US, UK, AU Document Safeguarding: SECRET
Attend Classified One-on-one Meetings Attend Classified Group Follow-up Session	Facility Security Clearance: SECRET, CAN, US, UK, AU Personnel Attending: SECRET, CAN, US, UK, AU
Unclassified Questions and Answers	None – will be publically posted
Phase 2	
Draft Request for Proposal*	Document Safeguarding: SECRET
View Classified Information	Personnel: SECRET, Canadian Eyes Only
Obtain a hard copy of Classified Information	Facility Security Clearance: SECRET, Canadian Eyes Only Personnel Transporting Document: SECRET, Canadian Eyes Only Document Safeguarding: SECRET
Attend Classified Meetings	Personnel: SECRET, Canadian Eyes Only
Phase 3	
Request for Proposal*	Facility Security Clearance: SECRET, Canadian Eyes Only Personnel: SECRET, Canadian Eyes Only Document Safeguarding: SECRET
View Classified Information	Personnel: SECRET, Canadian Eyes Only
Obtain a hard copy of Classified Information	Facility Security Clearance: SECRET, Canadian Eyes Only Personnel Transporting Document: SECRET, Canadian Eyes Only Document Safeguarding: SECRET
Attend Classified Meetings	Personnel: SECRET, Canadian Eyes Only
Phase 4	
Contract*	Facility Security Clearance: TOP SECRET, Canadian Eyes Only Personnel: TOP SECRET SIGINT, Canadian Eyes Only* Document Safeguarding: SECRET, NATO SECRET

*Draft only at this time. Security Requirements may be amended throughout the procurement process. Please be advised the proposed procurement activities beyond this initial RFI are for discussion only and may be amended at any time. The decision to conduct any further procurement activities has not been taken.

3.2 Security Clearance Sponsorship for Phases 1-3

Interested suppliers or potential bidders in the Cyber Security Industry whose organizations currently do not hold the required clearance(s) for the first three phase of the project are encouraged to initiate the security clearance process immediately. The process for requests for sponsorship is detailed in Annex J. It is the responsibility of the supplier to ensure that the information required concerning the security clearance is provided on time to either the Contracting Authority or the CISD.

Early submission of all applications for security clearances is strongly encouraged. Suppliers are also strongly encouraged to submit applications for security clearances for key individuals who may be required to have access to sensitive information and/or access to secured sites during any phase of the project starting with the current Industry Engagement up to Contract Award and Delivery.

Similar processes apply, with variances, to all of the countries with which Canada has bilateral security instruments. We encourage foreign suppliers to research the requirements of their own domestic industrial security programs to discover whether they are eligible to meet these requirements, and what the specific procedures that apply to their country might be. As mentioned, early submission is strongly encouraged.

Engagement Activities and any resulting Procurements will not be delayed in order to provide time for suppliers to obtain required security clearances.

3.3 Security Clearance Sponsorship for Phase 4

As the security requirements for the contract have not been finalized Canada may at a later date sponsor interested suppliers or potential bidders in the Cyber Security Industry whose organizations currently do not hold the anticipated clearance(s). Should Canada choose to sponsor suppliers for Phase 4, this RFI will be amended to add that process.

4. INDUSTRIAL AND TECHNOLOGICAL BENEFITS (ITB) POLICY

The Industrial and Technological Benefits (ITB) Policy may be applied on the Cyber Security Awareness and Defensive Cyber Operations – Decision Support projects. 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. Suppliers are directed to ANNEX F - Application of the Industrial and Technological Benefits (ITB) Policy for an overview of the ITB Policy and questions to industry for this requirement.

5. OFFICIAL LANGUAGES

Any future contract for a solution to these projects will require the Contractor to provide all documentation and technical and client support in both official languages.

6. ENGAGEMENT APPROACH

The industry engagement process began with a Letter of Interest and will concludes when a final Request for Proposal(s) is issued or when Canada advises suppliers that the engagement process has concluded. As any final solicitation documents may themselves be classified they may not be publically posted. Please be advised the proposed engagement approach and related procurement activities beyond this initial RFI are for discussion only and may be amended at any time. The decision to conduct any further procurement activities has not been taken.

Suppliers interested in participating in any of the engagement activities, including requesting Annex C, are advised to review the Rules of Engagement at Annex G.

Canada intends to undertake the following phased industry engagement approach:

Phase 1 Activities

Letter of Interest: An initial Letter of Interest (LOI) for both projects was issued in December of 2016 and closed January 2017. The LOI's informed industry, at a high level, of the projects and sought to gain general feedback on potential solutions, costs and advise potential suppliers the ITB Policy may be applied. A total of 31 companies

responded to the LOIs. The results of the LOIs indicated the need for a more detailed Request for Information (RFI).

Request for Information: This RFI provides more detailed information to industry and will act as a continuous single point of official project(s) communication. It will:

- Advises suppliers of the security requirements of the RFI, RFP(s) and resulting contract(s) and provide direction and assistance to non-cleared suppliers in obtaining security clearances.
- Solicit detailed industry feedback on operational and technical requirements, cost and schedule.
- Solicit advice on industry capabilities to develop the ITB Value Proposition with questions about industrial capacity for performing work related to the future contracts in Canada, strengthening Canadian supply chains and making long-term investments in the Canadian cyber security sector.
- Answer questions from industry to ensure all interested participants receive the same information. Classified responses will be disseminated accordingly.

Unclassified Industry Day: An unclassified Industry Day will be held in the National Capital Region, Ottawa, ON. The purpose of Industry Day is to present registered industry representatives with an outline of the procurement process, the engagement approach, security requirements and an unclassified overview of the projects. The Industry Day is intended to be an open forum allowing Canada to communicate its requirements at a high level, and for industry to ask questions and seek information in order to gain a sound understanding of the requirement.

The anticipated agenda for the Industry Day session is:

1. Opening Remarks
2. Procurement Process – Engagement Approach
3. Security Requirements
4. Project Overview
5. Invite suppliers to give feedback and discuss the projects.
6. Next Steps /Question and Answer Period

Industry Day material to be provided to attendees:

a. Agenda
b. Copies of presentation material

One-on-One Meetings: For suppliers meeting the security requirements as detailed in Annex E representatives from Canada will make themselves available to registered suppliers for one-on-one meetings. These meetings will be classified and will be held at a secure DND facility.

The intention of the meeting is to:

1. Provide suppliers with a hard copy of Annex C. Annex C will only be provided in person.
2. Provide suppliers with an overview of the classified Annex C.
3. Invite suppliers to give feedback and discuss Annex C only.

Suppliers meeting the security requirements who would like to take part in a one-on-one supplier consultation must send a request and register as outlined in Annex I. Suppliers who request a meeting will be provided with additional information and will be asked to identify potential schedule times within the specified window for a meeting with Canada. Canada will either confirm a requested time or will reply with an alternative suggested time. Meeting times will be allocated on a first come, first served basis.

All one-on-one supplier consultations and the group follow-up meeting will be concluded prior to the Requested Response Date of the RFI. Canada may request one-on-one consultations with any suppliers at any time during or after the Requested Response Date of the RFI to obtain clarifications on feedback received.

Group Follow-up Meeting: In order to distribute classified questions and answers to suppliers meeting the security requirements detailed in Annex E, a single group follow-up meeting will be held at a secure facility at DND. At the Group Follow-up Meeting hard copies of the questions and answers generated during the one-on-one meetings will be distributed to suppliers meeting the security requirements. No discussions will occur at this meeting. Suppliers meeting the security requirements who did not attend a one-on-one meeting are welcome to attend the group follow-up meeting in order to obtain a copy of Annex C and any classified questions and answers.

Phase 2 Activities

Request for Information: The RFI issued in Phase 1 will remain open and continue to:

- Advises suppliers of the security requirements of the RFI, RFP(s) and potential resulting contract(s) and provide direction and assistance to non-cleared suppliers in obtaining security clearances.
- Answer questions from industry to ensure all interested participants receive the same information. This will continue to be done in accordance to the security requirements related to Annex C.

Draft Request for Proposal: A draft RFP for each project or a single combined project will be issued to industry to further refine the requirement by addressing industry concerns and considering industry recommendations. Only suppliers meeting the security requirements as detailed in Annex E will have access to the classified components of the Draft RFP.

Phase 3 Activities

Request for Proposal: The final Request for Proposal for each project or a single combined project will be issued to industry. A standard question and answer process will be followed. As the industry is actively consulted in the early industry engagement process, less questions or concerns are expected.

Evaluation: Bids will be evaluated in accordance with the terms of the RFP.

Phase 4 Activities

Contract Award: A contract(s) will be awarded to the winning bidder in accordance with the terms of the RFP.

7. INFORMATION REQUESTED BY CANADA

7.1. Documents of Interest

Attached to this RFI are the following documents for which Canada is seeking comments from industry:

- Annex A – Project Background;
- Annex B – Preliminary Statement of Operational Requirements;
- Annex C – Current Concept of Operations and In-Service Capabilities (CLASSIFIED); and
- Annex F – Application of the Industrial and Technological Benefits (ITB) Policy.

The information contained in this document are at a preliminary stage and remain a work in progress and respondents should not assume that new requirements will not be added to any bid solicitation that is ultimately published by Canada. Nor should respondents assume that none of the requirements will be deleted or revised. Comments regarding any aspect of these draft documents are welcome.

7.2 Guidance and Registration

The following annexes provide additional guidance on how to respond to this RFI, Rules of Engagement and the registration process for meetings and requesting classified information:

- Annex D – Product Offerings and Pricing Information Response Template;
- Annex E – Security Requirements;
- Annex G – Rules of Engagement;
- Annex H – Registration to Attend Group Industry Meeting;
- Annex I – Registration for One-on-One Meetings, Group Follow-up Meeting; and
- Annex J – Request for Security Sponsorship.

7.3 Invitation to Respond

All interested respondents, regardless of whether they meet the security requirements, are invited to provide a written submission to include (among others):

a. A description of proposed products and solutions covering each or a set of the notional functional components described in Annex B within the Notional Component Architectural View;
b. Indicative pricing, work breakdown structure, and scheduling of proposed products and solutions, including their integration, installation, configuration, testing, and training tasks;
c. Indicative pricing and scheduling of proposed in-service support and on-going maintenance tasks;
d. Proposed procurement approach with recommendations for competitive procurement, selection criteria, and basis of payment approach; and
e. Additional recommendations or advice concerning the project requirements and plans.

7.4 Information Requested

Using the format identified in section 1.8, Canada requests responses as follows:

Section 1 - Executive Summary: – 1 to 2 pages, summarizing the respondent's submission in total,

Section 2 - Corporate Profile:

1) Provide a brief introduction and corporate capability description, highlighting products, services, Canadian based capabilities, and experience in delivering solutions relevant to the project objectives,

2) Describe intent and ability to play the role as prime system integrator, a potential subcontractor or a supplier of products and/or services as may apply to one or both projects or any specific component or part of this RFI,

3) Describe established partnerships with other industries, if any, that would be of benefit to the development of the project capability requirements,

4) Describe role or approach to the Industrial and Technological Benefits (ITB) Policy outlined in Annex F, and

5) Outline any key assumptions, constraints, concerns, conclusions and recommendations that, in respondent's opinion, Canada should consider as the project evaluates the various options,

Section 3 - Proposed Concept of Solution. Respondents are asked to provide:

1) **Outline Plan of Solution** - an outline concept, high-level work breakdown structure, and schedule for any or all deliverables defined in Annex B that the respondent intends to provide, describing key products and components, software, hardware, and engineering services. Suppliers should, in the context of the information in Annex B:

   i. provide a description of how their proposed system specifications and capabilities meet or exceed the requirements outlined in Annex B (note that suppliers may offer solutions that do not necessarily conform to the functional components described in Annex B within the Conceptual Architectural View as long as the total solution meets the requirements);

   ii. provide their approach to maintaining data, product, sub-system and system integrity in a contested environment,

   iii. provide their approach to innovation, with a view to maintaining capability relevance throughout the life-cycle. Describe how the proposed solution achieves the desired operational qualities identified in Annex B,

   iv. indicate the degree of deployable modularity with their solution and its components,

   v. provide their approach to ingesting and integrating existing data feeds, supported by data models and previous experience in this area as applicable,

   vi. indicate their solutions' scalability to meet larger enterprise needs of up to 150,000 network users, 125,000 endpoints (desktop and VHD), 6000 servers and up to 150 Cyber Operators simultaneously having access to query the system.

   vii. provide solution deployment details, including phasing approaches, to development, testing, implementation, training and upgrades,

   viii. provide product, sub-system and system-level reliability and availability from historical information, and

   ix. state the identified Technical, Management, Training, Security, Support and Schedule-related risks, and mitigations that they recommend. If a risk can be mitigated by altering the existing policies, CONOPs or architecture, the Supplier should feel free to recommend such a mitigation strategy.

2) **High Level Outline Plan and Sequence of Events** - an indicative project plan and schedule (measured in Months after Contract Award) for the delivery of any or all deliverables defined in Annex B that the respondent intends to provide. For System Integrators' responses, for the purpose of accurately costing both projects, separate CSA and DCO-DS outline plans are requested but, as applicable, identification and comments to the effect of any potential savings resulting from the implementation of both projects as a single initiative can also be submitted,

3) **Estimated Costs for Each Deliverable** - an indicative cost estimate, with a per-unit description, for any or all deliverables defined in Annex B that the respondent intends to provide. The goal is to confidently estimate the Total Cost of Ownership over the life of the capability. To that end, the supplier should present a view so that the development, test, roll-out, support and upgrade costs, including recurring and non-recurring costs, are clearly identified and broken out for the entire life cycle. Additional supporting cost

information is desirable. It is recognized that supplier pricing models vary from number of events per second, number of end-point devices deployed, per user or flat fee subscriptions and others. In completing the Cost Data Model, provided as Annex D, Respondents are requested to clearly state how each deliverable is provided along with its estimated annual in-service support costs. For example, if delivering a capability requires discrete hardware and software units, support personnel or operations centre staff, suppliers should clearly indicate such in the Unit Cost Basis, the Price/Unit and the Number of Units required. At a minimum, the response must indicate the solution as a clearly calculable cost based on a simple model of: **Cost = Price/Unit x Quantity of Units**

Section 4 - General Comments and Advice. Respondents are asked to provide comments, remarks, and advice concerning:

1) The performance objectives, operational requirements and/or notional functional components as described in Annex B,

2) The current capabilities as described in Annex C, including operational unit organizational structures,

3) Completing the Cyber Entities Attribute Data Compliance matrices for both Human and Non-Human Cyber Entities provided in the appendices to Annex D,

4) The ITB/VP questions provided in Annex F,

5) Improvements to project descriptions, objectives, management and procurement approaches to enhance overall implementation efficiencies, and

6) Proposed solutions:

   i. Whether the proposed solution is for CSA, DCO or both? Does the proposed solution fulfill all the requirements for the selected (CSA/DCO-DS) solution?

   ii. List the open source and/or commercially available 3rd party components (suppliers) required to integrate with the proposed solution to make it complete?

   iii. How does the proposed solution, including selected open source and/or commercially available 3rd party components, integrate and interoperate in a diversified technology environment? Is the proposed solution intended to reuse and integrate existing DND/CAF components?

   iv. How does the proposed solution integrate data from and distribute data to multiple security levels and caveats?

   v. Will components of the proposed solution be rendered ineffective in a Disconnected, Intermittent and Low Bandwidth environment and to what extent can interruptions be recovered? What are the proposed alternatives to support in a Disconnected, Intermittent and Low Bandwidth environment and costing associated with that?

   vi. How would the proposed solution track all details related to non-human cyber entities connected to the network (authorized & non-authorized), their logical and physical state, and location?

   vii. Does the proposed solution provide any customizability and extensibility, through a scripting or programming interface?

viii. What is the proposed enterprise-capable data store solution?

ix. Could the DND/CAF obtain a demonstration license of the proposed solution components for its test and evaluation environment?

7) Threat Information:

i. Which threat information sources and formats would be integrated?

ii. How could the threat sources be exchanged / shared with mission partners and allies?

8) Supply Chain Integrity and Security

i. 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

ii. 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.

iii. 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.

iv. 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.

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

vi. **Question**: How could these contracting clauses potentially affect the cost, schedule and design of your proposed solution? What additional information would your company need to better address cost, schedule and design risks imposed by Supply Chain Integrity related restrictions?

9) Any other areas of concern or advice that would aid in providing a recommendation for improvement for the definition of the projects and their implementation.

