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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet CD-DAR Draft ITQ	
Solicitation No. - N° de l'invitation W6369-20CY06/A	**Date** 2020-07-09
Client Reference No. - N° de référence du client W6369-20CY06	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-049-27831
File No. - N° de dossier 049qe.W6369-20CY06	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-08-18**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. Specified Herein - Précisé dans les présentes **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☑	
Address Enquiries to: - Adresser toutes questions à: See herein	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone ( ) - ( )	**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

Cyber Defence – Decision Analysis and Response (CD-DAR) Project

Draft Invitation to Qualify

This notice provides the opportunity for interested suppliers to submit their written feedback on the draft Invitation to Qualify (ITQ) before Canada releases the final ITQ.

This opportunity for written feedback to Canada is neither a call for tender nor a Request for Proposal (RFP) and is not to be considered in any way a commitment by Canada, nor as authority to potential respondents to undertake any work that could be charged to Canada. Participation in this opportunity for written feedback is not a condition or prerequisite for responding to any subsequent ITQ.

All enquiries and other communications related to this notice, including the feedback on the draft ITQ, are to be submitted in writing to the attention of the Public Services and Procurement Canada (PSPC) Contracting Authority, using the Project's e-mail address below:

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

Interested suppliers are requested to provide their feedback as early as possible. Feedback received after the closing date and time may not be considered.

Invitation to Qualify (ITQ)

FOR THE
CYBER DEFENCE – DECISION ANALYSIS AND RESPONSE

ITQ NO, W6369-20-CY06

Table of Contents

1. General Information

1.1 Introduction

Purpose of this Invitation to Qualify (ITQ): The Cyber Defence – Decision Analysis and Response (CD-DAR) project is the amalgamation of the Cyber Security Awareness (CSA) and Defensive Cyber Operations – Decision Support (DCO-DS) projects. The purpose of this Invitation to Qualify (ITQ) issued by Public Services and Procurement Canada (PSPC)[1] is to qualify Suppliers that have the ability to provide a CD-DAR capability to proceed to the subsequent phases of the procurement process. A more detailed overview of the agile and collaborative procurement process is provided in section 1.3 and Annex E.

This ITQ is not a Bid Solicitation: This ITQ process is not a solicitation of bids or tenders. No contract will be awarded as a result of the activities during the ITQ phase. Canada reserves the right to cancel any of the qualification requirements included as part of the Project at any time during the ITQ phase. Given that the ITQ process may be partially or completely cancelled by Canada, it may not result in any of the subsequent procurement process described in this document. Pre-qualified Suppliers may withdraw from the procurement process at any time. Therefore, Pre-qualified Suppliers can choose not to bid on any subsequent solicitation.

1.2 Overview of the Project

a) **Background:** The Department of National Defence (DND) / Canadian Armed Forces (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.

CD-DAR project aligns with *Strong, Secure, Engaged*: Canada's Defence Policy initiative #65 which cites DND/CAF has committed to "*improving cryptographic capabilities, information operations capabilities, and cyber capabilities to include: cyber security and situational awareness projects, cyber threat identification and response, and the development of military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."* [2]

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 the CD-DAR project within the DND/CAF cyber force development program focuses on addressing these requirements. CD-DAR is the single project created by the amalgamation of the CSA and DCO-DS projects.

[1] The legal name of the Department is "Department of Public Works and Government Services". "Public Services and Procurement Canada" and "PSPC" as well as "Public Works and Government Services Canada" and "PWGSC" are the common usage names.

[2] Strong, Secure, Engaged: Canada's Defence Policy Initiative #65.

b) **Project Overview:** Through the CD-DAR Project DND/CAF will acquire defensive cyber solutions (translated into capabilities) to improve overall decision support and security of the DND/CAF cyberspace, including the ability to detect, analyze and respond to threats. The integrated CD-DAR capability must provide reliable contextual analysis to support DND/CAF decisions and actions within designated Command Network (Comd-Net) Extensions and Interfaces, and deployable Defence Wide Area Network (DWAN) systems. Ultimately, the CD-DAR capability will enable the CAF Cyber Force to defend the CAF's freedom of action and interests in cyberspace in support of CAF missions and operations. Notwithstanding, CD-DAR must be designed to enable scalability to additional networking environments as and when appropriate.

The project moved into the Definition Phase in June 2020.

Further details on the Project requirements, objectives and outcomes, and scope can be found in Annex A: Preliminary Statement of Operational Requirements (PSOR).**Scope of Anticipated Procurement:**

i) **Potential Clients:** This ITQ is being issued by PSPC. It is intended that the contract(s) resulting from any subsequent solicitation would be used by DND to fulfill the requirements of the CD-DAR project.

ii) **Number of contracts**: PSPC is currently contemplating the award of at least one (1) contract.

iii) **Term of contract**: PSPC will identify the term of any resulting contract and any options associated, once the procurement progresses to the Request for Proposal (RFP) phase.

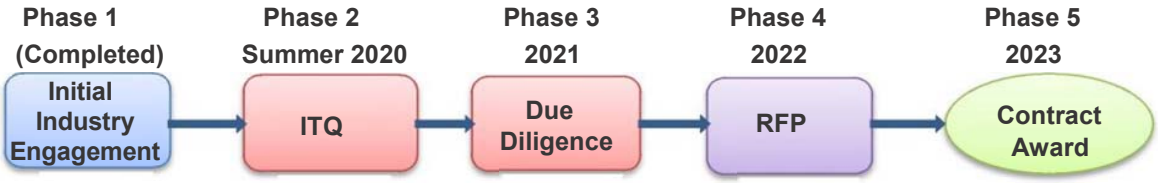
d) **Controlled Goods Program:** This procurement is subject to the Controlled Goods Program. The Defence Production Act defines Canadian Controlled Goods as certain goods listed in Canada's Export Control List, a regulation made pursuant to the Export and Import Permits Act (EIPA)."

e) **Financial Capability:** SACC Manual clause A9033T (2012-07-16), Financial Capability, will apply to the RFP.

1.3 Overview of the Planned Procurement Process

This ITQ is the second phase in the procurement process for the Project. Although the procurement process remains subject to change (and even to cancellation, in accordance with PWGSCs' Standard Instructions), Canada currently anticipates undertaking the multi-phase agile and collaborative procurement process detailed below.

CD-DAR Planned Procurement Process and Timeline



Activities per phase include:

LOI	**Draft ITQ**	**Draft RFP**	**RFP**
RFI	**ITQ**	**Bidders Conference**	
Industry Day		**One-on-one Meetings**	
One-on-one Meetings			

a) **Phase 1– Initial Engagement with Industry (completed)**

PSPC and DND commenced its industry engagement by releasing LOIs for DCO-DS and CSA in 2016 and followed by a RFI in 2017. An Industry Day and classified one-on-one meetings were held in the spring of 2018. This was done with the objective of obtaining feedback on the operational and technical requirements, cost and schedule, and Industrial and Technological Benefits. Supplier feedback from these industry engagement activities was of great assistance to Canada and resulted in DND/CAF moving forward with the CD-DAR Project

b) **Phase 2 – Invitation to Qualify**

Draft ITQ: This draft ITQ is the commencement of the second phase in the procurement for the CD-DAR project. Suppliers are invited to submit written questions and comments on this draft ITQ. Questions and Responses will be posted on Buy and Sell.

Formal ITQ: The ITQ will be used to pre-qualify suppliers to participate in the subsequent Due Diligence and RFP Phase and any other potential phases of the procurement process. Suppliers are invited to pre-qualify in accordance with the terms and conditions of this ITQ. Only Pre-qualified Suppliers will be permitted to bid on any subsequent solicitation issued as part of the procurement process.

c) **Phase 3 – Due Diligence**

PSPC will be conducting the Due Diligence Phase only with the Pre-qualified Suppliers as determined in the Qualification Phase (Phase 2 – Invitation to Qualify). The objective of the Due Diligence Phase is to further refine the CD-DAR requirements by obtaining feedback from Pre-qualified Suppliers, addressing industry's concerns and considering industry best practices prior to issuing the final bid solicitation. Activities during the Due Diligence Phase are as follows:

Draft RFP: It is anticipated that Pre-qualified Suppliers will be engaged to provide feedback on the Draft RFP documents, including system information, draft Statement of Requirements (SOR) and draft Evaluation Criteria. Components of the Draft RFP will be classified and only available to those Pre-qualified Suppliers that meet the RFP security requirements detailed in

Annex C. Pre-qualified Supplier not meeting the security requirements will only have access to the non-classified components of the draft RFP. The unclassified components of the Draft RFP will also be published on Buy and Sell to allow for non-qualified suppliers to also provide feedback. Canada will review and respond this to feedback when possible and publish the results on Buy and Sell.

Classified Bidders Conference and Classified One-on-one Meetings with Pre-qualified Suppliers: A Bidders Conference and one-on-one meetings with Pre-qualified Suppliers will be held to discuss specific issues relating to the content of the Draft RFP documents. Further details regarding the Due Diligence Phase will be provided to Pre-qualified Suppliers through the Draft RFP process. And finally, a review of Industry's feedback will be considered in finalizing the RFP post Draft RFP process. Participation in the classified bidders conference and classified one-on-one meeting is only available to those Pre-qualified Suppliers that meet the RFP security requirements detailed in Annex C.

d) **Phase 4 - Request for Proposals (RFP)**

PSPC anticipates releasing a RFP to those Pre-qualified Suppliers who remain qualified at the time the RFP is released and who meet the RFP Security Requirements detailed in Annex C. If a supplier fails to meet the RFP security requirements on the date the RFP is issued they will be removed from the list of Pre-qualified Suppliers. The unclassified components of the RFP will also be published on Buy and Sell to inform non-qualified suppliers. When possible Canada will review and respond to feedback from non-qualified suppliers and publish the results on Buy and Sell.

e) **Phase 5 - Contract Award**

PSPC anticipates awarding a contract to the winning supplier in accordance with the terms of the RFP.

1.4 Debriefings

The Contracting Authority will notify unsuccessful Suppliers after the Pre-Qualification Phase and provide a debriefing upon request. The unsuccessful Suppliers should make the request to the Contracting Authority within 15 working days from receipt of the results of the Qualification Phase. Debriefings may be in writing, by telephone or in person. The Contracting Authority is to determine which method will be the most effective.

1.5 National Security Exception

The national security exceptions provided for in the trade agreements have been invoked; therefore, this procurement is excluded from all of the obligations of all the trade agreements.

1.6 Industrial and Technological Benefits

The **Industrial and Technological Benefits (ITB) Policy** will apply to the Cyber Defence - Decision Analysis and Response (CD-DAR) project. 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 includes the Value Proposition, which requires bidders to compete based on the economic benefits to Canada associated with its bid. Winning bidders are selected based on price, technical merit and their

Value Proposition. Value Proposition commitments made by the winning bidder become contractual obligations in the ensuing contract. To maximize the economic benefits that can be leveraged through the Value Proposition, Canada will use the Value Proposition to motivate Prime Contractors to invest in **Key Industrial Capabilities (KICs)**, such as Cyber Resilience and Artificial Intelligence. As emerging technologies, these KICs are areas with the potential for rapid growth and innovation. As a result, Canada will be seeking to foster opportunities in these emerging technologies by motivating partnerships and investments with industry and post-secondary institutions that promote skills development and research and development

Canada will engage with Pre-qualified Suppliers as we develop the requirements for the ITB Value Proposition.

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

1.7 Consultants

a) Canada may engage consultants in the future at its sole discretion, for the purposes of the CD-DAR Project.

b) Canada will share with consultants, on a need to know basis, information and documents provided to Canada, which may include those of Pre-qualified Suppliers, as part of the procurement process.

c) Consultants are required to sign non-disclosure agreement(s) before gaining access to the Project information and documents as part of this procurement process.

1.8 Conflict of Interest or Unfair Advantage

As set out in the provisions of the Standard Instructions – Goods or Services – Competitive Requirements 2003 (2019-03-04), a response can be rejected due to an actual or apparent conflict of interest or unfair advantage.

In this regard, Canada advises that it has used the services of a number of private sector consultants/contractors in preparing strategies and documentation related to this procurement process, including the following:

Contractors:

i. Modis Canada;
ii. Veritaaq; and
iii. Procom.

Resources (Past and Present):

i. Marc Lessard;
ii. Paris Lampsos;
iii. Maurice Tremblay;
iv. Peter Ng; and
v. Stuart Morrison.

1.9 Fairness Monitor

Canada has engaged *The Public Sector Company* as a fairness monitor for this procurement. The fairness monitor will, for example, observe the evaluation of responses to determine whether PSPC has adhered to the evaluation process described in the solicitation. The fairness monitor is under obligations pursuant to its contract with Canada to maintain the confidentiality of all information received as a result of its participation in this procurement process.

2. Instructions for Respondents

2.1 Standard Instructions, Clauses and Conditions

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

b) Firms who submit a response agree to be bound by the instructions, clauses and conditions of the ITQ.

c) The 2003 (2020-05-28) Standard Instructions – Goods or Services – Competitive Requirements, are incorporated by reference into and form part of the ITQ, except that:

i) Wherever the term “bid solicitation” is used, substitute “Invitation to Qualify”;

ii) Wherever the term “bid” is used, substitute “Response”; and

iii) Wherever the term “Bidder(s)” is used, substitute “Respondent(s)”;

d) Subsection 05(4), which discusses a validity period, does not apply, given that this ITQ invites firms to qualify. Canada will assume that all firms who submit a Response wish to continue to qualify unless they advise the Contracting Authority that they wish to withdraw their Response;

e) Delete subsection 01 – Integrity Provisions – Bid;

f) Delete subsection 14 – Price Justification; and

g) By submitting a response, the Respondent is confirming that it agrees to be bound by all the instructions, clauses and conditions of the ITQ.

h) The Phased Bid Compliance Process applies to this requirement.

2.2 Submission of Only One Response

a) A Respondent can be an individual, a sole proprietorship, a corporation, a partnership, or a joint venture.

b) Each Respondent (including related entities) will be permitted to qualify only once. If a Respondent or any related entities participate in more than one response (participating means being part of the Respondent, not being a subcontractor), Canada will provide those Respondents with 2 working days to identify the single response to be considered by Canada. Failure to meet this deadline may result in all the affected responses being disqualified or in Canada choosing, in its discretion, which of the responses to evaluate.

c) For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity is an individual, corporation, partnership, etc.) an entity will be considered to be “related” to a Respondent if:

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

ii) the entity and the Respondent are “related persons” or “affiliated persons” according to the Canada *Income Tax Act*;

iii) the entity and the Respondent have now or in the two years before the ITQ closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

iv) the entity and the Respondent otherwise do not deal with one another at arm’s length, or each of them does not deal at arm’s length with the same third party.

d) A Respondent may act as a subcontractor to another Respondent. However, subcontractors may not be permitted to participate in the Due Diligence phase with the Qualified Respondent for whom they will be doing subcontracting work.

e) Any individual, sole proprietorship, corporation, or partnership that is a Respondent as part of a joint venture cannot submit another response on its own or as part of another joint venture.

Example 1: Supplier A does not itself have all the experience required by the ITQ. However, Supplier B has the experience that Supplier A lacks. If Supplier A and Supplier B decide to team up to submit a response together as a joint venture, both entities are together considered the Respondent. Neither Supplier A nor Supplier B can team up with another supplier to submit a separate response, because each is already part of a Respondent.

Example 2: Supplier X is a Respondent. Supplier X’s subsidiary, Supplier Y, decides to team up with Supplier Z to submit a response as a joint venture. Suppliers Y and Z, as well as Supplier X, will all be asked to determine which one of the two responses will be considered by Canada. Both responses cannot be submitted, because Supplier Y is related to Supplier X as an affiliate.

f) By submitting a response, the Respondent is certifying that it does not consider itself to be related to any other Respondent.

2.3 Applicable Laws

The relations between the parties will be governed by the laws in force in the Province of Ontario.

A Respondent may, at its discretion, substitute the applicable laws of a Canadian province or territory of its choice without affecting the validity of its response, by inserting the name of the Canadian province or territory of its choice in the ITQ Submission Form (Annex D). If no other province or territory is specified, the Respondent agrees that the laws of Ontario are acceptable to it.