ANNEX A: PROJECT BACKGROUND

ANNEX A: PROJECT BACKGROUND

1 Introduction

1.1 Project Status

The capability requirements are presented as two separate but related projects: Cyber Security[1] Awareness (CSA) and Defensive Cyber Operations – Decision Support (DCO-DS). Both projects are currently in the Options Analysis[2] phase with the goal to present the preferred approach to Treasury Board (TB) of Canada in spring 2019. To receive approval to move into the Definition Phase[3] for the projects, it is **essential** that indicative[4] costs and schedules be determined for the implementation of the projects. Industry feedback is therefore sought in terms of costing models and quotes for the professional services, technology, hardware, software, project management support, and integration and sustainment work that are required to satisfy the business need and requirements for these two projects.

1.2 Business Need

To meet the operational demands of a contested cyberspace and maintain corporate and operational effectiveness as an identified Lead Security Agency within the Government of Canada (GC), DND/CAF commanders, executives, managers and operators require a capability to maintain Cyber Security and situational awareness (the objective of the CSA Project), integrated with a capability to provide deep contextual analysis to support their decisions and actions through Defensive Cyber Operations (DCO) (the objective of the DCO-DS Project).

The CSA project aims to provide an end-to-end awareness of the location (logical and physical), status, and configuration of DND/CAF cyberspace. This increased awareness will improve accountability of DND/CAF cyberspace entities and enhance the DND/CAF cyberspace security posture, enabling measured responses to cyber events. With the knowledge gained through this automated system DND/CAF can create, enforce, and

---

1 **Cyber Security** is defined as the “body of technologies, processes, practices, and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability”, TERMIUM Plus®, The Government of Canada’s terminology and linguistic data bank, 9 Oct 2014.

2 **Options Analysis Phase** is the second step in the Project Approval process used by DND/CAF. A key deliverable of this phase is an Indicative Cost estimate (usually established through Requests for Information and Price and Available requests from industry) of the budget that will be required to implement the project solution.

3 **Definition Phase** is the third step in the Project Approval process used by DND/CAF. A key deliverable of this phase is a *Substantive* Cost estimate (usually established through a formal Request for Proposal from industry) of the budget that will be required to implement the project solution.

4 **Indicative Costs** are a developed estimate supported by standardized costs and research. The level of detail would encompass granularity of planned expenditures to all cost items greater than 10% of contract value supported by multiple quotes from vendors, identification of component parts, and plans for positions by rank *[required skills/expertise]*. The actual price of the contract will be within +/- 25 % of an indicative number. DND Costing Handbook, Second Edition – April 2006.

monitor its complex and dispersed cyberspace. Confirmation of standards compliance can be maintained, and the engineering process by which cyberspace change is implemented can be quantified and verified. The knowledge of cyberspace entities will also permit the implementation of increased security measures around identified vital services or areas of known cyber vulnerability essential to operations.

The DCO-DS project aims to enhance DND/CAF's ability to detect, analyse and share suspicious cyberspace activities, and upon discovery, support the decision making process for DCO by identifying available response actions and their consequences. In addition, it will automate the execution of response actions when approved or if pre-approved.

The intent of the projects collectively is to create a sustainable, state-of-the-art defensive cyber security operations capability, comprised of DND/CAF personnel and professional services, enabled with appropriate governance and policy, and equipped with the right tools and processes.

1.3 Initial Letters of Interest

On 16 December 2016 the two projects published their initial Letters of Interest (LOIs)[5] where the intent was to inform and prepare industry for potential procurement opportunities concerning the projects and seek input and contribution regarding the projects' scope, requirements, schedule, risks and potential costs.

Responses to these LOIs assisted the project team in reaching the following general conclusions:

a. There is significant interest within Industry at large to provide solutions for both projects;
b. The technology exists to provide solutions for both projects in a timely, cost-effective manner that:
    1) Cover the entire cyber-attack life cycle,
    2) Cover the Information Technology Infrastructure (ITI) network architecture from edge to core,
    3) Provide intelligence-based decision making,
    4) Address threats and attack vectors relevant to the constituency,
    5) Target systems and programs that are mission relevant,
    6) Are adaptable to the environment, architecture, and limitations of end systems,
    7) Use open standards,
    8) Incorporate both network-based and host-based sensors, data feeds, logs, and Intrusion Detection, Intrusion Prevention and Anti-Virus systems,
    9) Mix signature and heuristics-based detection,

[5] For further information on the initial project information and requirements, respondents are asked to refer to the initial Letter of Interest that was published on BuydandSell.gc.ca (https://buyandsell.gc.ca/procurement-data/tender-notice/PW-QE-049-26099 and https://buyandsell.gc.ca/procurement-data/tender-notice/PW-QE-049-26100 on 16 December 2016.)

10) Provide overlapping, complementary observables and techniques, where needed, and

11) Use a mix of freestanding ITI monitoring technologies with security-relevant data feeds;

12) Industry is prepared to fulfill the following supplier roles:

    i. **Prime System Integrator**. These suppliers would offer Total System Responsibility (TSR) solutions for the project, bringing together new and existing component sub-systems into a whole and ensuring that those sub-systems function together. Prime System Integrators may subcontract responsibilities and delivery of sub-systems and specific products to other suppliers, but will retain overall system capability performance responsibility. These suppliers will require detailed and broad classified understanding of the DND/CAF ITI, Cyber Security Awareness and Defensive Cyber Operations requirements.

    ii. **Sub-System Integrator**. These suppliers would offer solutions to specific sub-systems of the total capability. Sub-System Integrators may subcontract responsibilities and delivery of components and specific products to other suppliers but will retain overall performance responsibility for their sub-system. These suppliers will require detailed classified understanding of the DND/CAF ITI in specific Cyber Security Awareness and Defensive Cyber Operations sub-system segments and their relationship to the total capability being sought, or

    iii. **Product Supplier**. Product suppliers would offer specific turn-key products that may be used by one or more sub-systems. As a result, no specific classified knowledge of DND/CAF ITI nor Cyber Security Awareness and Defensive Cyber Operations would normally be required,

13) Industry noted the close-coupling of the two projects and, in some cases, the need to consider them in a joint fashion, potentially as a single project;

14) More detailed information is required by industry to support a reasonable cost estimation exercise; and

15) To complete the information gathering tasks and appreciating the potential security requirements, it is essential to conduct more detailed information exchange with Industry to support the analysis of potential solutions, risks and cost estimations.

1.4 Preliminary Operational Requirements

Refer to Annex B for a description of the Preliminary Operational Requirements. Note that Annex B presents the current CSA and DCO-DS operational requirements within a Conceptual Model Architectural View.

1.5 Current Situation

Refer to Annex C for a description of the current situation.

ANNEX B: PRELIMINARY STATEMENT OF OPERATIONAL REQUIREMENTS

ANNEX B: PRELIMINARY STATEMENT OF OPERATIONAL REQUIREMENTS

1 Introduction

1.1 Background

As a preliminary Statement of Operational Requirements (SOR), this document will continue to evolve in concert with industry and stakeholder discussion. The intent is to arrive at the end of the projects' Definition Phase, in early 2019, with an approved SOR for a military capability that industry can deliver. Enabled by the governmental and departmental policies listed at Appendix 1, the requirements definition effort continues until requirements finalization. As a result, Canada may decide to change, add or delete requirements. The Request for Information (RFI) allows respondents to propose solutions. The solutions should not be constrained by the conceptual elements described herein and should, where applicable, contribute to the refinement of the requirements, processes and workflows associated with each project.

Requirements definition is also a trade-off exercise with factors such as affordability and feasibility. To this end, given the current architecture and concept of operations described in Annex C, the project team has a need to determine the indicative Total Cost of Ownership (TCO) for the desired capability, from deployment through an expected 10-year life-cycle.

1.2 Vision

With a view to securing and defending Canadian Armed Forces (CAF) cyberspace, the combined Cyber Security Awareness (CSA) and Defensive Cyber Operations-Decision Support (DCO-DS) project vision is to provide the CAF with a sustainable, state-of-the-art cross domain defensive cyber security operations capability. More specifically, the capability will be operating at SECRET and TOP SECRET level, delivering Cyber Defence for networks at SECRET and DESGINATED levels using data collected from UNCLASSIFIED to SECRET sources.

The delivered capability will be comprised of DND/CAF personnel and professional services, enabled with appropriate governance and policy, and equipped with the right tools and processes. Sustained by responsive in-service support and training, the outcome brings CAF's cyber security[1] and Defensive Cyber Operations (DCO) [2] capabilities to world-class standards. The intent is to provide the Joint Force Cyber Component Commander (JFCCC, as described in Annex C) with the required factual situational awareness, available courses of action, and their operational impacts, to make evidence-based cyber security and DCO decisions.

The plan is to provide an Initial operating capability, with a cyber security and DCO equivalent to the National Institute of Standards and Technology (NIST) IT Security Maturity Level 5[3]. The capability must remain effective, adaptive and in-service throughout its 10-year life-cycle; it will evolve rapidly and on demand to pre-empt and respond to threats and remain effective despite the ever changing cyber landscape.

1.3 Scope

For the purposes of this RFI, the capabilities required are currently concentrated on providing integrated functionality

---

[1] **Cyber Security**. The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

[2] **Defensive Cyber Operation**. A defensive operation conducted in or through cyberspace to detect, defeat and/or mitigate offensive and exploitive actions to maintain freedom of action.

[3] http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html

on the classified domain and the Deployed Designated Domain. Any references, within this document, to "DND/CAF cyber domain" or "DND/CAF cyberspace" should be taken in that context with an understanding that the delivered solution requires the flexibility to be expanded in scope to include additional network domains or data feeds. Annex C provides the representative infrastructure. Additional assessment will be done during the Options Analysis phase to determine the project scope within the broader DND/CAF cyber domain.

The scope of the requirements enables the above vision by providing cyber operators a single integrated environment that enables the collaboration on, and the conduct of, cyber security and DCO across multiple domains of varying classification. This includes, but is not limited to, the people, policies, processes and tools required to provide visualization, task management, individual and collective training, and an accessible, actionable data repository leading to a defensible DND/CAF cyber domain.

1.4 Operational Qualities

The capability sought for both projects are focused on having the following operational qualities.

1.4.1 **Awareness**

The ability to gather, fuse and display quality, timely information across different security domains.

a. **Need**. Cross-domain awareness is paramount to the quality of decision outcomes in cyber security and cyber defence. Fused data from multiple and growing number of sources is necessary to visualize the DND/CAF cyber domain, with a view to facilitating command of the Cyber Force.

b. **Outcome**. An unobstructed, persistent and manageable visualization of DND/CAF cyberspace - from the tactical to the strategic levels - that enables analysis and command decision making. Throughout all operations, DND/CAF information remains secure.

1.4.2 **Responsiveness**

The ability to take action when and where required.

a. **Need**. DND/CAF requires the ability to exercise authoritative control over the sustained and transformational cyberspace security posture, across operational and developmental instances, at tactical, operational and strategic levels.

b. **Outcome**. In order to identify, characterize and mitigate against threats, attacks and vulnerabilities, DND/CAF has a dynamic, adaptable reactive and proactive capability which continuously analyzes the cyberspace security posture and supports response actions.

1.4.3 **Flexibility**

The ability to support multiple courses of action and the freedom to manoeuvre within them.

a. **Need**. An operational capacity that is: deployable, able to work within CAF operational context; scalable, modular and can be readily expanded; and, can effectively function in a cross domain environment.

b. **Outcome**. A capability that is effective, scalable and sustainable across CAF operational scenarios and functional within the DND/CAF cyber defence environment.

1.4.4 **Resilience**

The ability to recover from or adjust to, network change, attack, misfortune, damage, or destabilizing perturbations in the cyber, operational and natural environment.

a. **Need**. A capacity that can readily recover from, or adjust to, the operational situation while maintaining quality cyber security and DCO capability. The capacity considers the present and evolving threats and the evolution of technologies within the cyber domain, ensuring the confidentiality, integrity and availability of operational information and cyber security information.

b. **Outcome**. A sustainable capability that can continuously support network operations, cybersecurity, and DCO within a highly contested environment.

1.4.5 **Innovative**

The ability to do new things or to do old things in a new way.

a. **Need**. An operationally effective capacity that continuously evolves and exploits emerging opportunities (such as Artificial Intelligence (AI), Machine Learning (ML), and advanced analytics) through new processes, upgradable tools and adaptive training.

b. **Outcome**. Throughout its life-cycle, a best-of-breed capability that easily evolves with the changing environment, mission and threat, contributing to the broader cyber security of Government of Canada (GC).

1.4.6 **Interoperability**

All force entities seamlessly connect, or provide information to, each other.

a. **Need**. A Joint capacity for multiple data sources to be fused and exchanged across DND/CAF, with key allies and amongst partners, operationally effective across the existing and planned DND/CAF cyberspace infrastructure. (GC, US, FVEY, NATO, Public Safety, Shared Services Canada (SSC), the Communications Security Establishment (CSE) and the private sector)

b. **Outcome**. A technical and informational capability that enables seamless operations within DND/CAF and with our key allies and partners.

2 General Concept of Operation

2.1 Introduction

Appreciating that many products, concepts, tools, software and hardware exist within the IT, cyber security and cyber defence industries as a whole, the operational requirement is presented in a generalized, modular approach with conceptual functional building blocks, or modules.

2.2 Operational View

Figure B - 1 provides a high-level operational view of the desired system where the Cyber Operators are the personnel tasked with cyber security and defensive cyber operations. These operators are on the front line of the CAF operations, supporting the JFCCC in their roles. Refer to Annex C for the lines of command, control and communication. In establishing the capability, the organizational authorizations, enabling policies and business processes are put in place to allow the defensive cyber security operations capability to execute its mission.

The intent is to create, equip, organize and train a Cyber Security Operations Centre capability that defends DND/CAF networks in the current 24/7 non-stop environment while providing initial training, on-going training, professional development and mentoring of DND/CAF Cyber Operators who may be deployed to support DND/CAF cyber security and defence operations domestically or internationally.

The current concept of operations sees all Cyber Operators and other users (managers, executives, commanders and their staffs) perform their tasks through a single integrated environment. These tasks include, but are not limited to: workflow, monitoring, analysis, alerting, reporting, situational awareness, response actions and training (individual and collective). Each Cyber Operator is presented with a common dashboard visualization tool, customizable to their specific role and responsibilities. Personnel such as departmental executives, commanders, managers and other elements of the DND/CAF network operations (such as the Royal Canadian Navy, the Royal Canadian Air Force, the Canadian Army, CJOC, CANSOFCOM and the Strategic Joint Staff) would be similarly enabled with rights and privileges to information and actions based on their designated and assigned roles within

DND/CAF.

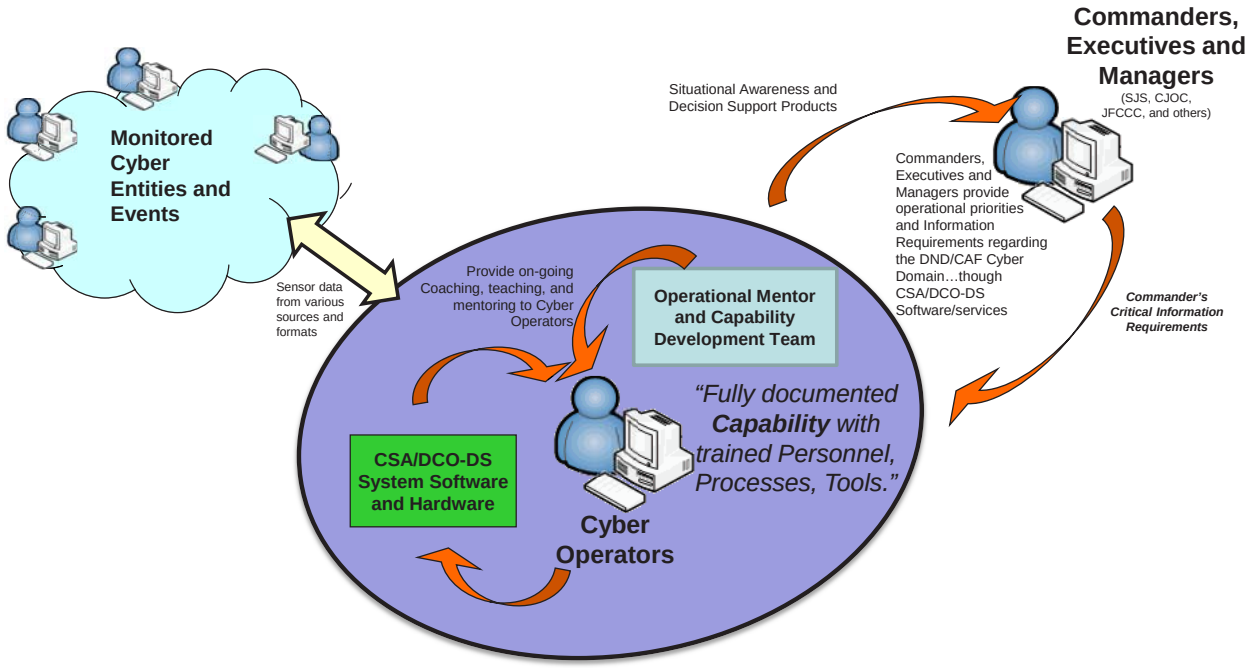

Figure B - 1 - Operational View

2.3 Functional requirements

2.3.1 **Key Operators and Roles**

Within the DCO, the proposed solution will establish a 24/7 operating environment that sees no more than ten (10) Cyber Operators on shift at any one time for every 10,000 users within a defined DND/CAF cyberspace. Each shift includes Tier 1, 2 and 3 [4] Security Analysts and Specialists, Cyber Intelligence Analysts, a System Administrator, and a Manager. The manager-to-staff ratio, and number of staff, are expected to vary with time of day, day of week and threat activity.

Building on traditional, industry-standard Security Operations Centre concepts, and guided by the CAF cyber defence mandate, the team will conduct DCO that are enabled by timely cyber security situational awareness.

With the intent of delineating the essential activities, and drawing from evolving Joint Doctrine, Defence R&D Canada articulated the Cyber Defence Functions and Tasks in 2015. This Mission-Function-Task analysis translated the required cyber defence capabilities into cyber defence missions and their functions, and then enumerated the tasks needed to perform each function. Figure B - 2 presents the core cyber defence activities that cyber security and DCO capabilities must affect.

[4] As described in Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, May 2015, SANS Institute: **Tier 1** – Alert Analyst, **Tier 2** – Incident Responder, **Tier 3** – Subject Matter Expert/Hunter

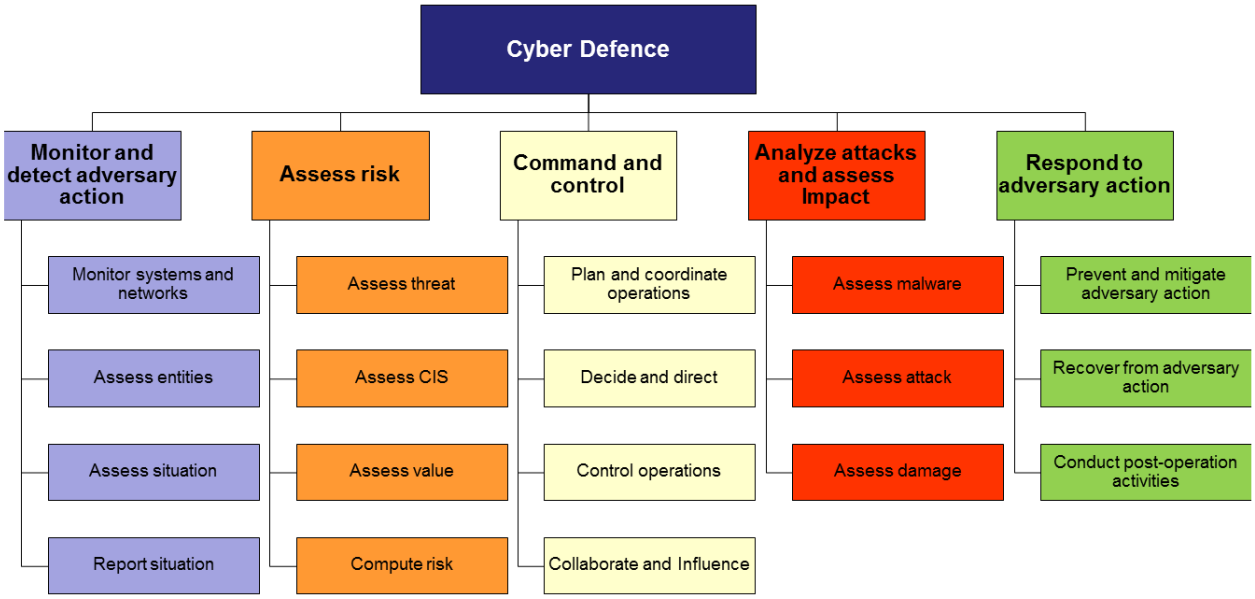

Figure B - 2 - Cyber Defence Functions and Tasks

2.3.2 **Operational Mentor and Capability Development (OMCD)**

Professional services, in the form of an OMCD team(s), will be co-located with the delivered capability during implementation and throughout its life-cycle. The role of OMCD is to coach, teach and mentor the cyber operators (at all applied rank levels) to achieve their mission through continuous business transformation, skills development, collective training development and coordination, and cyber tool development and sustainment. The OMCD will:

a. Support the business transformation of the CAF cyber security and DCO capabilities to become a NIST Level 5 security operations capability;

b. Support cyber security operations and DCO; and

c. Mentor Cyber Operators at all levels to improve skills and enhance CAF cyber operations in order to maintain proficiency.

2.3.3 **Cyber Capability Assessment and Evaluation Facility (CCAEF)**

The task of the Cyber Capability Assessment and Evaluation Facility is to provide the CSA and DCO-DS projects with a capability to exercise and test cyber defence and security solutions within a simulated environment, representative of the targeted cyber domain (ie CSNI or some other cyber domain or portion thereof) of interest, to support decisions regarding further investigations or plans for implementation, if deemed appropriate.

The vision of the CCAEF is to provide cybersecurity research; test and evaluation services that improve the cybersecurity posture of and address the changing threat landscape to the DND/CAF Cyber Domain. To achieve the vision, the CCAEF will provide a scalable and adaptable environment to support:

a. The identification and validation of cybersecurity threats and risks by simulating the DND/CAF Cyber Domain to determine impact to the DND/CAF mission.

b. The integration of cybersecurity capabilities, tools and technologies to protect information systems, data and infrastructure, while satisfying the strict needs for safety, security and availability.
c. The transition to a continuous monitoring of the information system environment to effectively and efficiently detect and prevent cybersecurity events.
d. The process improvement to respond and recover from cybersecurity events and attacks including advanced and persistent attacks from criminal groups and nation-state adversaries.
e. The process to assess and improve the resilience of information systems ability to operate and perform the DND/CAF mission even when affected by a cybersecurity event or attack.

The CCAEF system solution will:

a. Accurately simulate the performance of all DND/CAF Cyber Domains at SECRET level and below, and provides a configuration managed baseline representation of each facet of these networks;

b. Provide, within the DND/CAF Cyber Domains under evaluation, reliable and accurate performance evaluations of:

    1) New hardware and/or software,

    2) configuration changes to existing installed hardware and/or software,

    3) additions or changes to the nature and number of authorized users,

    4) additions or changes to points of presence and their locations;

    5) effects on data throughput and/or bandwidth at any point within the networks,

    6) the collection of system log data and SIEM data, and

    7) the distribution of system log data and SIEM data;

c. Integrate with existing or planned DND/CAF ITI test and evaluation systems;

d. Improve Technical Awareness and understanding of how existing DND/CAF Cyber Domains are configured and operating; and

e. Improve Identification of vulnerabilities in the existing DND/CAF Cyber Domains.

2.4 Cyber Entities

A Cyber Entity is defined as “any distinct thing or actor that exists within the cyber infrastructure [cyberspace].” [5] Cyber situational awareness is therefore dependent upon the “knowledge of cyber entities in the cyberspace necessary to make well-informed decisions regarding cyber security.”

There are two types of cyber entities of interest and it is essential that as many of the key attributes possible of cyber entities be discovered, captured, recorded, tracked and maintained:

a. **Non-human Cyber Entities**. These are participant system elements (physical or virtual) such as workstations, routers, switches, processes, files, servers and memory. The table at Appendix 2 to this

[5] Source: NATO Cooperative Cyber Defence Centre of Excellence.

annex lists the key attributes that must (where applicable) be collected for each non-human cyber entity.

b. **Human Cyber Entities**. These are actual people and their personas operating within cyberspace. The table at Appendix 3 to this annex lists the key attributes that must (where applicable) be collected for each human cyber entity.

2.5 Performance Objectives

Building upon open industry standards, Table B - 1 presents the general system activity rates and their performance objectives, and provides preliminary Measures of Effectiveness for each.

Table B - 1 - General Performance Objectives

Rate of Activity	Objective	Measure of Effectiveness
Within Seconds	• Detect that a cyber entity becomes active (connected) within the DND/CAF cyberspace. (e.g. a laptop has connected to the network, a user has logged-in, a USB stick has been plugged into a computer, etc) - CSA • Automatically prevent an attack at the network or host through a protective tool such as Host Intrusion Prevention System (HIPS) – DCO-DS • Generate an audit entry and send it to a Security Information and Event Management (SIEM) console – DCO-DS • Automatically extract files such as an email attachment or download from or across the network, execute it in a detonation chamber, and analyze it for signs of malicious activity – DCO-DS • Trigger an Intrusion Detection System (IDS) alert and send both the alert and the associated packets to the SIEM console – DCO-DS	• MOE 1: Cyber common operating picture automatically updated. • MOE 2: The system has near real time detection capabilities and can detect anomalous cyber events across all DND/CAF cyber domain. • MOE 3: Sufficient capacity to store network traffic captures metadata, logs, alerts and statistics from DND/CAF cyber domain. • MOE 4: Sufficient capacity to monitor all network traffic, metadata, logs, alerts and statistics from the DND/CAF cyber domain. • MOE 5: Support the conduct of manual analysis for multiple cyber events from DND/CAF accredited cyber domain and data which can be analysed in near real time to report on targets, impacts and attack characteristics. • MOE 6: Automated initial analysis process based on historical data, intelligence, and current threats, to predict and report on the characteristics of the cyber event, attribution and possible future threats
Within Minutes	• Recognize that a detected cyber entity within the DND/CAF cyberspace is either human or non-human, and discover its key attributes - CSA • Determine sufficient key attributes of a detected cyber entity within the DND/CAF cyberspace to determine its specific identity and location (physical and/or logical) - CSA • Determine an accurate operational characterization of detected cyber entities within the DND/CAF cyberspace as Friendly, Enemy and Unknown, sufficient to support an engagement decision – DCO-DS	• MOE 1: Location, activity, and configuration of network devices are monitored and updated as changes occur. • MOE 2: Baseline status of the network is established and the status of the network is known. • MOE 3: Network and cyberspace changes can be confirmed remotely to track their implementation on the network. • MOE 4: Cyber threats are aligned with physical and personal security considerations so security

Rate of Activity	Objective	Measure of Effectiveness
	• Query each month's log data for any system in the DND/CAF cyberspace and gather results - DCO-DS • Generate pivot tables to assist cyber operators in identifying entities with similar or connected malicious behaviour and prompt the operator to initiate response actions – DCO-DS • Retrieve a week's worth of indexed Packet Capture (PCAP) from online storage for any entity criteria such as set of IP addresses, hostnames, ports, user accounts or content – DCO-DS • Recognize an event of concern and tag it as benign or fill out a case and escalate it to Tier 2[6] – DCO-DS • Isolate an infected host – DCO-DS • Identify and contact a sysadmin, security officer or operations officer at a site whose system was involved in a potential incident – DCO-DS	changes can be automatically approved, tracked, and responsive to multiple threat vectors. • MOE 5: Security software and systems cannot compromise the cyber domain functionality. • MOE 6: Security systems operate when connected to the network, and stand-alone. • MOE 7: Upon reconnection to the network, nodes access is automatically confirmed to enable trust with the device. • MOE 8: The ability to automatically implement an update or upgrade if identified as being required by an associated cyber participant. • MOE 9: Interoperability (communication and shared situational awareness) with GC and allied systems. • MOE 10: Report and presentation of the necessary information for decision makers including: o Affected cyber data; o Analysis results; o Action taken from automated response; o Known comparable events, previous responses, and lessons learned; o Known pre-defined response options; and o Available manual response options. • MOE 11: System to receive acknowledgement of successful information exchange. • MOE 12: System to use agreed upon standards and conversion capabilities when needed, to exchange information.
Within an Hour	• Develop, download, test and deploy IDS signatures to a fleet of sensors – DCO-DS • Identify, analyze, and develop a response plan to an intrusion involving multiple systems or accounts – DCO-DS • Provide Tier 2 to Tier 3[7] analysis of the payload for a new strain of malware – DCO-DS	• MOE 1: Configuration control of all cyber entities is achieved including access points, and software utilized to create a baseline. • MOE 2: Configuration changes can be automatically implemented when required. • MOE 3: Support operational impact evaluation of the cyber event.

[6] As described in Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, May 2015, SANS Institute: **Tier 1** – Alert Analyst, **Tier 2** – Incident Responder, **Tier 3** – Subject Matter Expert/Hunter

[7] As described in Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, May 2015, SANS Institute: **Tier 1** – Alert Analyst, **Tier 2** – Incident Responder, **Tier 3** – Subject Matter Expert/Hunter

Rate of Activity	Objective	Measure of Effectiveness
	• Identify and recover from a downed sensor or data feed – DCO-DS • Gather stakeholders and brief them on details of a major incident in progress – DCO-DS	• MOE 4: Reports executed actions and time for completion.
Within a Day	• Do a monthly/quarterly scrub of all signatures deployed to an IDS fleet or content deployed to SIEM – DCO-DS • Test and recommend a major patch to the enterprise - CSA • While adhering to legal chain-of-custody standards, analyze and document the contents system involved in a serious incident – DCO-DS o Deploy an Incident Response Team o Recover data o Triage data • Remotely extract Forensics Artifacts for analysis and evidence - DCO-DS o Files o Processes o Memory o Registry o Logical hard drive image o Bit level hard drive image • Assess the actions and potential motives and intentions of an adversary operating on constituency networks – DCO-DS	• MOE 1: External vulnerability assessment - System is able to analyse new and evolving cyber threats to create a quantified assessment of the impact it will have on the network. • MOE 2: Cyber domain changes impacts and risk can be measured and their impact quantified.
Within a Week	• Report analysis results and present legally admissible evidence – DCO-DS • Develop, deploy, and make operational complex custom detection and analytics tools such as Perl scripts and SIEM use cases – DCO-DS • Revise, review, and baseline an internal defensive cyber security operations standard operating procedure (SOP) – DCO-DS • Exercise Cyber Operator shifts on new procedures – DCO-DS • Inform Cyber Operators on new and emerging threats and vulnerabilities – DCO-DS • Make new defense techniques operational with new tactics, techniques and procedures – DCO-DS	• MOE 1: Internal vulnerability assessment - Reduction in the time required to conduct an impact assessment in order to approve cyber domain changes. • MOE 2: Reduced time to complete certification of entities connecting to the network due to automation of engineering and change request systems.

Rate of Activity	Objective	Measure of Effectiveness
Within a Month	• Make new defence techniques operational with new tools to address newly identified and prioritized threats – DCO-DS • Evolve the overall security posture (policy, processes, tools) of vulnerable DND/CAF cyberspace to address newly identified and prioritized vulnerabilities - CSA	

Table B - 2 identifies the required system level performance criteria and objectives:

Table B - 2 - System Level Performance Criteria and Objectives

Criteria	Objective
Losses	• Zero packet loss at the monitoring points of presence. • Zero event log loss. • Zero information loss. • Verifiable data integrity.
Detection	• Prevent adversaries from detecting the presence of (and evading) monitoring capabilities.
Delivery	• Ensure delivery of 100 percent of security events from end devices to the defensive cyber security operations centre while protecting them from unauthorized access or modification.
Survivability	• Support the survivability of the cyber security and DCO capabilities, even when portions of the cyberspace are compromised or contested.
Confidentiality	• Protect from disclosure sensitive documents and records maintained by the defensive cyber security operations capability.

3 Operational Requirements

3.1 Operational Requirements

Table B - 3 describes the CAF operational requirements.

Table B - 3 - Operational Requirements Description

Serial	Requirement	Project	Description
1	The user must be able to establish and maintain an authoritative cyber entity inventory and configuration database for DND/CAF cyber domain	CSA	• The system shall provide the authoritative and secure cyber entity inventory database. • The system shall provide an easily visualized network map for all cyber entities. • The network map shall include discovery of authorized cyber entities (through change, configuration or release management) and unauthorized (malicious or other) cyber entities.