2.4 Questions, Comments and Communications

a) **Single Point of Contact:** To ensure the integrity of the competitive procurement process, questions and other communications regarding this ITQ must be submitted in writing and directed only to the Contracting Authority at the email address below:

Contracting Authority
Public Services and Procurement Canada
Laurie Stewart

Email address: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

b) **Deadline for Asking Questions:** All questions and comments regarding the solicitation must be submitted by email to the Contracting Authority no later than 5 calendar days before the ITQ closing date. Questions received after that time may not be answered.

c) **Content of Questions:** Respondents should reference as accurately as possible the numbered item of the ITQ to which the question relates. Respondents should explain each question in sufficient detail in order to allow Canada to provide an accurate answer. Any questions that a Respondent believes include proprietary information must be clearly marked “proprietary” at each relevant item. Items identified as proprietary will be treated as such unless Canada determines that the question is not of a proprietary nature. Canada may edit the questions or may request that the Respondent do so, so that the proprietary nature of the question is eliminated, and the edited question and answer can be provided to all Respondents. Questions not submitted in a form that can be provided to all Respondents may not be answered by Canada.

d) **Publication of Answers:** To ensure consistency and quality of information provided to Respondents, the questions and answers will be posted on the Government Electronic Tendering Service (GETS) BuyandSell.gc.ca as an amendment to the ITQ.

2.5 Rights of Canada

In addition to any other rights described in this ITQ, Canada reserves the right, at its sole discretion, to:

a) amend this ITQ, including the qualification criteria, at any time;

b) cancel this ITQ at any time;

c) reissue the ITQ;

d) if no Respondents are qualified and the requirement is not substantially modified, reissue the ITQ by inviting only those Respondents who submitted responses to the ITQ to submit new responses within a period designated by Canada;

e) reject and not consider further a response if, in Canada’s opinion, any component of the response presents potential, perceived or real issues or matters that may be injurious to the national security of Canada;

f) remove at any time, any Qualified Respondent, if it presents potential, perceived or real issues that may be injurious to the national security of Canada; and

g) at any time during Phase3 – Due Diligence, suspend Phase 3 and re-open Phase 2 – ITQ.

2.6 Security Requirements

a) As the CD-DAR project advances through the different procurement phases, security requirements evolve and largely increase.

b) A Respondent is not required to have a security clearance in order to become a Pre-qualified Supplier, however there will be required security clearances and other security requirements at the next phases of the procurement process.

c) In order to be invited to the Bidder Conference (which is the commencement of the Due Diligence Phase) and classified one-on-one meetings, Pre-qualified Suppliers must meet the Security Requirements detailed in Annex C, Section 1.2 Security Requirements for Phase 3 – Due Diligence.

d) When Canada is prepared to invite Pre-qualified Suppliers to the Bidder Conference and classified one-on-one meeting (dates to be determined), the PSPC Contracting Authority will contact the Industrial Security Program to verify each Pre-qualified Suppliers' clearances. Those Pre-qualified Suppliers who do not hold the appropriate clearances at that time will be contacted and advised that they cannot participate.

e) There will be additional security requirements for the final RFP and Contract. Anticipated security requirements for the final RFP and Contract are also outlined in Annex C. Pre-qualified Suppliers that do not meet the security requirements for the Final RFP as detailed in Annex C Section 1.2 on the date the final RFP is released will be removed from the list of Pre-qualified Suppliers.

Pre-qualified Suppliers that do not currently have personnel and organization security clearances through the Canadian federal government or their respective domestic Industrial Security Program, or Suppliers that do not meet the anticipated security requirements outlined in Annex C, should begin the clearance process early by contacting the Industrial Security Program (ISP) of PWGSC (https://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html) website.

3. Preparing and Submitting a Response

3.1 Language for Future Communications

Each Respondent is requested to identify, in its Response Submission Form, which of Canada's two official languages it chooses to use for future communications with Canada regarding this ITQ and any subsequent phases of the procurement process.

Should all suppliers who qualify under this ITQ choose the same official language Canada may choose to conduct future communications and procurement phases with those pre-qualified suppliers only in that official language.

3.2 Content of Response

A complete response to this ITQ consists of all of the following:

a) **Response Submission Form at Annex D (Requested at ITQ Closing)**: Respondents are requested to include the Response Submission Form, found at **Annex D**, with their responses. It provides a common form in which Respondents can provide information required for evaluation, such as a contact name, the Respondent's Procurement Business Number, the language for future communications with Canada about this procurement process, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information requested by the Response Submission Form is incomplete or requires correction, Canada will provide the Respondent with an opportunity to provide the additional information or make the correction. Providing the information when requested during the evaluation period is mandatory.

b) **Responses to the Qualification Requirements at Annex B – Evaluation Criteria (Mandatory at ITQ Closing)**: The Supplier's mandatory response must substantiate its compliance with and address clearly and in sufficient depth the mandatory criteria that are subject to evaluation in Annex B - Evaluation Criteria. Each of the Mandatory Evaluation Criteria must be addressed in sufficient detail to permit the evaluation team to verify the Supplier's compliance. Simply repeating the statement contained in the ITQ is not sufficient. In order to facilitate the evaluation of the response, Canada requests that Suppliers address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Suppliers may refer to different sections of their responses by identifying the specific paragraph and page number where the subject topic has already been addressed.

3.3 Electronic Submission of Response

a) Responses must be submitted only to the Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time indicated on page 1 of this ITQ.

a) Only bids submitted using epost Connect service or facsimile will be accepted. Bids are closing at the Bid Receiving Unit (BRU) in the National Capital Region (NCR):

The BRU email address is: To be provided in Formal ITQ

Note: Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to

send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

The BRU facsimile number is: To be inserted in Formal ITQ

b) It is the Bidder's responsibility to ensure the request for opening an epost Connect conversation is sent to the email address above at least six calendar days before the ITQ closing date.

c) Canada requests that the Respondent submits its bid in accordance with section 08 of the 2003 Standard Instructions. Respondent must provide their bid in a single transmission. The epost Connect service has the capacity to receive multiple documents, up to 1GB per individual attachment.

d) If the Respondent is simultaneously providing copies of the response using multiple acceptable delivery methods, and if there is a discrepancy between the wording of any of these copies and the electronic copy provided through epost Connect service, the wording of the electronic copy provided through epost Connect service will have priority over the wording of the other copies.

Bids submitted in hardcopy to PWGSC will not be accepted.

4. Process for Evaluating Responses

4.1 Evaluation of Respondent Qualifications

Canada will evaluate whether each Response satisfies all the mandatory requirements described in this ITQ. The provisions of Standard Instructions – Goods or Services – Competitive Requirements 2003 (2020-05-28) that relate to evaluation also apply. A response must comply with all the requirements of the ITQ in order to be declared compliant.

4.2 Conduct of the Evaluation

a) **Assessment of Responses:** responses will be assessed in accordance with all the requirements described in this ITQ, including the mandatory qualification requirements in Annex B – Mandatory Evaluation Criteria.

b) **Evaluation Team:** An evaluation team composed of representatives of Canada will evaluate the responses. Canada may hire any independent consultant, or use any Government of Canada resources, to evaluate any response. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

c) **Requests for Clarifications:** If Canada seeks clarification or verification or additional information from a Respondent about the response, the Respondent will have seven (7) calendar days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Depending on the nature of the request, failure to meet this deadline may result in the response being rejected.

d) **Extension of Time to Respond:** If additional time is requested by a Respondent, the Contracting Authority may grant an extension in his or her sole discretion.

4.3 Phased Bid Compliance Process (PBCP)

(2018-07-19) General

a) Canada is conducting the PBCP described below for this requirement.

b) Notwithstanding any review by Canada at Phase I or II of the PBCP, Respondents are and will remain solely responsible for the accuracy, consistency and completeness of their Bids and Canada does not undertake, by reason of this review, any obligations or responsibility for identifying any or all errors or omissions in Bids or in responses by a Respondent to any communication from Canada.