Serial	Requirement	Project	Description
			• The system shall use a defined naming convention for cyber entity identification. • The system entity identification shall include: entity type(s), networks, virtual/physical entity, applications/software, configuration, border devices, entity criticality, physical zone, Cross Domain Solution (CDS) info, and ownership (refer to Appendices 2 and 3).
2	The user must be able to identify cyber entities in DND/CAF cyber domain	CSA	• The system shall provide an automated process and tools to identify all entities and their configuration (authorized and non-authorized). • The system shall validate authorized entity identity. • The system shall provide an automated process and tools to respond to the discovery of non-authorized entities (e.g. host special zone, walled garden).
3	The user must be able to identify cyber entities in DND/CAF cyber domain	DCO-DS	• The system shall provide an Endpoint Detection and Response (EDR) capability with the following sub-requirements: a. The system shall provide an ability to gather detailed information regarding the current state of each endpoint device (such as running processes, registry settings, files currently opened, active network connections, hardware details like current CPU and memory usage, and user account in use). b. The system shall provide an ability to gather forensics data (historical) about endpoint devices (such as processes ran, files accessed and created, applications/commands/scripts used, user accounts used, and applications installed). c. The system shall provide an ability to remotely gather memory images or files for forensics investigation. d. The system shall provide an ability to gather hard drive images (server, workstation or mobile) for forensics investigation.
4	The user must be able to track cyber entities in DND/CAF cyber domain	CSA	• The system shall provide an automated process and tools to track all entities connected to the network (authorized and non-authorized). • The system shall provide the logical and physical state and location of the tracked entity. • The system shall track administrative accounts and evaluate this entity on a periodic basis to ensure compliance and cyber defence.
5	The user must be able to assess vulnerability of cyber entities in DND/CAF cyber domain	CSA	• The system shall provide an automated process and tools to assess the impact of known vulnerabilities (e.g. CVE data) on entities in cyberspace. • The system vulnerability impact assessment shall include DND cyberspace entity type and configuration to a complete system or service perspective. • The system vulnerability impact assessment shall consider the entire cyber kill chain.

Serial	Requirement	Project	Description
			• The system vulnerability impact assessment shall identify the likelihood of a compromise based on all known vulnerabilities. • The system shall provide support prioritizing remediation actions by identifying critical entities. • The system shall log findings, trigger alerts and generate vulnerability assessment reports.
6	The user must be able to assess configuration compliance of cyber entities in DND/CAF cyber domain	CSA	• The system shall provide an automated process and tools to assess compliance with authorized baseline configurations for all entities. • The system shall support prioritizing remediation actions by identifying critical entities. • The system shall have the ability for the Cyber Operator to automatically ingest, process and detect on indicators of compromise. • The system shall log findings, trigger alerts and generate configuration compliance reports.
7	The user must be able to correlate multiple data sources and supporting assessment processes through pre-made and custom-made reports and queries	DCO-DS	• The system shall provide an automated process and tools to ingest authoritative information sources from the following: a. accredited user identity data; b. accredited administrator identity data; c. threat intelligence data; d. entity inventory data; e. vulnerability data; f. configuration management data; g. SIEM data; h. PCAP data; i. forensic data; j. newly identified data sets and metadata; and k. security assessment & authorization data. • The authoritative system data sources will be hosted on networks of low, medium and high sensitivity. • For new data source, data formats and communication protocols must adhere to current industry standards or be supported through open APIs.
8	The user must be provided with a configurable workstation interface	CSA DCO-DS	• The system shall provide a user-friendly configurable interface providing Situational Awareness suitable to the Cyber Operator's role, functions and tasks. • The system shall provide an automated process and tools to request tailored assessments. • The system shall provide a customizable method to view report results and send reports and alerts. • The system shall permit scheduled or on-demand assessment.

Serial	Requirement	Project	Description
			• The system shall provide an indicator for priorities of current mitigation tasks. • The system shall provide a configurable user interface to perform Decision Support tasks and access role-based tools, view status and send reports/updates.
9	The user must be able to assess risk resulting from proposed changes to existing DND/CAF cyber entities	CSA	• The system shall provide an automated process and tools to analyse the impact of proposed DND/CAF cyberspace changes. • The system shall provide an automated means to report on the impact of proposed DND/CAF cyberspace changes. • The cyberspace changes shall include: response to threats, net new, update or removal of software, hardware, configuration or design. • Change risk assessment shall ingest RFC and Configuration Management updates.
10	The user must be able to perform all tasks in DIL (Disconnected, Intermittent or Low-bandwidth) environments	CSA DCO-DS	• The system must provide a rapidly deployable, local assessment capability to support DIL environments (e.g. ships, aircraft and austere deployments). • The system must provide a centralized assessment capability to obtain and fuse all information from DIL environments, when connectivity conditions allow. • The system must be flexible enough to work in operationally imposed bandwidth constraints. • The system must provide an alternate information transfer method to facilitate DIL environments, while not compromising information when connectivity conditions improve.
11	Optional, the user should have the ability to monitor and understand platform IT and operational technology[8] security data feeds	CSA	• The system should integrate platform IT data feeds, such as connectivity status, security posture and configuration as may permit. • The system should integrate operational technology data feeds, such as connectivity status, security posture and configuration as may permit. • All data feeds should conform to defined open source interoperability standards.
12	The user must be able to perform all tasks through automated tasking and workflow	CSA DCO-DS	• The system must provide an automated tasking and workflow capability for responding to a trigger or alert. • The system must integrate workflows and define processes/linkages between the different functional organizations. • The system must automate repetitive analysis tasks.

[8] **Platform IT** is the technology that runs/controls the platform itself (eg. HVAC, CANBUS, 1553 bus, engines controls, SCADA)

Operational Technology is the specialized technology that resides on the platform but is not part of the platform IT (eg. surveillance suite, weapon system, radar)

<table>
<tr><th>Serial</th><th>Requirement</th><th>Project</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>• The system must provide a capability to track and monitor progress.
• The system must identify critical entities to support task prioritization.</td></tr>
<tr><td>13</td><td>The user must be able to monitor and query against document control policies</td><td>CSA</td><td>• The system must automate and enforce the use of DND/CAF data labelling on specified file types to support inventorying of data holdings and to support security policy compliance checks.</td></tr>
<tr><td>14</td><td>The user must be able to effectively perform Risk Management</td><td>CSA
DCO-DS</td><td>• The system shall identify, define, integrate and automate the processes required to support Risk Management of the DND/CAF Cyber Domain (continuous security posture and response actions).
• The system Risk Management processes and tools shall include: information categorization, security control selection, safeguard evaluation, configuration compliance check, and risk calculation.</td></tr>
<tr><td>15</td><td>The user must be able to effect Patch Management</td><td>CSA</td><td>• The system shall automate an efficient and effective patch management process.
• The system patch management process shall identify, acquire, install, and verify patches for all products and systems (commercial or government).
• The system patch management system shall include all operating systems, applications, switches, routers and devices.</td></tr>
<tr><td>16</td><td>The user must be able to understand consolidated Threat Intelligence</td><td>DCO-DS</td><td>• The system shall ingest reputable, sustainable and adjustable cyber OSINT service feed(s).
• The system shall provide an automated, effective and reliable threat intelligence fusion capability that enables multi-source and multi-caveat analytics.</td></tr>
<tr><td>17</td><td>The system must operate across multiple security domains</td><td>CSA
DCO-DS</td><td>• The system must operate in the DND/CAF user-based CDS environment (e.g. multiple security domains on a single workstation).
• The system must operate in the DND/CAF server-side CDS environment.</td></tr>
<tr><td>18</td><td>The user must be able to collect and analyze raw traffic data</td><td>DCO-DS</td><td>• The system shall provide out-of-band collection and retention of all raw network traffic in CAF cyberspace (internal, in-bound, and out-bound);
• For the purpose of costing, obtaining requirement input and establishing design requirements, consider the following data retention guidelines:
<table>
<tr><th>Data</th><th>Tier 1</th><th>Tier 2+</th></tr>
<tr><td>IDS alerts and SIEM-correlated alerts</td><td>2 weeks</td><td>5+ years</td></tr>
<tr><td>NetFlow / SuperFlow logs</td><td>1 month</td><td>5+ years</td></tr>
<tr><td>Full-session PCAP</td><td>48 hours</td><td>2+ years</td></tr>
<tr><td>Audit logs</td><td>48 hours</td><td>5+ years</td></tr>
</table></td></tr>
</table>

Serial	Requirement	Project	Description
			• The system shall support retrospective analyses and audit functions.
19	The user must be able to perform Real-Time Network Traffic Monitoring and Event Detection	DCO-DS	• The system shall provide real-time continuous monitoring and analysis of network traffic to provide signature-based and behaviour-based event detection. • The system shall correlate user activity across domains/caveats. • The system shall provide the ability to log findings, trigger alerts, and generate reports.
20	The user must be able to perform Real-Time Entity Monitoring and Event Detection	DCO-DS	• The system shall provide real-time continuous monitoring and analysis of entity activity to provide event detection. • The system shall provide and ability to log findings, trigger alerts, and generate reports.
21	The user must be able to perform Real-Time User Activity Monitoring and Event Detection	DCO-DS	• The system shall provide real-time continuous monitoring and analysis of contextualized user activity to provide event detection. • The system shall provide an ability to log findings, trigger alerts, and generate reports.
22	The user must be able to perform Enterprise Data Collection and Analysis	DCO-DS	• The system shall provide continuous collection, consolidation and correlation of security information and event logs from networked assets into a single enterprise repository to provide context, metadata and analytics; supports manual and automated (scheduled and ad hoc) queries and reports. • The system shall provide tailored analysis of short-term historical data (e.g. crafted queries, use case modelling); ability to log findings, trigger alerts, and generate reports.
23	The user must be able to perform Retrospective Analysis	DCO-DS	• The system shall provide an analysis of enterprise data to detect suspicious and anomalous activity. • The system shall provide correlation of historic events, trends and behaviours to real-time events; reconstruct activities based on context/metadata. • The system shall provide features and data supporting the hunt for Advanced Persistent Threats (APTs), insider threats, and indicators. • The system shall provide audit tools; supports manual and automated (scheduled and ad hoc) queries and reports. • The system shall provide tailored analysis of short-term historical data (e.g. crafted queries, use case modelling).
24	The user must be able to respond to alerts and triggers	CSA DCO-DS	• The system shall respond to actionable items and triggers. • The system shall report on progress/findings back to the process [or sub-system or module] that originated the tasking.
25	The user must be able to set automatic and semi-automatic event response	DCO-DS	• The system shall enable pre-determined technical responses to be automatically actioned for documented events which exceed documented thresholds. • The system shall provide a manual override option. • The system shall perform logging and reporting.

Serial	Requirement	Project	Description
26	The user must have an automated Incident Response Workflow	DCO-DS	• The system shall identify, define and automate the processes and workflow required to perform Incident Response. • The system shall perform logging, reporting, tasking, and task management.
27	The user must be able to perform forensics within Digital Chain of Custody standards	DCO-DS	• The system technologies and processes must be sufficient to meet GC investigative requirements for digital chain of custody.
28	The user must be able to exchange information and threat intelligence with partners, allies and other government departments.	CSA DCO-DS	• The system data formats and communication protocols must adhere to current industry standards or be supported through open APIs, such as: o Intrusion Detection Framework (CIDF), o Incident Object Description and Exchange Format (IODEF), o Security Device Event Exchange (SDEE), o WebTrends Enhanced Log File (WELF), o Common Event Infrastructure/Common Base Event (CEI/CBE), o Common Vulnerabilities and Exposures (CVE), o Common Event Format (CEF), o Common Event Expression (CEE). o Structured Threat Information Expression (STIX) o Trusted Automated Exchange of Indicator Information (TAXII), and o Cyber Observable Expression (CYBOX)

3.2 Notional Functional Components

The integrated capability of the CSA and DCO-DS projects will enable DND/CAF cyber security operations and provide the JCCC with the ability to defend DND/CAF networks and conduct defensive cyber operations. To this end, the capability must be able to perform several essential functions. While it is expected that several cyber security tools will be necessary to fulfill the requirements for CSA and DCO-DS, notionally, the key functional elements or components sought could be regrouped as follows:

a. an ability to create and maintain an accurate and up to date cyber Common Operational Picture (COP) operational through visualisation aids such as a Cyber Operational Dashboard (COD) and widgets, and through standard and customizable reports;

b. an ability to create and maintain an authoritative Cyber Data Repository (CDR) that includes a multi-source cyber intelligence data;

c. an ability to perform automated Cyber Entity and Event Discovery (CEED);

d. an ability to perform automated Cyber Security Monitoring and Actions (CSMA);

e. an ability to conduct Cyber Defence Analysis and implement Decision Support (CDADS);

f. an ability to perform automated Task Management (TM); and

g. an ability to utilize an integrated Operational Training System (OTS) for the cyber operators.

Table B - 4 describes each of these notional functional elements.

Table B - 4 - Notional Functional Components Description

Serial	Component	Project	Description
1	Cyber Operational Dashboard	CSA DCO-DS	The COD is the visual interface for all human users to access the information stored in the CDR, in order to improve cyber defence situational awareness and to support incident handling. The COD presents the graphical analysis tools and view into the underlying CEED, CSMA, CDR, CDADS and TM system components. The COD provides various dashboards, dynamic views and reporting features in order to support all required use cases for relevant users. The COD may either be implemented as a single interface or as a set of several different applications, depending on design choices and implementation constraints. The COD also provides standard data feeds that may be consumed by existing COP (Common Operational Picture) and C2 (Command and Control) applications, in order to visualize the cyber defence situation together with other layers of the military situation such as land, air and maritime units. The term “dashboard” refers to a single screen information display that is used to monitor the status of Cyber Entities and their behaviour. It can present multiple different views based on user configurable requirements. Views can be text based, table list text, graphical bar charts, trending line graphs, geographical map based, etc. The dashboard allows our key users (such as managers, executives, analysts, etc) sitting at their desk to see how the status of Cyber Entities. The COD also provides data feeds for existing command and control (C2) systems using standard data formats such as KML (Keyhole Markup Language, [KML]) and NVG (NATO Vector Graphics, [NVG]). This innovative capability enables the integration of cyber defence data into the military Common Operational Picture (COP), in order to combine cyber and physical domains for the overall situational awareness. The COD is the primary place of work for all Cyber Operators and all users of the CDR. It is through the COD that tasks for each Cyber Operator (ie workflows, event monitoring, work tickets, analysis, CDR data entry & management, etc) are conducted and managed.
2	Task Management	CSA DCO-DS	This component is a task allocation, work-ticket and workflow management system. Used through the COD by the appropriate Cyber Operators and Managers, the TM sub-system provides task, ticket and workflow services to control, monitor and manage the work and priorities of Cyber Operators. The TM provides a means for shift supervisors, managers, commanders and other executives to define tasks, surveillance priorities, priorities of work, review status of tasks, manage schedules and work load, etc.
3	Operational Training	CSA DCO-DS	This is the training component used to ensure that Cyber Operators, Managers, Executives and other operators are up to date and proficient in the tasks, roles and responsibilities within the integrated system, and includes: a. Operational Threat, Penetration and Attack simulation capability to exercise the Cyber Operator team and evaluate its operational readiness and effectiveness, b. an individual operator training component focussed on individual operators (task, roles and advancement in role), c. skills training and validation for cyber operators and non-cyber operators, and civilians, in their assigned roles, individually and collectively,

Serial	Component	Project	Description
			d. a collective training component for the defensive cyber security operations capability. It is a replication of the set of operation systems with offline datasets allowing complete range of functionalities and running realistic scenarios for training purposes.
4	Cyber Security Monitoring and Action	CSA	This component continuously monitors the CDR to identify the presence of non-compliant cyber entities, events, alerts, vulnerabilities, or other changes to the status of the cyber entities within the DND/CAF cyberspace. The system raises alerts to the appropriate Cyber Operators on the detection of non-compliant cyber entities or behaviours. This sub-system also reacts to cyber alerts associated with non-compliance to approved cyber security configurations of cyber entities and recommends the corrective action automatically (e.g. patch management, system update, walled garden, reduction of user/application privileges, etc.) or with Cyber Operator intervention. This component performs essential security-related activities such as Asset Management, Vulnerability Assessment, Document Control, Configuration Management, as well as Change Management functions such as the Security Assessment and Authorization process. It also includes implementation of the Centre for Internet Security (CIS) Critical Security Controls (CSC) 1 to 5, through interactions with CDR. These minimum essential CSCs are: 1. Inventory of authorized and unauthorized devices 2. Inventory of authorized and unauthorized software 3. Secure configuration of end-user devices 4. Continuous vulnerability assessment and remediation 5. Controlled use of Administrative privileges.
5	Cyber Defence Analysis and Decisions Support	DCO-DS	This component continuously monitors and analyses the CDR to identify the potential vulnerabilities or cyber-attacks and intrusions within the DND/CAF Cyber Domain. The system raises alerts to the appropriate Cyber Operators on the detection of vulnerabilities, threats, risks, and behaviours. It continuously self-tunes to reduce false positive and false negative alerts. This system also reacts to all cyber alerts and recommends appropriate corrective actions and their impacts for the Cyber Operator to consider. It will also be capable of automating the delivery of pre-approved response actions. The system provides: a. Dynamic Risk Assessment (DRA) to enable relevant stakeholders to define (and maintain over time) the criticality of their mission objectives, and the dependencies from these objectives to the DND/CAF cyberspace. This DRA capability will dynamically correlate all the information provided by CDR to continually assess the risks, and the risk signature will be available to all relevant users in the COD interface. b. Dynamic Risk Management (DRM) to support decision makers in the management of the risks that are identified by DRA. For this, the DRM capability may recommend individual response actions or complete courses of action, and assess their effectiveness, costs and side effects with respect to mission objectives. c. cyber intelligence and OSINT analysis. d. hunt and advanced analytics.