THE RESPONDENT ACKNOWLEDGES THAT THE REVIEWS IN PHASE I AND II OF THIS PBCP ARE PRELIMINARY AND DO NOT PRECLUDE A FINDING IN PHASE III THAT THE BID IS NON-RESPONSIVE, EVEN FOR MANDATORY REQUIREMENTS WHICH WERE SUBJECT TO REVIEW IN PHASE I OR II AND NOTWITHSTANDING THAT THE BID HAD BEEN FOUND RESPONSIVE IN SUCH EARLIER PHASE. CANADA MAY DEEM A BID TO BE NON-RESPONSIVE TO A MANDATORY REQUIREMENT AT ANY PHASE.

THE RESPONDENT ALSO ACKNOWLEDGES THAT ITS RESPONSE TO A NOTICE OR A COMPLIANCE ASSESSMENT REPORT (CAR) (EACH DEFINED BELOW) IN PHASE I OR II MAY NOT BE SUCCESSFUL IN RENDERING ITS BID RESPONSIVE TO THE MANDATORY REQUIREMENTS THAT ARE THE SUBJECT OF THE NOTICE OR CAR, AND MAY RENDER ITS BID NON-RESPONSIVE TO OTHER MANDATORY REQUIREMENTS.

(c) Canada may, in its discretion, request and accept at any time from a Respondent and consider as part of the Bid, any information to correct errors or deficiencies in the Bid that are clerical or administrative, such as, without limitation, failure to sign the Bid or any part or to checkmark a box in a form, or other failure of format or form or failure to acknowledge; failure to provide a procurement business number or contact information such as names, addresses and telephone numbers; inadvertent errors in numbers or calculations that do not change the amount the Respondent has specified as the price or of any component thereof that is subject to evaluation. This shall not limit Canada's right to request or accept any information after the ITQ closing in circumstances where the ITQ expressly provides for this right. The Respondent will have the time period specified in writing by Canada to provide the necessary documentation. Failure to meet this deadline will result in the Bid being declared non-responsive.

(d) The PBCP does not limit Canada's rights under Standard Acquisition Clauses and Conditions (SACC) 2003 (2019-03-04) Standard Instructions – Goods or Services – Competitive Requirements nor Canada's right to request or accept any information during the solicitation period or after bid solicitation closing in circumstances where the ITQ expressly provides for this right, or in the circumstances described in subsection (c).

(e) Canada will send any Notice or CAR by any method Canada chooses, in its absolute discretion. The Respondent must submit its response by the method stipulated in the Notice or CAR. Responses are deemed to be received by Canada at the date and time they are delivered to Canada by the method and at the address specified in the Notice or CAR. An email response permitted by the Notice or CAR is deemed received by Canada on the date and time it is received in Canada's email inbox at Canada's email address specified in the Notice or CAR. A Notice or CAR sent by Canada to the Respondent at any address provided by the Respondent in or pursuant to the Bid is deemed received by the Respondent on the date it is sent by Canada. Canada is not responsible for late receipt by Canada of a response, however caused.

Phase I: Financial Bid – Not Applicable to ITQ

Phase II: Technical Bid

a) Canada's review at Phase II will be limited to a review of the Technical Bid to identify any instances where the Respondent has failed to meet any Eligible Mandatory Criterion. This review will not assess whether the Technical Bid meets any standard or is responsive to all solicitation requirements. Eligible Mandatory Criteria are all mandatory technical criteria that are identified in this solicitation as being subject to the PBCP. Mandatory technical criteria that are not identified in the solicitation as being subject to the PBCP, will not be evaluated until Phase III.

b) Canada will send a written notice to the Respondent (Compliance Assessment Report or "CAR") identifying any Eligible Mandatory Criteria that the Bid has failed to meet. A Respondent whose Bid

has been found responsive to the requirements that are reviewed at Phase II will receive a CAR that states that its Bid has been found responsive to the requirements reviewed at Phase II. Such Respondent shall not be entitled to submit any response to the CAR.

c) A Respondent shall have the period specified in the CAR (the “Remedy Period”) to remedy the failure to meet any Eligible Mandatory Criterion identified in the CAR by providing to Canada in writing additional or different information or clarification in response to the CAR. Responses received after the end of the Remedy Period will not be considered by Canada, except in circumstances and on terms expressly provided for in the CAR.

d) The Respondent’s response must address only the Eligible Mandatory Criteria listed in the CAR as not having been achieved, and must include only such information as is necessary to achieve such compliance. Any additional information provided by the Respondent which is not necessary to achieve such compliance will not be considered by Canada, except that, in those instances where such a response to the Eligible Mandatory Criteria specified in the CAR will necessarily result in a consequential change to other parts of the Bid, the Respondent shall identify such additional changes, provided that its response must not include any change to the Financial Bid.

e) The Respondent’s response to the CAR should identify in each case the Eligible Mandatory Criterion in the CAR to which it is responding, including identifying in the corresponding section of the original Bid, the wording of the proposed change to that section, and the wording and location in the Bid of any other consequential changes that necessarily result from such change. In respect of any such consequential change, the Respondent must include a rationale explaining why such consequential change is a necessary result of the change proposed to meet the Eligible Mandatory Criterion. It is not up to Canada to revise the Respondent’s Bid, and failure of the Respondent to do so in accordance with this subparagraph is at the Respondent’s own risk. All submitted information must comply with the requirements of this solicitation.

f) Any changes to the Bid submitted by the Respondent other than as permitted in this solicitation, will be considered to be new information and will be disregarded. Information submitted in accordance with the requirements of this solicitation in response to the CAR will replace, in full, only that part of the original Bid as is permitted in this Section.

g) Additional or different information submitted during Phase II permitted by this section will be considered as included in the Bid, but will be considered by Canada in the evaluation of the Bid at Phase II only for the purpose of determining whether the Bid meets the Eligible Mandatory Criteria. It will not be used at any Phase of the evaluation to increase any score that the original Bid would achieve without the benefit of such additional or different information. For instance, an Eligible Mandatory Criterion that requires a mandatory minimum number of points to achieve compliance will be assessed at Phase II to determine whether such mandatory minimum score would be achieved with such additional or different information submitted by the Respondent in response to the CAR. If so, the Bid will be considered responsive in respect of such Eligible Mandatory Criterion, and the additional or different information submitted by the Respondent shall bind the Respondent as part of its Bid, but the Respondent’s original score, which was less than the mandatory minimum for such Eligible Mandatory Criterion, will not change, and it will be that original score that is used to calculate any score for the Bid

h) Canada will determine whether the Bid is responsive for the requirements reviewed at Phase II, considering such additional or different information or clarification as may have been provided by the Respondent in accordance with this Section. If the Bid is not found responsive for the requirements reviewed at Phase II to the satisfaction of Canada, then the Bid shall be considered non-responsive and will receive no further consideration.

i) Only Bids found responsive to the requirements reviewed in Phase II to the satisfaction of Canada, will receive a Phase III evaluation.

4.3 Basis of Qualification

a) Each Respondent whose response

i. complies with all the requirements of this ITQ; and

ii. meets all the mandatory evaluation criteria at Annex B.

will become a Pre-qualified Supplier for the next phase of the procurement process.

b) Canada reserves the right to re-evaluate the qualification of any Qualified Respondent at any time during the procurement process. For example, if a particular security clearance is a requirement of this ITQ and the Respondent's security clearance changes or lapses, so that the Respondent no longer meets the requirements of this ITQ, Canada may disqualify that Qualified Respondent. Similarly, if information comes to the attention of Canada that calls into question any of the Qualified Respondent's qualifications under this ITQ, Canada may re-evaluate that Qualified Respondent. If Canada re-evaluates the qualification of any Qualified Respondent, Canada may request further information and, if the Qualified Respondent fails to provide it within five (5) working days (or a longer period provided by the Contracting Authority), Canada may disqualify the Pre-qualified Supplier.

c) Unsuccessful Respondents will not be given another opportunity to participate or be re-evaluated for the subsequent phases of the procurement process, unless Canada determines, in its sole discretion, that the circumstances require such a change.

d) Canada will provide written notice to each Respondent informing of their qualification status.