Serial	Component	Project	Description
			e. forensics analysis. f. incident handling. g. incident response with courses of action analysis. h. network security monitoring and reporting. i. operational planning.
6	Cyber Data Repository (CDR)	CSA DCO-DS	A database repository that acts as the authoritative cyber entity and event data warehouse for the DND/CAF cyberspace. It holds all data relating to the collection of all cyber entities within DND/CAF cyberspace as well as a descriptive relationship between such entities for the purposes of link analysis, vulnerability analysis, intrusion detection, forensic analysis and other cyber security tasks. The database includes all industry standard report generation, query and graphical analysis tools. The CDR is the capability that stores and consolidates all the information required to perform cyber defence activities, from various existing data sources. All the information is normalized into a unified and global data model based on standards, and made available to any application that needs it. The main goals of CDR are to consolidate information from existing tools and products that are not interoperable, and to enable more global correlation for various cyber defence activities. It is also the core component to build a modular, flexible, agile and interoperable DCO capability. This CDR also gathers, stores and maintains all-source and cyber intelligence from open source, government, allied, military and subscription services with a view to providing a comprehensive, accurate and up-to-date view of threats to the DND/CAF cyber domain, both cyber in nature or otherwise. Source information will span unclassified to TOP SECRET feeds. For security reasons, this database will be kept separate from the CDR. The database includes all industry standard report generation, query and graphical analysis tools.
7	Cyber Entity and Event Discovery	CSA DCO-DS	This component discovers, collects and stores all data related to all cyber entities and cyber events and stores it within the CDR. For manually entered data, the system uses the COD. The system discovers and collects data on pre-defined routine basis, automatically as the result of data changes on cyber entities, in response to alerts from existing monitoring systems, or on demand from a Cyber Operator. This sub-system uses: raw traffic data collection and retention, real-time network traffic monitoring and event detection, near real-time host monitoring and event detection, near real-time user activity monitoring and event detection, supported by full-packet capture at designated key points within the DND/CAF cyberspace when and where available.

Figure B - 3 shows the notional component architectural view of the modules described above.

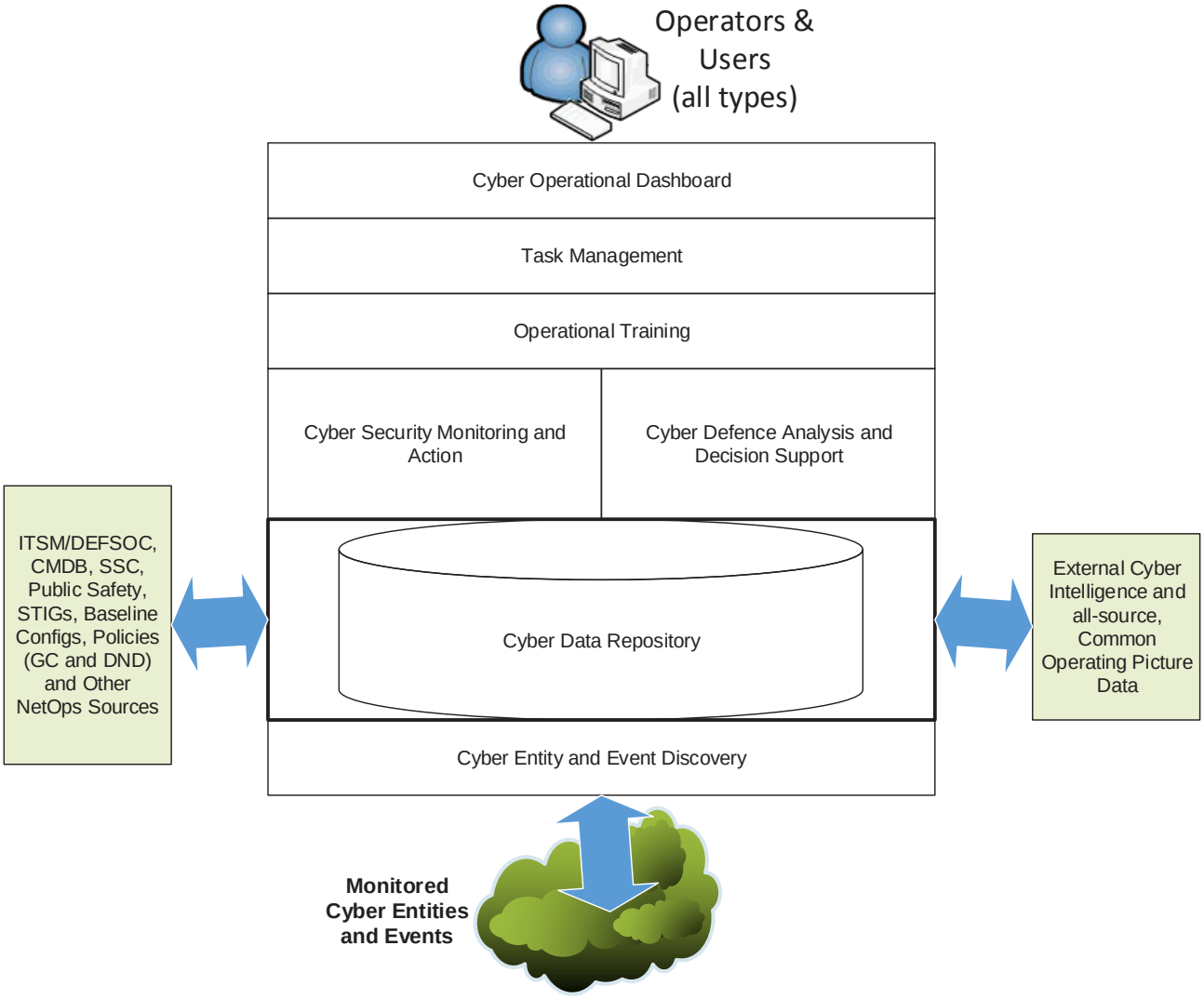

Figure B - 3 - Notional Component Architecture View

3.3 Requirements Context

The CAF operational environment is global and ever changing. DCO in the tactical battlespace requires that episodic networks are engineered to operate in austere conditions and so too must their cyber security and cyber defence capabilities. This includes deployments where there is high probability of disconnection between the enduring and episodic environments (instability of the transport infrastructure), low-bandwidth conditions (ships) and the potential presence of adversaries who will attempt to disrupt operations by contesting the CAF use of cyberspace.

Deployment involves a specific technical skillset to operate and maintain. The chain of command must ensure that the right contributions of limited skilled personnel are deployed to operate these capabilities, as required, while maintaining a core capability nationally. A common deployable configuration maximizes efficiencies from training, technical development, engineering and service operations perspectives.

Deployment within a coalition/mission partner environment requires that episodic instances created for an event which involves a coalition or mission partner deployment will be the Canadian component to the established

Federated Mission Networking environment (FMN). Cyber security and DCO capabilities deployed within such an environment, must be able to operate within the governance and policies agreed to by the Coalition.

For each operational requirement described in Table B - 1, the components and/or services must be designed to adapt to the dynamically changing nature of the cyber domain. It is accepted that it is not possible to protect the enterprise from every threat vector - the intent is to provide a system to withstand attack and continue to deliver essential command and control, no matter the event, while preserving operational freedom of action. To this end, the qualities described at paragraph 1.4 should be reflected in the implementation of each operational requirement.

3.4 Data Quality and Confidence

For every data field or attribute collected, stored or deduced through analysis, a data quality and confidence figure of merit is required to enable sound decision making.

In arriving at the quality and confidence evaluation, consider if the information/data is accurate, impactful and timely. The system must present analytic confidence measures applied to:

a. Overall information quality and confidence, based on entity records in the CDR;

b. Generalized situational awareness, from alert and ticketing status to system health maps, incident status and response;

c. Organizational, strategic, operational, tactical and technical threat intelligence confidence; and

d. Vulnerability assessment confidence.

The quality and confidence figure of merit will consider:

a. The manner in which the data was collected, gathered or generated (the source);

b. If the data had been independently verified from one or more other source;

c. The likelihood of the data changing over time; and

d. The time since the data was gathered or last verified and thus its staleness;

The quality and confidence figure of merit will be expressed in clearly unambiguous terms such as:

a. **Remote**. 1-15% likelihood of being true, complete and accurate;

b. **Very Unlikely**. 16-30%% likelihood of being true, complete and accurate;

c. **Unlikely**. 31-45% likelihood of being true, complete and accurate;

d. **Even Chance**. 46-55% likelihood of being true, complete and accurate;

e. **Likely**. 56-70% likelihood of being true, complete and accurate;

f. **Very Likely**. 71-85% likelihood of being true, complete and accurate;

g. **Almost Certain**.86-99 % likelihood of being true, complete and accurate; and

h. **Certain**. 100% true, complete and accurate.

3.5 Security

The solutions must be implemented in such a manner that supports the capability operating at SECRET and TOP SECRET level, delivering Cyber Defence for networks at SECRET and DESGINATED levels using data collected from UNCLASSIFIED to SECRET sources..

3.6 Security Assessment & Authorization

The solutions must be implemented in accordance with the requirements of the DND/CAF Security Assessment & Authorization (SA&A) Guideline (available upon request). A complete SA&A process will be conducted resulting in

the promulgation of appropriate direction regarding the implementation of the hardware, software, personnel and procedures necessary to meet the capability security requirements.

Suppliers and their sub-contractors may be required to access sensitive data and systems and may require appropriate-level personnel and facility security clearances.

Suppliers and their sub-contractors may be required to abide by Non-Disclosure Agreements (NDA) or other security restrictions.

Given the threat associated with the cyber domain, the continued, reliable, and assured supply of the goods and services to be acquired under this project must be assured at all times.

3.7 Survivability

The solutions must employ features that minimize the disruption to operations caused by component failures of all natures.

3.8 Maintainability and Support

The solutions deployment and support must be integrated with the configuration and change management processes within DND and SSC.

The support must be coordinated through established and future SSC-provided interconnectivity.

The solutions should provide the rights for DND/CAF to create, maintain and modify custom interface software used to interface information sources into the capability.

The solutions should be able to incorporate upgrades to functionality without major software engineering tasks.

The solutions must be supportable with minimum additional training for support personnel.

The solutions must be capable of quadrupling the number of endpoints with no upgrades to the existing backend system, infrastructure, components, hardware or software.

3.9 Operational Availability

The capability availability for critical components, excluding workstations (assuming a user can move to another workstation), is:

a. Mandatory: 99.9% of the time; or

b. Desirable: 99.99% of the time.

3.10 Reliability

The system must have a Mean-time-between failure (MTBF) of 100 days.

The system must be repaired and operating in a timely manner as determined through the Statement of Sensitivity (SoS) and the SA&A process.

3.11 Environmental Sustainability

The solutions must meet the DND standards for environmental stewardship.

3.12 Health and Safety

The solutions must not generate health or safety concerns for the operators over and above those imposed by the

operational environment.

The solutions must comply with all the DND/CAF health and safety codes.

3.13 Delivery Requirements

The solutions must include a secure patch and update mechanism, accessible across the globe from approved locations and assets.

The solutions must support and permit access to all users (Operational Authorities, Cyber Operators and Support Staff) concurrently located and operating within the geographic and Service Locale bounded by the National Capital Region (NCR).

The solutions must support and permit access to all users (Operational Authorities, Cyber Operators and Support Staff) concurrently located and operating:

a. outside the geographic and Service Locale bounded by the NCR but within Canada, and

b. outside the geographic and Service Locale bounded by the NCR but internationally deployed in disadvantaged Service Locales with limited Bandwidth capabilities.

3.14 Personnel and Training Requirements

The solutions must deliver all necessary training for appropriate users representing the Operational Authority, the Cyber Operators and the Support Staff, by working within CAF training policy and standards and following the conclusions of the training needs assessment. This will include facilities, training material and qualified trainers, necessary to achieve Initial operating capability and a steady state training system to ensure full operating capability.

The solutions must provide a training simulation capability to support collective operational training in a customizable operational context. The training simulation capability scenarios must be created, maintained, edited and executed by the Cyber Operators using existing workstations and systems within an exercise/training environment.

The solutions must capture best practices and implement knowledge-based learning from previous operations and actions.

4 Preliminary Contract Deliverables

In providing the indicative costs identified in Annex D, the Respondent should plan for the following contract deliverables:

a. **Project Management, Integration Engineering and System Documentation**:

1) Overall Project Management Plan,
2) Integration Plan (if declaring the Sub or Prime System Integrator role),
3) Compliance and Test Plan,
4) Business Transformation Plan,
5) All required system engineering documentation,
6) Training Plans and Training Material with online tools hosted within the DND/CAF cyberspace:
   i. Initial Cadre Training, both individual operator and collective Cyber Operator focussed;
   ii. On-going continuous training, both individual and collective Cyber Operator focussed.

b. **Notional Functional Components**. All hardware and software necessary to provide the supplier's intended capability, as installed, configured, tested and accepted and meeting the intent of the functional requirements defined in this Annex and as defined in the conceptual architectural view;

c. **Initial-cadre training** for each functional component based on the quantities listed in Annex D;

d. **Business Transformation Services**. Professional services necessary to transform the operational units and personnel to provide the defined capability;

e. **In-Service Support and Professional Engineering Services** for a 10-year period following final operational capability, contracted support personnel, hardware, software, licenses or subscriptions and all professional and engineering support services for the capability as a whole, with daily rates for categories. These services should include recurring, planned support as well as “on-call” services to respond to urgent and important incident handling or response actions; and

f. **Provision of an Operational Mentoring and Capability Development team**. As described in paragraph 2.3.2.

g. **Provision of a Cyber Capability Assessment and Evaluation Facility**. As described in paragraph 2.3.3.

APPENDIX 1 TO ANNEX B – POLICIES

1 Enabling Policies

There are a number of governmental and departmental policies that enable effective cyber security and CAF defensive cyber operations.