4.4 ITQ Second Qualification Round

a) Canada reserves the right, in its sole discretion, to conduct a second qualification round among the unsuccessful Respondents if, in Canada's opinion, the first qualification round results in an insufficient number of Pre-qualified Suppliers.

b) If Canada determines that unsuccessful Respondents will be given a second opportunity to qualify, Canada will provide written information to all unsuccessful Respondents on the same day regarding the reasons they were unsuccessful during the first qualification round.

c) Any Respondent who does not qualify as a result of any second qualification round conducted by Canada will not be given another opportunity to participate or be re-evaluated for any subsequent phases of this procurement process.

Annex A: Preliminary Statement of Requirements

National Defence Défense nationale

Assistant Deputy Minister (Information Management)

Preliminary Statement of Operational Requirement (SOR)

DSP NO	C.000707
TITLE	Cyber Defence - Decision Analysis and Response (CD-DAR)
PROJECT PHASE	Options Analysis
PROJECT SPONSOR	Chief of Cyberspace Staff
EFFECTIVE DATE	18 April 2019
VERSION	1.6

This page intentionally left blank

TABLE OF CONTENTS

Table of Figures

List of Tables

1. INTRODUCTION

1.1. Background [R7]

There have been significant changes in the cyber threat landscape over the last two decades. Today's cyber attackers are far more sophisticated and may have significant resources available to them, some of whom are funded by nation states or organized crime syndicates. Their primary interests are the acquisition of an adversary's data and corrupting their ability to effectively operate in cyberspace. Attackers have evolved their methods to subvert many current cyber defenses and have adapted to mobile computing devices and cloud environments to exploit their capabilities. New approaches are required to more quickly identify emerging threats and expedite detection and response, which are the capabilities the CD-DAR solution will deliver

Currently, organizations deploy various strategies and solutions which focus on defending the network perimeter and/or end devices (laptops, printers, tablets, etc.) by looking for known methods of attack (viruses, malware, etc.). These solutions tend to be inefficient as they are prone to generating a large amount of alerts, the majority of which are false, but still must be evaluated manually which takes a significant amount of time and expertise. Due to sheer volume, the Department of National Defence (DND) and Canadian Armed Forces (CAF) lack the time and expertise required to respond to all alerts and many go unaddressed. Despite the government's efforts, attackers continuously evolve their methods to subvert cyber defenses and exploit changes in technology perpetuating the threat to national security and welfare of Canada and Canadians.

The CD-DAR Project, C.000707, will acquire defensive cyber solutions (translated into capabilities) to improve overall Decision Support and security of the DND/CAF cyberspace, including the ability to detect, analyze and respond to threats. The integrated solution will provide reliable contextual analysis to support DND/CAF decisions and actions within designated Command Network[1] (Comd-Net) Extensions and Interfaces, and deployable Defence Wide Area Network (DWAN) systems in the conduct of Defensive Cyber Operations.

1.2. Business Need Statement and Outcomes

1.2.1. Business Need Statement [R7]

DND/CAF requires a Cyber Defence capability for strategic, operational, and mission-specific domains that provides network discovery, integrated software cyber defence tools, a trusted database repository, a Common Operating Picture (COP), addressing the human factors and the ability to do cyber forensics remotely. DND/CAF needs integrated monitoring of its network architecture and relevant information

[1] The Command Net is a communications network that connects an echelon of command with some or all of its subordinate echelons for the purpose of command and control.

therein; and complete situation awareness, detection, analysis, and formulation of a response to cyber threats in a timely manner across strategic, operational, tactical domains.

1.2.2. Drivers for Change [R7]

Discovering and keeping track of all network assets and distinguishing the known from the new (and the unknown) is currently challenging. Software flaws and the improper configuration of components are significant vulnerabilities of information systems that allow for exploitation. To provide network security best practices as outlined by the Canadian Centre for Cyber Security, DND/CAF must start with the understanding of the composition of the network and have a robust network asset discovery capability. Canadian Forces Network Operations Center (CFNOC) analysts are often working with multiple tool sets; they are looking at many consoles for new alerts, threat intelligence service portals for information about the entities involved, and endpoint detection and response tools for context on what is happening on affected endpoints. CFNOC is using workflow tools to control triage and investigation processes; this work often requires the analyst to copy and paste data from one tool to another, fill in forms and submit search queries or upload artifacts for analysis and storage. The automation provided by CD-DAR solutions can eliminate many of these tasks, streamline processes and introduce repeatable quality and consistency, even if the processes remain essentially the same. The elimination or reduction of this type of repetitive manual process will have a direct impact on analysts' productivity; security analysts can then spend more time on harder problems that are higher in priority and require human expertise.

Additionally, security monitoring systems are known to generate a high number of alerts, including many that are found to be "false positives" (or simply not relevant) after further investigation. Alert triage is often done in a manual way and subject to mistakes by analysts that can lead to incidents being ignored. There are many reports in media reference organizations that have been breached after security tools had generated alerts about intrusion, only to be incorrectly dismissed by (likely overwhelmed) analysts. DND/CAF are dealing with increasingly aggressive threats, such as ransomware[2], where effective response is measured in seconds. This scenario forces organizations to reduce the time they take to respond to those incidents, typically by delegating more tasks to machines. Reducing the response time, including incident containment and remediation, is one of the most effective ways to control the impact of security incidents. The CD-DAR solutions automatically provide context to alerts and add key information to enable automated or, at least, easier and faster manual triage.

CFNOC can leverage CD-DAR solutions to reduce the time required to train new cyber analysts. Automation removes the need for the analyst to know the details of which manual steps should be followed for each scenario. Knowledge is stored and managed within the CD-DAR solutions, and will provide a reduced need for the analyst to memorize process flow and consistently repeat the process. Analysts can retrieve precise details for numerous scenarios, should the need ever arise. CD-DAR

2 A type of malicious software designed to block access to a computer system until a sum of money is paid.

solutions will combine the functionality of existing tools, providing a Common Operating Picture reducing the need to train every security analyst on each individual tool.

The DND/CAF do not have an integrated COP. The Coalition Warrior Interoperability eXploration eXperiment eXamination eXercise (CWIX) is a NATO-led capability development, interoperability testing, and experimentation forum conducted annually. The CWIX 2018 event was to perform test cases within the Cyber Focus Areas with emphasis upon interoperability testing and experimentation. One of the main testing objectives was to examine the integration of cyber domain activities into a proposed COP with Command and Control applications and processes. A total of 23 test cases were derived; however, COP was not successful. The experimentation led to the confirmation that much additional work is required and that it is essential that CD-DAR solutions focus more upon the higher-level objective of a Cyber COP.

It is a known fact that today, the number of cyber events and security alerts surpasses easily the number of cyber personnel with the necessary background and experience hired to protect and investigate these events. It is challenging and very difficult to remain up-to-date on this ever-changing front. Coupled with the current out-of-date and inefficient cyber defence capabilities, Canadian national security and defence remain vulnerable to an ever increasing cyber threat.

1.2.3. Capability Gap [R7]

As further detailed in section 1.3, the capability gaps are deficiencies in or a lack of:

- Network Discovery;
- Integrated software cyber defence tools;
- A trusted database repository;
- Common Operating Picture;
- Human Factors; and
- Forensics.

1.2.4. Business Outcomes [R7]

CD-DAR will bring a fundamental shift to the DND/CAF cyber security by implementing the capability for complete responses to sophisticated and evolving cyber security events. It will address both immediate and long-term needs, while maintaining and allowing for the enforcement of cyber security requirements.

This project will deliver and implement a complex system consisting of computer hardware and software, operated by trained personnel and following associated processes, which will perform a reliable, near real-time security monitoring and event response function on designated networks.

The ***immediate*** outcomes of the project will evolve CFNOC into a modern Cyber Operations Centre equipped with a CD-DAR solution that will be operated by a Cyber Force. The capability to be delivered by the project will greatly impact the way Cyber Operators are educated, trained, equipped and conduct

their daily routine. Improved Decision Support and Decision Analysis and Response (DAR) will ensure that they are ready to operate within cyberspace to protect DND/CAF Comd-Net Extensions and Interfaces, and deployed DWAN systems.

The ***intermediate*** outcomes will include refined performance indicators, reporting measures and reporting systems (if essential), and refined and/or newly defined operational processes put into place where needed. These operational processes will further use the hardware and software tools to establish reliable, relevant and meaningful Cyber security situational awareness of the Information Technology Infrastructure (ITI), and decision support concerning DCO, that affects all aspects of DND/CAF operations.

The ***ultimate*** outcomes of the proposed investment will see the DND/CAF with a cyber force that is equipped, trained and prepared to effectively conduct DCO built on a strong foundational cyber capability which will allow future growth development for years to come. In addition, through application of the Defence Procurement Strategy policy, this project will contribute to the development and sustainment of a viable cyber industry in Canada that is prepared to support the Government of Canada and the Defence Team through the provision of innovative, scientifically advanced technologies and personnel solutions into the future.

1.2.5. High Level Mandatory Requirements (HLMRs) [R7]

Key operational Drivers of the required capability are addressed by the High Level Mandatory Requirements. High Level Mandatory Requirements describe a set of capabilities which the CD-DAR project must achieve. Essentially, they define the expected outcomes, effects or services to be delivered by the project.

The High Level Mandatory Requirements for the investment are described in Table 1 below. These HLMRs will be further refined into a detailed Statement of Operational Requirement (SOR).

For the purposes of the SOR, the scope of CD-DAR is “Command Network”. A Command Network is a communications network that connects an echelon of command with some or all of its subordinate echelons for the purpose of command and control. Consolidated Secret Network Infrastructure (CSNI) is a part of the Command Network within DND/CAF and a significant portion of the scope of this project will be applied to CSNI. Included under the Command Network are Comd-Net Extensions and Interfaces, and Deployable DWAN systems. Throughout this Business Case “Command Network” will be used to include the above terms.

Table 1 - High Level Mandatory Requirements

#	Capability	HLMR
1	Cyber Assets (Network Discovery)	The ability to rapidly identify and track, all assets (authorized and non-authorized) connected to the Command Network and assess their attributes for vulnerability, configuration, risk and patch compliance.
2	Cyber Analysis	The ability to continuously collect, retain, and analyze cyber threat information on the Command Network environment and detect and characterize suspicious

#	Capability	HLMR
		activity, provide context for risk and vulnerability assessments in near real-time.
3	Cyber Response	The ability to adaptively and dynamically identify contain and eradicate a threat.
4	Cyber Command and Control	The ability to maintain situation awareness, through a Common Operating Picture, of alerts, threats, and remediation's across the DND/CAF Command Network, and to feed situational awareness to processes for decision on, and execution of, responses through standardized interfaces and supporting automated workflows for the decision support to the command element, and the implementation of responses as directed.
5	CD-DAR Integration	The ability to be integrated (hosted and interoperated with applications and a trusted repository) into the assigned Command Network as one cohesive system.
6	Cyber Interoperability	The ability to exchange cyber threat vector and analyses information for internal compatibility requirements as well as the systems and assigned network environment of specified Other Government Departments (OGDs), Five Eyes (FVEY) nations, North Atlantic Treaty Organization (NATO) nations, and other external organizations.
7	Cyber Resilience	The ability to perform localized monitoring of network architecture, assets, and potential threat information, analysis, and response decision-making in deployed environments where the connectivity is unavailable, unreliable or has limited capacity.
8	Cyber Capability Continuous Evolution and Development	The ability to continuously evolve as a response to change (threat, policy, technological) to DND/CAF network infrastructure (remote forensics and containment / remediation are part of this response) with minimal impact to connected systems or modification to the underlying IT infrastructure, baseline standards, and policies.
9	Cyber Flexibility	The ability for CD-DAR capability to be scalable, modular and readily expanded, regardless of static or operationally deployed asset location or duration.

1.2.6. Key Assumptions [R7]

Following an internal and external review, the assumptions affecting this project are listed in Table 2 below.

Table 2 - Assumptions

#	Category	It is assumed that:	Effects on Project	Reliability Level: Low / Medium / High	Strategies if not Realized
1	Infrastructure	The project will use existing physical and network infrastructure but might require specific network enclaves for security purposes and testing.	If the existing physical and network infrastructure cannot be re-used, there will be increased costs to the project.	High	A reassessment will take place and funds reallocated.
2	System Engineering	The current bandwidth within the ITI will be able to accommodate the Situational Awareness (SA) data updates required by the CD-DAR solution, especially at deployed locations.	A lack of available bandwidth may overload the operational cyber environment and negatively affect mission assurance. A requirement for additional bandwidth would increase operational costs.	High	If there is a lack of sufficient bandwidth, it will be addressed with appropriate agencies (DIMEI, SSC) to formulate a resolution

1.2.7. Initial Operational Capability (IOC)

The IOC will see the attainment of all HLMR capabilities as outlined in Table 1. It will be limited to pre-established Comd-NET infrastructures and deployed DWAN assets identified in the Statement of Requirement (SOR) generated within the Definition Phase of the Project in consultation with Stakeholders and applicable Subject Matter Experts (SMEs). This will include the installation/configuration of supporting infrastructure at applicable sites where select personnel will also be trained on CD-DAR specific systems.

It will also achieve the “Immediate” and “Intermediate” business outcomes, as stated in the Business Outcomes in Section 1.2.4 of this document.

Prior to Implementation, the Project Sponsor and the Implementer will jointly agree on the specific System Effectiveness Requirements that must be achieved to declare IOC. The Project Sponsor and the Implementer will also jointly develop and agree on an IOC Certificate to be used to certify achievement of the milestone.

1.2.8. Full Operational Capability (FOC)

The FOC will see the attainment of capabilities of all HLMRs, outlined in Table 1, on the remainder of Comd-NET infrastructures and deployed DWAN assets. The networks will be identified in the Statement of Requirement (SOR) generated within the Definition Phase of the Project and in consultation with Stakeholders and applicable Subject Matter Experts (SMEs). This will include the installation/configuration of supporting infrastructure and the training of select personnel on CD-DAR specific systems for all applicable sites.

In addition to the business outcomes achieved in the IOC on the affected networks, the FOC will also achieve the "Ultimate" business outcome, as stated in the Business Outcomes Section 1.2.4, achieving full CD-DAR capabilities on all Comd-NET infrastructures and deployed DWAN assets within the CAF.

The Project Sponsor and the Implementer will jointly agree on the specific System Effectiveness Requirements that must be achieved to declare FOC. The Project Sponsor and the Implementer will also jointly develop and agree on an FOC Certificate to be used to certify achievement of the milestone.

1.3. Capability Deficiency [R7]

The DND/CAF cyber domain is currently under persistent, enduring and increasing threat from adversaries. It is imperative that the CD-DAR solutions replace today's multiple systems and manual processes with a modern, single platform with automated and correlated operational processes. The CD-DAR project is a major step forward in defending and protecting the DND/CAF cyber domain with a centralized focus on the Canadian Forces Information Operations Group (CFIOG) and Canadian Forces Network Operations Center (CFNOC).

Together with stakeholders (those with vested interests in operating the networks described below primarily within DND and does include other government departments or agencies such as CSE and SSC as well as our Five Eyes and NATO allies) the CD-DAR project has assessed the current DND/CAF cyber capabilities and concluded that they are insufficient for current needs. They are based on short-term solutions with irregular injections of new technologies that achieve limited effect. Within DND the lead organization for Cyber Defence is Canadian Forces Network Operation Center (CFNOC). Their mission is to gain and maintain Cyber Superiority within DND/CAF Cyber Area of Responsibility (AOR) in order to "Assure Friendly-Force Freedom of Action." Operationally focused, highly motivated and uniquely skilled in specialized technologies and techniques, they are proactive, dynamic, 24/7 and dedicated to maintaining IT services under all conditions. CFNOC is the national operational cyber defence unit permanently assigned mission critical tasks to represent the Chief of the Defence Staff (CDS) and applicable network Operational Authorities (OAs). CFNOC, on behalf of ADM(IM), will direct the routine operation and defence of DND/CAF networks.