1.1 Government of Canada Policies

a. Canada's Defence Policy "Secure, Strong, Engaged", 7 June 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf

b. Policy on Government Security, Treasury Board of Canada Secretariat, 1 April 2012, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

c. Directive on Departmental Security Management, Treasury Board of Canada Secretariat, 7 July 2009, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579

d. Operational Security Standard: Management of Information Technology Security (MITS), Treasury Board of Canada Secretariat, 31 May 2004, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328

e. Operational Security Standard on Physical Security, Treasury Board of Canada Secretariat, 18 February 2013, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329

f. Government of Canada Cyber Security Event Management Plan (GC CSEMP), Treasury Board of Canada Secretariat, 11 December 2015, https://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/sim-gsi/msi-gis/csemp-pgec-eng.asp

g. Policy Framework for Information and Technology, Treasury Board of Canada Secretariat, 9 July 2009, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12452

h. Federal Emergency Response Plan, Minister of Public Safety, January 2011, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-eng.aspx#a53

i. Cyber Incident Management Framework for Canada, Treasury Board of Canada Secretariat, 15 December 2015, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-eng.aspx

j. Government of Canada Information Technology Strategic Plan 2016-2020, Treasury Board of Canada Secretariat, 3 October 2016, https://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/itpm-itgp/it-ti/itsp-tips/gcitsp-tigcps-eng.asp

k. Policy Framework for the Management of Assets and Acquired Services, Treasury Board of Canada Secretariat, 23 March 2012, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12022

l. Policy on Management of Materiel, Treasury Board of Canada Secretariat, 26 June 2006, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12062

1.2 Miscellaneous Departmental Polices

For the purposes of this RFI, respondents shall also assume the following policies exist:

a. User consent to monitoring: Giving the Cyber Operators and auditors the unambiguous ability to monitor and retain any and all activity on all systems and networks within DND/CAF;

b. Acceptable use policy: IT system usage rules of behavior, including restrictions on Internet and social media website use and authorized software on DND/CAF systems;

c. Privacy and sensitive data handling policies: Instructions for managing and protecting the types of information flowing across the monitored network, including personal, health, financial, and national security information;

d. Internally permitted ports and protocols: Enumeration of the ports and protocols allowed within the DND/CAF, across the core, and through enclave boundaries;

e. Externally permitted ports and protocols: Enumeration of ports and protocols allowed by devices through external boundaries such as through a demilitarized zone (DMZ), to business partners and to the Internet;

f. Host naming conventions: Describing conventions for naming and understanding the basic type and role of IT assets on the basis of their DNS record;

g. Other IT configuration and compliance policy: Everything from password complexity to how systems should be hardened and configured;

h. Bring your own device and mobile policies (if applicable): Rules that govern how employees may interface with DND/CAF networks, applications, and data with personally owned IT equipment and mobile devices;

i. Approved OSes, applications, and system images: The general approved list of OSes, applications, and system baselines for hosts of each type—desktops, laptops, servers, routers/switches, and appliances;

j. Authorized third-party scanning: Rules for notifying the operations centres when another organization wishes to perform scanning activity such as for vulnerabilities or network discovery;

k. Audit policy: High-level description of the event types that must be captured on which system types, how long the data must be retained, who is responsible for reviewing the data, and who is responsible for collecting and retaining the data—with recognition of the performance impact value of the data gathered;

l. Roles and responsibilities of other organizations with respect to incident response:

1) Internal to DND/CAF:

i. the Chief of the Defence Staff,

ii. Deputy Minister,

iii. Chief Information Officer (CIO),

iv. Departmental IT Security Coordinator,

v. the Departmental Security Officer,

vi. the Cyber Force Commander,

vii. the Joint Force Cyber Component Commander (JFCCC),

viii. The Defence Systems Operations Centre (DEFSOC),

ix. National Service Management Centre (NSMC),

x. Regional Service Management Centres (RSMC),

xi. Canadian Forces National Investigation Service,

xii. Canadian Forces Counter Intelligence Unit,

xiii. Departmental Level 1 Network Operations Centers and Security Operations Centres:

1. Royal Canadian Navy,

2. Canadian Army,
3. Royal Canadian Air Force,
4. Canadian Joint Operations Command,
5. Canadian Special Operations Forces Command, and
6. NORAD.

2) External to DND/CAF:

i. Shared Services Canada (SSC) – Government of Canada Cyber Incident Response Team (GC-CIRT),

ii. Communications Security Establishment (CSE),

iii. Public Safety Canada, and

iv. NATO and other allied partners.

m. Written service level agreements (SLAs) where applicable:

1) Network capacity and availability requirements,

2) Contingency planning if contracted network services fail,

3) Network outage (incident) alerts and restoration and escalation/reporting times,

4) Security incident alerts and remediation procedures and escalation/reporting times, and

5) Clear understanding of each party's responsibilities for implementing, operating, and maintaining the security controls or mechanisms that must be applied to the network services being purchased.

n. Legal policies: Concerning classifications of information, privacy, information retention, evidence admissibility, and testifying during investigations and prosecutions of incidents.

APPENDIX 2 TO ANNEX B – KEY ATTRIBUTES OF NON-HUMAN CYBER ENTITIES

Serial	Description
1	Host Type - physical or virtual
2	Host Name (in accordance with naming convention in use)
3	Hardware manufacturer/serial number/asset tag number (with asset tag to correlate with account holder)
4	Processor (manufacturer, serial number, model, etc)
5	Memory (manufacturer, serial number, model, etc)
6	Inventory and Identification of all Line Replaceable Units (LRUs) on board the device (CDROM/DVDRW/USB ports, physical/ keyboard/ mouse/ monitors/ NICs, processors, mother boards, power supplies, containers/frames etc)
7	Type or Primary Purpose of Device (workstation, virtual desktop router, switch, firewall, gateway, web filter, intrusion detection system, intrusion prevention system, domain controller, wireless access points, application servers, mail server, databases, intranet applications, etc)
8	Device Model, sub-model, version
9	MAC address (or addresses if more than one interface) for all natures of external interfaces
10	IP address and subnet (fixed or DHCP assigned)
11	Host URL name
12	How IP address assigned, DHCP, DHCP reserved, or fixed host assigned
13	Host Time
14	Host Network Time Server (if set remotely)
15	Host Gateway(s)
16	Host DNS main, alternate, second alternate
17	Host DHCP server
18	Host WINS server
19	Host Web Proxy server (if applicable)
20	Host Routing Tables
21	Host Port Forwarding Tables
22	Host Network Address Translation Tables (NAT)
23	Host Domain
24	Assigned Primary Domain Controller
25	Assigned Secondary Domain Controller
26	Active Directory (AD), Lightweight Directory Access Protocol (LDAP), X.500 registration status
27	IPv4 or IPv6
28	Host Permission Rights (owner, administrators, users, guests, etc) and how assigned/controlled (local or active directory)
29	SNMP data used and version number
30	ICMP status
31	Host based anti-virus software and version
32	Host based intrusion prevention software and version
33	Host based intrusion detection software and version

Serial	Description
34	Host based firewall service status
35	Host Certificate Authority
36	Host Ports (open, closed, listening, stealth mode)
37	OS and version
38	Baseline image version (if applicable)
39	Installed software inventory - High level
40	Installed software inventory - Detailed level - all DLLs, and supporting executables, configuration files, and related software modules or components.
41	Baseline configuration hashcode (for ease in baseline configuration change detection)
42	Services running on device and ports in use
43	Host services certificates
44	Username(s) logged-in and currently authenticated
45	Location – Physical place name (as in CFB Petawawa, building P114, Room 101, desk 5) and its Geodetic equivalent (latitude, longitude and altitude), or simply if mobile, its latitude, longitude and altitude.
46	Owner – Hardware account holder
47	Source of power (mains, internal battery, external battery)
48	Source of backup power system
49	Physical properties - temperature, humidity
50	Existing vulnerability reports, known threats, history of reports associated with events/incidents
51	Named network, enclave, subnet etc to which the device is connected directly
52	Date of last audit/inspect/review
53	Access/location of device internal logs (if any) (SIEM, SNMP, SCOM, etc)

APPENDIX 3 TO ANNEX B – KEY ATTRIBUTES OF HUMAN CYBER ENTITIES

Serial	Description
1	Primary user name and the networks/domains to which it's connected.
2	Alternate User Name(s) (one or more) and the networks/domains to which it's connected.
3	Complete personal name, rank, and identification info as per personnel records or in a way that it can be correlated later
4	Service, PRI or Industrial Security clearance number
5	Division, formation, unit, sub-unit, etc
6	Primary location/locale of work
7	Alternate/temporary locales of work
8	Primary domain/point of log-in
9	Alternate/temporary domains/points of log-in
10	Email addresses for each domain/network
11	User permissions/rights/owner for files, folders, networks, devices
12	Active Directory (AD), Lightweight Directory Access Protocol (LDAP), X.500 Registration status
13	Existing vulnerability reports such as file and records of documents and emails associated with the personna, known threats, history of reports associated with events/incidents, history of all end points used.
14	Date of last audit/inspect/review
15	Access/location of user data logs

ANNEX C: CURRENT CONCEPT OF OPERATIONS AND IN-SERVICE CAPABILITIES - CLASSIFIED

Annex C is classified: Suppliers who wish to review or obtain a copy of Annex C must meet the security requirements detailed in Annex E – Security Requirements

A hard copy only of the document will be provided in person to suppliers who attend either a one-on-one meeting or the group follow-up meeting. Guidance for registering for a one-on-one meeting and the group follow-up meeting is provided in Annex I.

Suppliers not meeting the security requirements are invited to request to be sponsored for the required security clearance as detailed in Annex J – Request for Security Clearance Sponsorship.

Annex C is also considered controlled goods: As Annex C 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 C). Details on how to register under the CGP are available at: http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html

ANNEX D: PRODUCT OFFERINGS AND PRICING INFORMATION RESPONSE TEMPLATE

ANNEX D: PRODUCT OFFERINGS AND PRICING INFORMATION RESPONSE TEMPLATE

Serial	Deliverable Component	Deliverable Element	Unit Cost Basis (per user, device, eps, etc)	Price per Unit						Remarks
				Qty of Units	Price per Unit	Qty of Units	Price per Unit	Qty of Units	Price per Unit	
1	**Cyber Operational Dashboard**	Project Management, Integration Engineering and System Design Documentation	Lot	1						
2		All hardware, software, installation, system configuration, and acceptance testing	per DND/CAF Cyber Operator or Executive/Manager	50		51 to 100		101 to 500		
3		Business Transformation Services	Lot	1						
4		In-Service Support System and Professional Engineering Services	Lot	1		0		0		
5		Initial-cadre training	per DND/CAF Cyber Operator or Executive/Manager	50		51 to 100		101 to 500		
6	**Task Management**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						
7		All hardware, software, installation, system configuration, and acceptance testing	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
8		Business Transformation Services	Lot	1						
9		In-Service Support System and Professional Engineering Services	Lot	1		0		0		
10		Initial-cadre training	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
11	**Operational Training**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						

Serial	Deliverable Component	Deliverable Element	Unit Cost Basis (per user, device, eps, etc)	Price per Unit						Remarks
				Qty of Units	Price per Unit	Qty of Units	Price per Unit	Qty of Units	Price per Unit	
12		All hardware, software, installation, system configuration, and acceptance testing	per DND/CAF Cyber Operator or Executive/Manager	50		51 to 100		101 to 500		
13		Business Transformation Services	Lot	1						
14		In-Service Support System and Professional Engineering Services	Lot	1		0		0		
15		Initial-cadre training	per DND/CAF Cyber Operator or Executive/Manager	50		51 to 100		101 to 500		
16	**Cyber Security Monitoring and Action**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						
17		All hardware, software, installation, system configuration, and acceptance testing	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
18		Business Transformation Services	Lot	1						
19		In-Service Support System and Professional Engineering Services	Lot	1		0		0		
20		Initial-cadre training	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
21	**Cyber Defence Analysis and Decisions Support**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						
22		All hardware, software, installation, system configuration, and acceptance testing	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
23		Business Transformation Services	Lot	1						

Serial	Deliverable Component	Deliverable Element	Unit Cost Basis (per user, device, eps, etc)	Price per Unit						Remarks
				Qty of Units	Price per Unit	Qty of Units	Price per Unit	Qty of Units	Price per Unit	
24		In-Service Support System and Professional Engineering Services	Lot	1						
25		Initial-cadre training	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
26	**Cyber Data Repository**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						
27		All hardware, software, installation, system configuration, and acceptance testing	per cyber entity within DND/CAF Cyber Domain	1 to 10,000		10,001 to 25,000		25,001 to 150,000		
28		Business Transformation Services	Lot	1						
29		In-Service Support System and Professional Engineering Services	Lot	1						
30		Initial-cadre training	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
31	**Cyber Entity and Event Discovery**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						
32		All hardware, software, installation, system configuration, and acceptance testing	per cyber entity within DND/CAF Cyber Domain	1 to 10,000		10,001 to 25,000		25,001 to 150,000		
33		Business Transformation Services	Lot	1						
34		In-Service Support System and Professional Engineering Services	Lot	1						
35		Initial-cadre training	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		

Serial	Deliverable Component	Deliverable Element	Unit Cost Basis (per user, device, eps, etc)	Price per Unit						Remarks
				Qty of Units	Price per Unit	Qty of Units	Price per Unit	Qty of Units	Price per Unit	
36	**Cyber Capability Assessment and Evaluation Facility**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						
37		All hardware, software, installation, system configuration, and acceptance testing	per cyber entity within DND/CAF Cyber Domain	1 to 10,000		10,001 to 25,000		25,001 to 150,000		
38		Business Transformation Services	Lot	1						
39		In-Service Support System and Professional Engineering Services	Lot	1						
40		Initial-cadre training	per DND/CAF Cyber Operator	50		51 to 100		101 to 500		
41	**Total Integrated System**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						
42		All hardware, software, installation, system configuration, and acceptance testing	per cyber entity within DND/CAF Cyber Domain	1 to 10,000		10,001 to 25,000		25,001 to 150,000		
43		Business Transformation Services	Lot	1						
44		In-Service Support System and Professional Engineering Services	Lot	1						
45		Initial-cadre training	per DND/CAF Cyber Operator or Executive/Manager	50		51 to 100		101 to 150		
46	**Supplier Defined Solution Basis**	Project Management, Integration Engineering and System Design and supporting Documentation	Lot	1						

Serial	Deliverable Component	Deliverable Element	Unit Cost Basis (per user, device, eps, etc)	Price per Unit						Remarks
				Qty of Units	Price per Unit	Qty of Units	Price per Unit	Qty of Units	Price per Unit	
47		All hardware, software, installation, system configuration, and acceptance testing	per Supplier Defined Quantity Basis							
48		Business Transformation Services	Lot	1						
49		In-Service Support System and Professional Engineering Services	Lot	1						
50		Initial-cadre training	per Supplier Defined Quantity Basis							
51	**Operational Mentoring and Capability Development Team**		Lot	1		1		1		

Note: As indicated in Section 7.4, Section 4 – General Comments and Advice, paragraph 6 of the main document, for System Integrators' responses, for the purpose of accurately costing both projects, separate CSA and DCO-DS outline plans are requested but, as applicable, identification and comments to the effect of any potential savings resulting from the implementation of both projects as a single initiative can also be submitted. Respondents may offer solutions that do not necessarily conform to the notional functional components described in Annex B, figure B-3 as long as the total solution meets the requirements. Respondents are requested to clearly state how each deliverable is fulfilled. For example, if delivering a capability requires discrete hardware and software units, support personnel or operations centre staff, respondents should clearly indicate such in the Unit Cost Basis, the Price/Unit and the Number of Units required. At a minimum, the response must indicate the solution as a clearly calculable cost based on a simple model of: Cost = Price/Unit x Quantity of Units.

.

APPENDIX 1 TO ANNEX D – KEY ATTRIBUTES OF NON-HUMAN CYBER ENTITIES

Serial	Description	Capability			Remarks or comments
		Compliant? (Compliant as Built Partially Compliant as Built, Possible but needs Engineering Efforts, Not Possible in foreseeable Future, Unknown)	**Explain how data determined** (Manual hand entry in CMDB, Routine Scanning of Known Device Services, Active On-Going Ananlysis of Existing Data from multiple sources, Other)	**Quality and Confidence Level in Data Element** (Remote, Very Unlikely, Unlikely Even Chance, Likely, Very Likely, Almost Certain, Certain)	
1	Host Type - Physical or Virtual				
2	Host Name (in accordance with naming convention in use)				
3	Hardware manufacturer/serial number/asset tag number (with asset tag to correlate with account holder)				
4	Processor (manufacturer, serial number, model, etc)				
5	Memory (manufacturer, serial number, model, etc)				
6	Inventory and Identification of all Line Replaceable Units (LRUs) on board the device (CDROM/DVDRW/USB ports, Physical/ Keyboard/ Mouse/ Monitors/ NICs, Processors, Mother boards, Power supplies, containers/frames etc)				
7	Type or Primary Purpose of Device (workstation, virtual desktop Router, Switch, Firewall, Gateway, Web filter, Intrusion Detection Systen, Intrusion Prevention System, Domain Controller, Wireless Access Points, Application Servers, Mai Server, Databases, Intranet Applications, etc)				
8	Device Model, sub-model, version				
9	MAC Address (or addresses if more than one interface) for all natures of external interfaces				
10	IP Address and subnet (fixed or DHCP assigned)				
11	Host URL name				

Serial	Description	Capability			Remarks or comments
		Compliant? (Compliant as Built Partially Compliant as Built, Possible but needs Engineering Efforts, Not Possible in foreseeable Future, Unknown)	**Explain how data determined** (Manual hand entry in CMDB, Routine Scanning of Known Device Services, Active On-Going Ananlysis of Existing Data from multiple sources, Other)	**Quality and Confidence Level in Data Element** (Remote, Very Unlikely, Unlikely Even Chance, Likely, Very Likely, Almost Certain, Certain)	
12	How IP address assigned, DHCP, DHCP reserved, or fixed Host assigned				
13	Host Time				
14	Host Network Time Server (if set remotely)				
15	Host Gateway(s)				
16	Host DNS main, alternate, second alternate				
17	Host DHCP Server				
18	Host WINS server				
19	Host Web Proxy server (if applicable)				
20	Host Routing Tables				
21	Host Port Forwarding Tables				
22	Host Network Address Translation Tables (NAT)				
23	Host Domain				
24	Assigned Primary Domain Controller				
25	Assigned Secondary Domain Controller				
26	Active Directory (AD), Lightweight Directory Access Protocol (LDAP), X.500 Registration status				
27	IPv4 or IPv6				
28	Host Permission Rights (owner, administrators, users, guests, etc) and how assigned/controlled (local or active directory)				
29	SNMP data used and version number				
30	ICMP Status				
31	Host based Anti Virus SW and version				
32	Host based Intrusion Prevention SW and version				