Within CFNOC there are the following teams that have capability gaps:

- Cyber Defence Operation - coordinates DND/CAF defensive cyber operations and incident response with organizations internal and external to the department;
- Cyber Threats Intelligence Cell - currently operates 8/5 (with a surge capability) to provide proactive and reactive intelligence to enhance cyber defence operations;
- Surveillance Team - conducts network traffic analysis of DND/CAF cyber domain in order to identify potentially compromised devices for further investigation;
- Reconnaissance Team - provides live, realistic vulnerability and advanced exploitation assessments of information systems and procedures to evaluate client's security posture and performs controlled demonstrations of what an attacker could accomplish within a client's IT infrastructure;
- Incident Handling Team - performs the national incident handling leadership role as part of the established framework for a coordinated enterprise approach;
- Enterprise Intrusion Detection System Support – responsible for providing 24/7 support of the following: (i) Configuration, testing, deployment of various IDS and analytical tools on CFNOC IDS sensors / servers for all CAF monitored networks; (ii) Configuration, testing, deployment of various IDS sensors/ servers on all networks; (iii) Patching and upgrades of the IDS suites and required; and (iv) Hardware / software support and maintenance of the IDS hardware (Security Onion[3], Sourcefire[4], and CFNOC purpose-built);
- Enterprise Vulnerability Assessment Support Team - performs vulnerability and risk management on selected networks; and
- Forensics Section - provides specialized digital analytical services to DND/CAF. It also provides technical analysis of cyber threats and malware techniques used by adversaries to penetrate DND/CAF cyber domain.

The capability gaps are deficiencies in or a lack of:

- Network Discovery;
- Integrated software cyber defence tools;
- A trusted database repository;

[3] Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management.
[4] Sourcefire, Inc (acquired by Cisco) was a technology company that developed network security hardware and software. The company's Firepower network security appliances are based on Snort, an open-source intrusion detection system (IDS)

- Common Operating Picture;
- Human Factors; and
- Forensics.

Network Discovery - In order to protect a network there must be a complete inventory of all of the network hardware devices such as servers, routers, switches, gateways and much more, and the software including the latest versions or patches[5] that are on the specified network. Currently network monitoring and device discovery are limited for DND/CAF. There are platforms able to conduct network discovery being tested and used in ad hoc fashions, covering portions of DND/CAF networks but not the complete network. Software such as Nessus, Cyber Information and Incident Sharing System (CIICS), and Malware Information Sharing Platform (MISP)[6] have been found to be capable of providing a solution but are not used in a cohesive fashion. The CD-DAR solutions will find the best possible answers, ensure network discovery platforms are interoperable and cover the full range of product design capabilities.

Integrated software cyber defence tools – The current tool set available is not integrated, and requires extremely specialised operator skills to use these software tools to isolate any issues, export information, and do manual comparisons with information extracted from other software tools. Two examples are:

- Surveillance Team - Currently the surveillance analyst is using isolated tool sets that are not linked. This does not allow for a complete picture of the cyber threat. To more effectively automate the detection of threats there is a need to use machine learning and automated algorithms to observe trends to detect previously unknown threats. This will help maintain network robustness, allowing DND/CAF to maintain better cyber security; and
- Incident Handling Team - Incident handling is a very cumbersome process. There are few platforms that have good workflows that allow traceability of how an incident is handled and/or accountability of the actions taken throughout the process. At this time, an analysis is completed on one platform and then the analysis data must be transferred physically to other applications to properly handle the incident.

A trusted database repository –The Cyber Threats Intelligence Cell provides proactive and reactive intelligence to enhance cyber defence operations. To conduct an analysis, DND/CAF must draw information from different systems. A central repository will enable commanders to make informed decisions for required defensive actions. Currently, the National Data Transfer Center within the Strategic

[5] A **patch** is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities (a weakness which can be exploited by a Threat Actor, such as an attacker, to perform unauthorized actions within a computer system).

[6] Nessus is a proprietary vulnerability scanner developed by Tenable Network Security; Cyber Information and Incident Coordination System (CIICS), is a web-based application that enables Nations to share cyber defence information within a trusted community; this community is called the NATO CIICS Federation; The Malware Information Sharing Platform (MISP) threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators.

Joint Staff has a capability to transfer information to and from 29 different networks for all DND/CAF. However, this is not a cyber capability, therefore, this information is out of reach for the CD-DAR solution set and limits how the information is stored and transferred for cyber intelligence purposes. There is a need to have task tailored Cyber Threats Intelligence in a central and robust repository with a large quantity of automation for trusted and known sources from low classified level to a high classified level (and vice versa) of information and basic system and network data. This will enable security monitoring and mechanisms such as link analysis, vulnerability analysis, intrusion detection, forensic analysis, collection and analysis of logs and other data from organization networks. This would also allow the conduct of security analysis reviews and advice and guidance for responses to security alerts.

Common Operating Picture (COP) – Closely associated with the integrated software defence tools is the ability to share the information to develop a COP. The current DND/CAF capabilities lack a central view to assess the impacts of cyber activities. These capabilities are insufficiently integrated, less responsive and are considered deficient in providing operational information to support effective command decision-making processes. A COP should be malleable and attuned to each commanders needs whether Strategic, Operational or Tactical. Currently, the CFNOC uses and internal program with no leeway in the operational views to consolidate information for the commander. There is also no way to use this program on networks that are unavailable, unreliable or that have limited capacity (episodic) environments.

Human Factors – There are two specific human factor aspects that CD-DAR solutions will address. The first is that too much specialization is required from cyber analysts and the second is cognitive overload for the cyber operators. To address these issues CD-DAR solutions will provide integrated cyber defence solutions that will ease the burden of manually comparing information from one tool to the output of another tool, this will reduce the detailed knowledge and specialisation required to become proficient with the various cyber defence tools. CD-DAR will ease cognitive overload by managing the volume of manual threat detection by automatically collecting security information from the network. It will analyze this information to identify threats, correlating information from multiple sources (Government of Canada and Allies). Security alerts will then be automatically prioritized along with recommendations on how to remediate the threat.

The CD-DAR solutions will employ advanced security analytics that go far beyond the signature-based approaches currently being used. Machine learning technologies will be leveraged to evaluate events across Command Network and detect threats and predict the evolution of attacks that would be impossible to do using manual approaches. These security analytics include:

- Integrated threat intelligence that looks for known bad actors by leveraging global threat intelligence;
- Behavioural analytics that applies known patterns to discover malicious behaviour; and
- Anomaly detection using statistical profiling to build a historical baseline to provide alerts on deviations from established baselines that conform to potential attack vectors.

Capability to conduct forensics - The Forensics Section provides specialized digital analytical services to DND/CAF. It also provides technical analysis of cyber threats and malware techniques used by adversaries to penetrate the DND/CAF cyber domain. In addition to malware analysis, the Forensics Section is responsible to maintain and collaborate with other agencies concerning cyber security events. Currently, when a data spill occurs, the physical removal and replacement of hardware can cost the DND/CAF thousands or even millions of dollars per instance. With CD-DAR, as an alternative to replacing physical hardware, an affected hard drive might have the image remotely sent to a sandboxed[7] environment where Forensics can do analysis and investigation while simultaneously allowing the physical hard drive to be wiped clean. Where equipment is located in different geographical regions without available analyst expertise, hard drives and other equipment have to be shipped to a local facility for analysis. These drives are subject to shipping damage which also further delays and/or potentially stops proper procedure from taking place and potential evidence from being reviewed. The CD-DAR solutions will save time and money as forensics will not have to wait for equipment to be transported across the country for analysis.

1.4. Project Constraints [R7]

Table 3 - Constraints

#	Category	Description
1	Design Requirement	The system of processes, software and hardware must be capable of being used by existing DND/CAF operational personnel, including those personnel currently producing and consuming Situational Awareness information.

1.5. Current Situation [R7]

The CD-DAR Project was reviewed by the Defence Capability Board (DCB) on 28 March 2019. The DCB approved the preferred option of the merged (CSA/DCO-DS projects) Business Case Analysis. The DCB also agreed that the project should proceed to Programme Management Board for the Definition Phase endorsement, following a review of project scope, scalability and timelines.

2. SYSTEM OPERATION

2.1. Mission and Scenarios

The **Mission** of the CAF Cyber Force is to conceive and design CAF cyber capabilities, then build and implement/integrate them with extant forces to conduct full spectrum cyber operations. Given the constant, integrated, worldwide, technologically dependent cyber domain within which the CAF operates

[7] In computer security, a "sandbox" is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading, without risking harm to the host machine or operating system.

as a whole, the Cyber Force plays a crucial role in the day-to-day defence of Canada, both now and into the future.