Serial	Description	Capability			Remarks or comments
		Compliant? (Compliant as Built Partially Compliant as Built, Possible but needs Engineering Efforts, Not Possible in foreseeable Future, Unknown)	**Explain how data determined** (Manual hand entry in CMDB, Routine Scanning of Known Device Services, Active On-Going Ananlysis of Existing Data from multiple sources, Other)	**Quality and Confidence Level in Data Element** (Remote, Very Unlikely, Unlikely Even Chance, Likely, Very Likely, Almost Certain, Certain)	
33	Host based Intrusion Detect SW and version				
34	Host based Firewall service status				
35	Host Certificate Authority				
36	Host Ports (Open, closed, listening, stealth mode)				
37	OS and version				
38	Baseline image version (if applicable)				
39	Installed Software Inventory - High level				
40	Installed Software Inventory - Detailed level - all DLLs, and supporting executables, config files, and related software moduals or components.				
41	Baseline Configuration Hashcode (for ease in baseline configuration change detection)				
42	Services Running on device and ports in use				
43	Host Services Certificates				
44	Username(s) logged-in and currently Authenticated				
45	Location – Physical Place Name (as in CFB Petawawa, building P114, Room 101, desk 5) and its Geodetic equivalent (Lat, Long, Altitude), or simply if mobile, its Lat, Long, Altitude.				
46	Owner – Hardware account holder				
47	Source of Power (Mains, internal battery, external battery)				
48	Source of Backup Power System				
49	Physical Properties - Temperature, Humidity				

Serial	Description	Capability			Remarks or comments
		Compliant? (Compliant as Built Partially Compliant as Built, Possible but needs Engineering Efforts, Not Possible in foreseeable Future, Unknown)	**Explain how data determined** (Manual hand entry in CMDB, Routine Scanning of Known Device Services, Active On-Going Ananlysis of Existing Data from multiple sources, Other)	**Quality and Confidence Level in Data Element** (Remote, Very Unlikely, Unlikely Even Chance, Likely, Very Likely, Almost Certain, Certain)	
50	Existing Vulnerability Reports, history of reports associated with events/incidents				
51	Named Network, enclave, subnet etc to which the device is connected directly				
52	Date of last audit/inspect/review				
53	Access/location of device internal logs (if any) (SIEM, SNMP, SCOM, etc)				

APPENDIX 2 TO ANNEX D – KEY ATTRIBUTES OF HUMAN CYBER ENTITIES

Serial	Description	Capability			Remarks or comments
		Compliant? (Compliant as Built Partially Compliant as Built, Possible but needs Engineering Efforts, Not Possible in foreseeable Future, Unknown)	**Explain how data determined** (Manual hand entry in CMDB, Routine Scanning of Known Device Services, Active On-Going Ananlysis of Existing Data from multiple sources, Other)	**Quality and Confidence Level in Data Element** (Remote, Very Unlikely, Unlikely Even Chance, Likely, Very Likely, Almost Certain, Certain)	
1	Primary User Name and the Networks/Domains to which it's connected.				
2	Alternate User Name(s) (one or more) and the Networks/Domains to which its connected.				
3	Complete personal name, Rank, and identification info as per personnel records or in a way that it can be correlated later				
4	Service Number				
5	Division, formation, Unit, sub-unit, etc				
6	Primary Location/locale of work				
7	Alternate/temporary locales of work				
8	Primary Domain/point of log-in				
9	Alternate/temporary Domains/points of log-in				
10	Email addresses for each Domain/network				
11	User permissions/rights/owner for files, folders, networks, devices				
12	Active Directory (AD), Lightweight Directory Access Protocol (LDAP), X.500 Registration status				
13	Date of last audit/inspect/review				
14	Access/location of user data logs				

ANNEX E: SECURITY REQUIREMENTS

1.0 SECURITY REQUIREMENT FOR CANADIAN SUPPLIER: PWGSC FILE #: SRCL - W636917DE25 and W636917DE26 – PHASE I

1. The **Supplier / Respondent** must, at all times during the performance of the request for information, 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).

2. This **request for information** includes access to controlled goods. Prior to access, the **Supplier / Respondent** must be registered in the Controlled Goods Program of Public Works and Government Services Canada.

3. The **Supplier / Respondent** personnel requiring access to CLASSIFIED information, assets or sensitive work site(s) must EACH hold a valid personnel security screening at the level of **SECRET**, granted or approved by CISD/PWGSC.

4. The **Supplier / Respondent** personnel requiring access to **RESTRICTED CLASSIFIED** information, assets or sensitive work site(s) **must be a citizen of Canada, United States, United Kingdom or Australia** must EACH hold a valid personnel security screening at the level of **SECRET**, granted or approved by CISD/PWGSC.

5. Processing of CLASSIFIED information electronically at the **Supplier / Respondent** site is NOT permitted under this **Request for Information**.

6. The **Supplier / Respondent** must comply with the provisions of the:

   a) Security Requirements Check List and security guide (if applicable)

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

2.0 SECURITY REQUIREMENT FOR INTERNATIONAL SUPPLIER: PWGSC FILE #: SRCL - W636917DE25 and W636917DE26 – PHASE 1

Protected A, Protected B, Confidential, Secret,

The supplier/respondent must be from a country with which Canada has an international bilateral industrial security instrument or will have such an instrument with Canada by the end of the bidding period. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html

All **CANADA PROTECTED / CLASSIFIED** information/assets, furnished to the Foreign recipient **Supplier/Respondent**, shall be safeguarded as follows:

1. The Foreign recipient **Supplier / Respondent** shall, at all times during the performance of the **Request for Information**, hold a valid Facility Security Clearance (FSC), issued by the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country**, at the equivalent level of **SECRET**, and hold an approved Document Safeguarding Capability Clearance at the level of **SECRET.**

2. All **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated under this **Request for Information** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Request for Information**, in accordance with the national policies of **the supplier's country.**

3. The Foreign recipient **Supplier / Respondent** 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 supplier's country**.

4. All **CANADA PROTECTED / CLASSIFIED** information/assets provided to the Foreign recipient **Supplier / Respondent** pursuant to this **Request for Information** by the Government of Canada, shall be marked by the Foreign recipient **Supplier / Respondent** with the equivalent security classification utilized by **the supplier's country** and in accordance with the national policies of **the supplier's country**.

5. The Foreign recipient **Supplier / Respondent** shall, at all times during the performance of this **Request for Information**, ensure the transfer of **CANADA PROTECTED / CLASSIFIED** information/assets be facilitated in accordance with the national policies of **the supplier's country**, and in compliance with the provisions of the Bilateral Industrial Security Instrument between **the supplier's country** and Canada.

6. Upon completion of the work, the Foreign recipient **Supplier / Respondent** shall return to the Government of Canada, via government-to-government channels, all **CANADA PROTECTED / CLASSIFIED** information/assets furnished or produced pursuant to this **Request for Information**, including all **CANADA PROTECTED / CLASSIFIED** information/assets released to and/or produced by its subcontractors.

7. Throughout the duration of this **Request for Information**, the Foreign recipient **Supplier / Respondent** 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 **Request for Information** 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 **Supplier / Respondent**, as part of this **Request for Information**. The *Defence Production Act* defines Canadian Controlled Goods (S.35).

8. The **Request for Information** involves access to Unclassified military data, which is subject to the Provisions of the Technical Data Control Regulations. The UNITED STATES of AMERICA recipient **Supplier / Respondent** is required to become a certified contractor in the US/Canada Joint Certification Program (JCP).

9. Such **CANADA PROTECTED and CLASSIFIED** information/assets shall be released only to foreign recipient **Supplier / Respondent** personnel who have a need to know for the performance of the **Request for Information**, must be a citizen of **Australia, the United Kingdom, 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 supplier's country.**

10. **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated pursuant to this **Request for Information** shall not be further provided to a third party Foreign recipient supplier 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 Supplier 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 supplier's country**, if the third-party Foreign recipient Supplier is located in a third country.

11. The Foreign recipient **Supplier / Respondent** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system any **CANADA PROTECTED / CLASSIFIED** information/assets until the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country** has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Supplier / Respondent**, these tasks may be performed up to the level of **SECRET.**

12. The Foreign recipient **Supplier / Respondent** shall not use the **CANADA PROTECTED / CLASSIFIED** information/assets for any purpose other than for the performance of the **Request for Information** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

13. The Foreign recipient **Supplier / Respondent** visiting Canadian Government or industrial facilities, under this **Request for Information**, 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).

14. The Foreign recipient **Supplier / Respondent** 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 **Request for Information** has been compromised.

15. The Foreign recipient **Supplier / Respondent** 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 **Supplier / Respondent**, pursuant this **Request for Information**, have been lost or disclosed to unauthorized persons.

16. The Foreign recipient **Supplier / Respondent** 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).

17. The Foreign recipient **Supplier / Respondent** shall comply with the provisions of the International bilateral industrial security instrument between **the supplier's country** and Canada, in relation to equivalencies.

18. The Foreign recipient **Supplier / Respondent** must comply with the provisions of the Security Requirements Check List

19. In the event that a Foreign recipient **Supplier / Respondent** is chosen as a supplier for any resulting Contract, subsequent Country-Specific Foreign security requirement clauses shall be generated and promulgated by the Canadian DSA, and provided to the Government of Canada Contracting Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.

ANNEX F: APPLICATION OF THE INDUSTRIAL AND TECHNOLOGICAL BENEFITS (ITB) POLICY

The Industrial and Technological Benefits (ITB) Policy may be applied on the **Cyber Security Awareness (CSA)** project and the **Defensive Cyber Operations-Decision Support (DCO-DS)** 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 these procurements.

Please provide your written feedback to the questions listed below and any other comments regarding ITB Policy, including Value Proposition, to the PSPC Contracting Authority by the RFI response request date.

The ITB Policy, including Value Proposition

Under the ITB Policy, 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 make long-term investments in Canada by establishing or growing their presence in Canada, strengthening Canadian supply chains, and developing Canada's industrial capabilities.

The ITB Policy requires bidders to compete on the basis of providing economic benefits to Canada through a Value Proposition associated with each bid. Successful bidders are therefore selected on the basis of price, technical merit and their Value Proposition. After a contract is awarded, the contractor is required to begin fulfilling its ITB obligation and the commitments made through the Value Proposition.

The goal of the ITB Policy, including the Value Proposition, is to support the long-term sustainability of the Canadian defence sector, enhance the competitiveness and growth of Canadian-based suppliers, including small and medium-sized businesses, invest in research and technological development activities in Canada, and enable or enhance access to global markets for Canadian firms and exports of goods and services from Canada. There is flexibility within the ITB Policy to target other areas of investment on a procurement-by-procurement basis.

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

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. What Canadian capabilities could be used to directly support the production and delivery of the Cyber Security Awareness (CSA) and Defensive Cyber Operations-Decision Support (DCO-DS) solutions?

2. What percentage of direct work on the CSA and DCO-DS projects can be achieved in Canada?

For ITB definitions, please visit: http://www.ic.gc.ca/eic/site/086.nsf/eng/h_00011.html

Supplier Development, including Small and Medium-sized Businesses

The ITB Policy seeks to improve the competitiveness of Canadian companies, independent of the Contractor or Eligible Donors, by strengthening productivity, skills development, and the ability to overcome market challenges.

1. The Canadian cybersecurity industry comprises close to 1000 companies, most of which are small and medium-sized businesses (SMB). What opportunities are there to partner with Canadian SMB with less than 250 employees to perform direct work on the CSA and DCO-DS projects?

2. What types of investments should Canada incentivize that would produce maximum benefit to Canadian companies in the cybersecurity market (defence or commercial sector)?
    a. Examples:
        i. Creation of skills and training initiatives to attract and retain skilled workers (e.g.: coding and programming, network engineering, and software development and integration);
        ii. Investments in new capital equipment and resources;
        iii. Support for security certifications (e.g.: Top Secret, ITAR) for Canadian companies, especially small and medium-sized businesses;

3. 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 these procurements and work in other business areas)?

4. Apart from these procurements, in what other areas of production and service-provision do you see opportunities to assist cybersecurity SMBs to scale up, in order to respond to domestic and global demand?

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.

1. Are there opportunities to partner with Canadian post-secondary or publicly-funded research institutions to perform direct work on the CSA and DCO-DS projects?
2. What high-value R&D investments in Canada, either in the defence or commercial sectors, could Canada motivate bidders to make as a result of these procurements (e.g. cloud security, mobile security, security analytics)?
    a. What opportunities exist to incentivize investment in emerging cross-sectoral technologies where Canadian capabilities exist (e.g. quantum computing, augmented/virtual reality, artificial intelligence/machine learning)?
3. Is there potential to develop research consortia or centres of excellence in partnership with Canadian post-secondary or publicly-funded research institutions, and if so, what research areas might your company pursue?
    a. If not, what other research or development partnerships could be formed to support technology development in areas related to the CSA and DCO-DS projects?

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

5. 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 cyber sector?

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.

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

2. 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?

3. Please describe any high value export opportunities from Canada related to broader cybersecurity applications, whether commercial or defence, that can be leveraged as a result of this procurement.

Other Questions

1. In comparison to price and technical merit, Value Proposition typically has a weight of 10% of the overall bid evaluation. What is your view on the weighting of the Value Proposition for the CSA and DCO-DS projects?

2. Within the Value Proposition, what are your recommended minimum percentages of weighting for each of the Value Proposition pillars (defence, supplier development, R&D, export, and other—if applicable)?

Please provide your written feedback to these questions and any other comments regarding Industrial and Technological Benefits/Value Proposition to the PSPC Contracting Authority by the RFI deadline.

ANNEX G: RULES OF ENGAGEMENT

Introduction

These Rules of Engagement apply to the entire Engagement Process and in particular the one-on-one meetings. :

General Rules and Principles

1. An overriding principle of the industry early engagement is that it be conducted with the utmost of fairness and equity between all parties. No one person or organization shall not receive nor be perceived to have received any unusual or unfair advantage over the others.
2. These Rules of Early Engagement will apply beginning with the release of this RFI document and conclude with the release of the Request for Proposal.
3. The Engagement Process will consist of the Request for Information, One-on-One Meetings, Group Follow-up Meeting and a possible draft RFP and any other processes deemed necessary by the Procurement Authority.
4. In order to maximize the benefits of the Engagement Process, Canada may endeavor to solicit comments from participants on various issues raised.
5. One-on-one sessions and the Group-follow-up meeting are only available to participants who meet the security requirements.
6. Classified information may only be released to participants who meet the security requirements.
7. Any solutions, ideas or issues raised during the One-on-One sessions will be analyzed for further consideration by Canada.
8. A draft RFP for a final review before the official RFP is issued may be made available to participants meeting the security requirements.
9. Canada will not disclose proprietary or commercially sensitive information concerning a participant to other participants or third parties except and only to the extent required by law.
10. Potential respondents are advised that any information submitted to Canada in the engagement process may be used by Canada in the development of a competitive Request for Proposal.

Terms and Conditions

The following terms and conditions apply to the Engagement Process. In order to encourage open dialogue, participants agree to the following:

1. Participants are expected to discuss their views concerning the procurement, and to provide positive resolutions to the issues in question. All interested participants meeting the security requirements shall have equal opportunity to share their ideas and suggestions.
2. No electronic recordings, audio or visual, will be permitted during the one-on-one meetings.
3. Participants must provide to Canada advance notification if they plan to have legal representation at the one-on-one meeting. Canada reserves the right to decline any meetings which include legal representation.
4. Participants will NOT reveal or discuss any information to the MEDIA/NEWSPAPER regarding this requirement during this engagement process. If participants receive a question from the Media, participants are to direct the Media to contact the PSPC Media Relations Office at 819-956-2313.
5. **Participants are to direct inquiries and comments ONLY to the PSPC Contracting Authority** or authorized representatives of Canada, as directed in notices given by the Contracting Authority. Any

communication to unauthorized representatives of Canada may be subject to full disclosure by Canada on Buy and Sell.

6. Media cannot participate in the process. Media outlets are to direct all queries to the PSPC Media Relations Office.
7. Canada is not obligated to issue any RFP, or to negotiate any contract for the projects.
8. If Canada does release a RFP, the terms and conditions of the RFP shall be subject to Canada's absolute discretion.
9. Canada will not reimburse any person or entity for any cost incurred in participating in this industry engagement process.
10. Participation is not a mandatory requirement. Not participating in this engagement process will not preclude a bidder from submitting a proposal when the final RFP is released.
11. Draft documentation (RFP, Evaluation Plan, SOW) will be released to Participants who meet the security requirements for comments.
12. Lobbyists will not be permitted to participate in the engagement process.
13. By informal discussion and good faith negotiation, PSPC and the participant shall make all reasonable efforts to resolve any dispute, controversy or claim, arising out of or in any way connected with this Industry Engagement.

ANNEX H: UNCLASSIFIED INDUSTRY DAY DETAILS AND REGISTRATION

Introduction

All interested industry respondents are invited to attend a unclassified group presentation to industry that will be conducted in the National Capital Region, Ottawa, ON, on the date specified in Table 1 - Procurement / Engagement Activity and Related Dates. This Industry Day will allow Department of National Defence project staff to present an overview of the two projects and to obtain industry input and allow industry to ask questions to PSCP, DND and ISED. The Industry Day will be conducted at the UNCLASSIFIED level. Suppliers who do not attend the Industry Day are still welcome to submit a response to this RFI.

Industry Day Details

Date: February 26, 2018
Time: 9:00 – 12:00 AM
Location: WOs&Sgts Mess, 4 Queen Elizabeth Dr., Ottawa

Registration Deadline: February 16, 2018

Suppliers are requested to arrive thirty minutes prior to Industry Day opening remarks in order to facilitate sign-in.

Registration Process

Interested suppliers are encouraged to register for the Industry Day no later than the Industry Day Registration Deadline. To register suppliers **must submit**, to the PSPC Contracting Authority identified below the following information:

- Number of people to attend the Industry Day
- Name and corporate title of each participant
- Point of contact email and phone number

Please note that:

a. Due to the space constraints of the location each interested supplier may only register up to two (2) representatives to attend the Industry Day.
b. The names of all attendees may be published after the Industry Day.

By participating in the Industry Day and/or One-on-One sessions and/or Group Follow-up Meeting, attendees agree to the Rules of Engagement detailed in Annex G.

Attendees are responsible for their own transportation, accommodation, meals parking and all other expenses.

Contracting Authority for the Industry Day

Caroline Labrie
Public Services and Procurement Canada
Place du Portage III, 8C2
11 Laurier Street Gatineau, Quebec K1A 0S5
819-420-5725

TPSGC.*PADivisionQE-APQEDivision*.PWGSC@tpsgc-pwgsc.gc.ca

The use of email to communicate is preferred.

Information Prior to Industry Day

Suppliers may provide comments or questions in either official language by submitting their information, in writing, to the Contracting Authority identified above.

Communication with Industry

Canada will document all Industry Day concerns/issues, questions, suggestions, together with their responses. During the engagement process, the PSPC Contracting Authority may choose to communicate with registered suppliers through direct email rather than posting additional notices on Government Electronic Tendering Service. To ensure the fairness, transparency and integrity of the Process, PSPC will share information resulting from the process (excluding proprietary and/or confidential information) with Industry.

The presentation made by Canada, responses to questions raised during the Industry Day, and the list of attendees will be published on the Government Electronic Tendering Service after the event.

Language

Documents will be available in both official languages.

ANNEX I: CLASSIFIED ONE-ON-ONE MEETING AND GROUP FOLLOW-UP MEETING DETAILS AND REGISTRATION

Introduction

The intention of the one-on-one meetings and group follow-up session is to distribute and present Annex C and hold classified discussions. Annex C provides an overview of the current concept of operations and in-service capabilities and is classified. The follow-up group meeting will be held to present and distribute classified questions and answers generated during the one-on-one meetings. **As the one-one-one meeting and any resulting follow-up group meeting includes classified information those attending and leaving with classified information must meet the security requirements detailed in Annex E.** Security clearances will be confirmed with the Canadian Industrial Security Directorate (CISD) or through the International Industrial Security Directorate (IISD) for foreign suppliers upon registration.

Annex C will also 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. Details on how to register under the CGP are available at: http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html

Suppliers are advised that although Annex C and its presentation at the one-on-one meeting will provide more granularity to DND requirements it is not required to provide a fulsome response to the RFI. Suppliers are not required to attend a one-on-one meeting or the group follow-up meeting. Suppliers who do not attend are still welcome to submit a response to this RFI.

One-on-one Meeting Details

Date: February 26, 2018 – March 2, 2018
Time: 1 hour time slots through-out the week beginning February 26, 2018.
Location: National Defence Headquarters, 101 Colonel By Drive, Ottawa

Suppliers are requested to arrive thirty minutes prior to their meeting time in order to facilitate sign-in.

Group Follow-up Meeting Details

Date: Will be announced at the Industry Day
Time: TBD - the week of March 5, 2018
Location: National Defence Headquarters, 101 Colonel By Drive, Ottawa

Suppliers are requested to arrive thirty minutes prior to Group Meeting in order to facilitate sign-in.

Registration Process

Interested suppliers must register for the One-one-one meetings no later than the One-on-one Registration Deadline listed in Table 1 - Procurement / Engagement Activity and Related Dates. One-on-one meetings and Group Follow-up meeting will be held at a Department of National Defence secure facility in the National Capital Region. Registration for one-on-one meetings will be conducted on a first come first serve basis, however, DND and supplier availability, confirmation of security clearances, visit requests etc. will affect the scheduling of the meeting dates. As the meetings will be held at a Department of National Defence facility a Visitor Clearance Request (VCR) is also required.

To register suppliers **must submit**, to the PSPC Contracting Authority identified below the following:

- Number of people to attend the meeting
- Name, corporate title and citizenship of each participant
- Point of contact email and phone number
- Controlled Goods Program registration number or written proof of exemption or exclusion of the supplier and of any other person to whom the supplier will give access to Annex C.
- Sign the corporate and individual Non-Disclosure Agreement in the form set out in Attachment 1 to this Annex and return to the Contracting Authority.

Please note that:

a. Further corporate and personal information will be required to confirm the security clearances and complete the DND Visitor Clearance Request (VCR).
b. Due to the space constraints of the location each interested supplier may only register up to four (4) representatives to attend the one-on-one meeting and up to two (2) suppliers to attend the Group Follow-up meeting.
c. The names of all attendees may be published after the Industry Day.

By participating in the Industry Day and/or One-on-One sessions and/or Group Follow-up Meeting, attendees agree to the Rules of Engagement detailed in Annex G.

On confirmation of security clearance credentials, the Contracting Authority will contact the supplier to confirm meeting location, date and time.

Attendees are responsible for their own transportation, accommodation, meals parking and all other expenses.

Process for Receipt and Transport of Annex C and Classified Questions and Answers

Annex C of this RFI and classified questions and answers resulting from the one-on-one meetings contains classified information that is only releasable to respondent companies that meet the security requirements detailed in Annex E. A hard copy of Annex C will be distributed at the one-on-one meetings, and if requested in the group follow-up meeting. A hard copy of the classified questions and answers will be distributed at the group follow-up meeting.

As advised previously **Prior** to the meeting suppliers should to refer to The Industrial Security Manual for guidance on the handling of classified documents as they **must** be compliant with the security requirements set out in this manual:
https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-eng.html

If a supplier intends to retain and transport the hard copy of Annex C and the classified questions and answers they must submit a written request to hand carry to documents to the Contracting Authority detailed below. The Contracting Authority will engage with DND, the Canadian Industrial Security Directorate (CISD) or the International Industrial Security Directorate (IISD) to process the request. As the approval process can take a number of weeks suppliers are advised to submit their request as soon as possible.

Contracting Authority for the One-on-One Meetings and Group Meeting

Patti Wight
Public Services and Procurement Canada

11 Laurier, Gatineau, Canada K1A 0S5
819-420-1757

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

The use of email to communicate is preferred.

Communication with Industry

Canada will document all one-on-one meeting concerns/issues, questions, and suggestions, and responses. During the engagement process, the PSPC Contracting Authority may choose to communicate with registered suppliers through direct email rather than posting additional notices on Government Electronic Tendering Service. To ensure the fairness, transparency and integrity of the Process, PSPC will share information resulting from the process (excluding proprietary and/or confidential information) with Industry.

Unclassified responses to unclassified questions raised during the one-on-one meetings as well as the list of meeting attendees will be published on the Government Electronic Tendering Service after the group follow-up meeting.

Language

Documents will be available in both official languages.

ATTACHMENT 1: NON – DISCLOSURE AGREEMENT

CORPORATE

NON-DISCLOSURE AGREEMENT FOR PARTICIPATION IN SOLICITATION PROCESS

PWGSC FILE #'s W636917DE25 and W636917DE26 – PHASE I

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 Annex A. 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 Annexes B and C (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: _____

ANNEX A

INDIVIDUAL

NON-DISCLOSURE AGREEMENT FOR PARTICIPATION IN SOLICITATION PROCESS

PWGSC FILE #'s W636917DE25 and W636917DE26 – PHASE I

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 Annexes B and C (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: _____	

ANNEX C

PWGSC FILE#'s W636917DE25 and W636917DE26 – PHASE I for International suppliers

Protected A, Protected B, Confidential, Secret,

The contractor and/or any and all subcontractors must be from a country with which Canada has an international bilateral industrial security instrument or will have such an instrument with Canada by the end of the bidding period. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html

All **CANADA PROTECTED / CLASSIFIED** information/assets, furnished to the Foreign recipient **Supplier/Respondent**, shall be safeguarded as follows:

1. The Foreign recipient **Supplier / Respondent** shall, at all times during the performance of the **Request for Information**, hold a valid Facility Security Clearance (FSC), issued by the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country**, at the equivalent level of **SECRET**, and hold an approved Document Safeguarding Capability Clearance at the level of **SECRET.**
2. All **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated under this **Request for Information** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Request for Information**, in accordance with the national policies of **the supplier's country.**
3. The Foreign recipient **Supplier / Respondent** 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 supplier's country**.
4. All **CANADA PROTECTED / CLASSIFIED** information/assets provided to the Foreign recipient **Supplier / Respondent** pursuant to this **Request for Information** by the Government of Canada, shall be marked by the Foreign recipient **Supplier / Respondent** with the equivalent security classification utilized by **the supplier's country** and in accordance with the national policies of **the supplier's country**.
5. The Foreign recipient **Supplier / Respondent** shall, at all times during the performance of this **Request for Information**, ensure the transfer of **CANADA PROTECTED / CLASSIFIED** information/assets be facilitated in accordance with the national policies of **the supplier's country**, and in compliance with the provisions of the Bilateral Industrial Security Instrument between **the supplier's country** and Canada.
6. Upon completion of the work, the Foreign recipient **Supplier / Respondent** shall return to the Government of Canada, via government-to-government channels, all **CANADA PROTECTED / CLASSIFIED** information/assets furnished or produced pursuant to this **Request for Information**, including all **CANADA PROTECTED / CLASSIFIED** information/assets released to and/or produced by its subcontractors.
7. Throughout the duration of this **Request for Information**, the Foreign recipient **Supplier / Respondent** 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 **Request for Information** 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 **Supplier / Respondent**, as part of this **Request for Information**. The *Defence Production Act* defines Canadian Controlled Goods (S.35).
8. The **Request for Information** involves access to Unclassified military data, which is subject to the Provisions of the Technical Data Control Regulations. The UNITED STATES of AMERICA recipient **Supplier / Respondent** is required to become a certified contractor in the US/Canada Joint Certification Program (JCP).
9. Such **CANADA PROTECTED and CLASSIFIED** information/assets shall be released only to foreign recipient **Supplier / Respondent** personnel who have a need to know for the performance of the **Request for Information**, must be a citizen of **Australia, the United Kingdom, 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 supplier's country.**
10. **CANADA PROTECTED / CLASSIFIED** information/assets provided or generated pursuant to this **Request for Information** shall not be further provided to a third party Foreign recipient supplier 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 Supplier 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 supplier's country**, if the third-party Foreign recipient Supplier is located in a third country.

11. The Foreign recipient **Supplier / Respondent** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system any **CANADA PROTECTED / CLASSIFIED** information/assets until the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country** has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Supplier / Respondent**, these tasks may be performed up to the level of **SECRET.**

12. The Foreign recipient **Supplier / Respondent** shall not use the **CANADA PROTECTED / CLASSIFIED** information/assets for any purpose other than for the performance of the **Request for Information** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

13. The Foreign recipient **Supplier / Respondent** visiting Canadian Government or industrial facilities, under this **Request for Information**, 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).

14. The Foreign recipient **Supplier / Respondent** 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 **Request for Information** has been compromised.

15. The Foreign recipient **Supplier / Respondent** 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 **Supplier / Respondent**, pursuant this **Request for Information**, have been lost or disclosed to unauthorized persons.

16. The Foreign recipient **Supplier / Respondent** 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).

17. The Foreign recipient **Supplier / Respondent** shall comply with the provisions of the International bilateral industrial security instrument between **the supplier's country** and Canada, in relation to equivalencies.

18. The Foreign recipient **Supplier / Respondent** must comply with the provisions of the Security Requirements Check List

19. In the event that a Foreign recipient **Supplier / Respondent** is chosen as a supplier for any resulting Contract, subsequent Country-Specific Foreign security requirement clauses shall be generated and promulgated by the Canadian DSA, and provided to the Government of Canada Contracting Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.

ANNEX B

PWGSC FILE # SRCL - W636917DE25 and W636917DE26 – PHASE I for Canadian Suppliers

1. The supplier/respondent must, at all times during the performance of the request for information, 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).

2. This request for information includes access to controlled goods. Prior to access, the supplier/respondent must be registered in the Controlled Goods Program of Public Works and Government Services Canada.

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

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

5. Processing of CLASSIFIED information electronically at the Contractor/Offeror's site is NOT permitted under this Request for Information.

6. The supplier/respondent must comply with the provisions of the:

a) Security Requirements Check List and security guide (if applicable)
b) *Industrial Security Manual* (Latest Edition).

ANNEX J: REQUEST FOR SECURITY SPONSORSHIP

Introduction

As the RFI contains a classified Annex and as the Draft RFP, final RFP and resulting contract may also contain classified information one of the key purposes of this RFI is to provide direction and assistance to interested suppliers who do not meet the security requirements detailed in Annex E in obtaining those clearances.

Sponsorship Request for Phase 1 – Phase 3 (RFI – RFP)

Suppliers whose organizations currently do not hold a valid SECRET level Facility Security Clearance (FSC), nor a valid SECRET level Document Safeguarding issued by PSPC's Canadian Industrial Security Directorate (CISD), are encouraged to initiate the security clearance process immediately. Requests for sponsorship can be sent to the PSPC Contacting Authority below via e-mail.

Prime Contracting Authority for Security Sponsorship

Caroline Labrie
Public Services and Procurement Canada
11 Laurier, Gatineau, Canada K1A 0S5
819-420-5725
TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

The use of email to communicate is preferred.

It is the responsibility of the supplier to ensure that the information required concerning the security clearance is provided on time to either the requesting authority or CISD. The request should include the following information:

a) Legal name of the company:
b) Business Name, if different from legal name:
c) Mailing address:
d) Civic address, if different from mailing address:
e) Company telephone number:
f) Company fax number:
g) Surname and Given Name of the contact person (Canadian Official):
h) Title of the contact person:
i) Telephone number of the contact person:
j) E-mail address of the contact person:
k) Language preference (English or French);

Upon receipt of a request for sponsorship, CISD will contact the Potential Bidder to complete the gathering of required information.

For any inquiries concerning any security requirements, the supplier should contact CISD at 1-866-368-4646, or (613) 948-4176 in the National Capital Region. CISD Website: http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html

There are no direct costs charged to suppliers wishing to obtain a Facility Security Clearance (FSC). However, the suppliers may incur indirect costs, which results from being required to meet the minimum standards such as installing mechanisms for document safeguarding, if applicable.

Sponsorship Request for Phase 4 (Contract Award)

As the Security Requirements for Phase 4 have not yet been finalized PSPC is **not currently** sponsoring the upgrade to the clearances detailed below. Once the security requirements have been finalized the RFI may be amended to include the security sponsorship of suppliers for the clearances detailed below.

Upon contract award, the selected supplier will be provided access to information that collectively is classified at TOP SECRET (SIGINT), releasable to Canadian Citizens only. At this time, it is estimated that the selected Prime Contractor must, at a minimum, hold the following mandatory facility security clearances:

1) TOP SECRET (SIGINT) for Personnel Assigned, limited to personnel who hold citizenship from Canada; and

2) SECRET and NATO SECRET for Document Safeguarding, with specific Information Technology Security requirements.