The **Primary Mission** of the CD-DAR Project will be to acquire defensive cyber capabilities to improve Cyber security SA and Decision Analysis and Response (DAR). These must be integrated into a solution to provide reliable contextual analysis in order to support the decisions and response actions of the people of the Command Network in the conduct of DCO. [R3]

The DND/CAF is responsible for providing military intelligence for threat and risk assessment processes. The DND/CAF can be called upon at any given time to undertake missions for the protection of Canada and Canadians and the maintenance of international peace and stability.

The CD-DAR capabilities will be available and active regardless of the mission's purpose, location, or duration. As CD-DAR monitors Comd-NETs and their extensions, operations utilising these Comd-NETs will be provided the same cyber defence capability in the support of their mission.

A cyber operation is the application of coordinated cyber capabilities to achieve an objective in or through cyberspace.[R24] Cyber operations are relevant across the full spectrum of military operations, from support to the civil authority, search and rescue, peace support operations, and war-fighting. [R25] As with all military operations, operational effects are done through formalized command and control relationships, operational groupings, command-driven information requirements, deliberate planning, staff procedures, and a trained and prepared force that can generate operational effects.

The aim of DCO is to actively counter threats and return the network to its original secure operating state. DCO are the actions taken to defend the availability, integrity and confidentiality of the CAF command and control system and data so that a commander can exercise their operational authorities. DCO actions

include intelligence support activities (Protect), surveillance and reconnaissance tasks (Detect and Orient), command decisions (Decide), and countermeasure deployment (Act).

The diagram in Figure 1 below presents a typical DCO action and decision template that shows branch and sequel plans all aimed at returning to a secure operating condition.

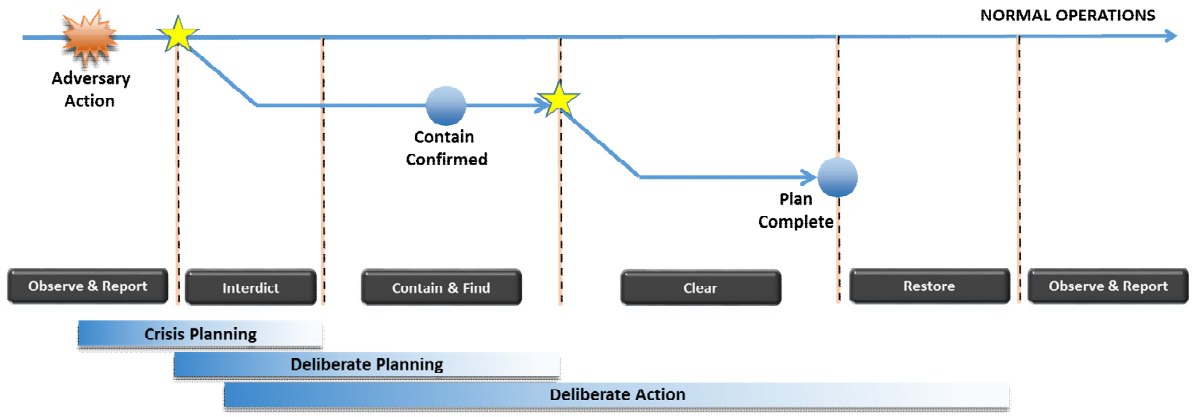


Figure 1 - DCO Action and Decision Template

Once CD-DAR is implemented, the role of CFNOC will include the detection, recognition and identification of hostile or otherwise unauthorized cyber entities (human and non-human) within a defined and designated Area of Cyber Responsibility and, depending on its disposition, will prevent its destruction or loss to enemy action.

CFNOC's cyber mission: "CFNOC will gain and maintain Cyber superiority within the DND/CAF's Cyber AOR in order to assure friendly forces freedom of action."

The CD-DAR Project will deliver a capability that will improve the DND/CAF Cyber security posture, decrease response time when cyber incidents occur and will assist in mitigating the threat of cyber-attacks by providing the force employer with a means to effectively operate within a contested cyber domain. The greater security visibility and standardization provided by CD-DAR will form the foundation upon which more advanced capabilities to manage, secure, and defend Canada and Canadians can be constructed.

2.2. Environment

With a significant portion of the world population now globally connected via evolving manifestations of the Internet, the security and defence challenges posed by cyberspace are significant. Additionally, increased connectivity has allowed, and will continue to allow adversaries to connect to and motivate ideological groups and individuals through a range of internet enabled platforms, currencies, and financial sources of power. The protection of national intelligence, defence, and security information, the assured access and use of Canadian and allied information technology systems and infrastructure, and the ability

to exploit cyberspace to achieve national security goals is a necessity, and will continue to be critical to the security of most countries. [R7]

The importance of the global ITI continues to expand and extend into new areas of modern life and society. Technological advances have opened the cyber domain to a variety of state and non-state actors resulting in an increased and significant threat. In the military context, potential adversaries are rapidly developing cyber means to exploit the vulnerabilities inherent in the Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) systems as well as combat systems. This key military and domestic requirement is described in Canada's Defence Policy: Strong, Secure, Engaged. [R6]

The CD-DAR solution will provide IT security and defence capabilities wherever Comd-Net Extensions and Interfaces, both static and deployed, and identified deployable DWAN systems are accessible. This impacts the following environments:

a. *Enduring Environment*: This includes fixed domestic and international locations such as Canadian Forces Network Operations Centre (CFNOC) and DEFSOC where there is a full suite of support infrastructure available as well as full connectivity to supporting networks and systems. The operating environment is robust and reliably available;

b. *Episodic Environment*: This involves all deployed mission locations where infrastructure will vary from robust to limited and availability will range from reliable to unreliable. These conditions add requirements to operate in and recover from disconnected, intermittent and low bandwidth (Limited) situations. Disconnected, Intermittent, and Limited environments predicate the need for local autonomous processing, for alternate communication channels and for the ability to seamlessly recover from connection limitations when reconnection is achieved;

c. *Collaborative Environment*: As most DND/CAF engagements operate in multi-system and multi-party environments, CD-DAR capabilities need to interoperate with DND-managed networks and systems, OGDs and agencies, allies and other international partners. The CD-DAR solution must also address the need to handle information across various security domains and caveats.

d. *Cyber Environment*: Weaknesses can be exploited and the impacts of exploits can spread across networks which require maximum responsiveness. This is usually accomplished by maximizing automation of monitoring, detection, analysis, decision-making and response capabilities as well as inclusion of flexible processes and systems to adapt to a rapidly evolving threat environment.

The cyber domain requires a strong and cohesive set of tools, resources and capabilities to enable DND/CAF to deliver on its mandate and effectively operate in a contested cyber domain.

2.3. Threats

Much like asymmetric warfare, cyber threats[8] are not immediately visible as compared to traditional military conflicts. Countless threat actors, hidden in cyberspace, can influence or target DND/CAF as a whole, a specific system or a particular individual.

To focus defence efforts in the cyber domain, Canada must have a sound knowledge of the leading threat actors to include their intentions, capabilities, and opportunities. An open source report produced by the US, *The Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee* [R38], identifies some of the leading cyber threat actors and the threats they pose. The following points from the report are highlighted to illustrate our adversaries' use of cyberspace in the operational environment:

a. Some nations are assuming a more assertive cyber posture based on their willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny;

b. Cyber operations are likely to target western interests to support several strategic objectives: intelligence[9] gathering to support decision making, influence operations to support military and political objectives, and continuing preparation of the cyber environment for future contingencies;

c. Several nations continue to have success in cyber espionage against governments and industry;

d. Cyber-attacks are being used against targets where there is a threat to domestic stability or regime legitimacy;

e. Cyber espionage, propaganda, and attacks are being used to support security priorities, influence events, and counter threats; and

f. Some nations are capable and willing to launch disruptive or destructive cyber-attacks to support political objectives.[R4]

The most sophisticated cyber threats come from the intelligence and military services of foreign states. Technologically-advanced governments, their militaries, and private businesses are vulnerable to state-

[8] **Cyber threat (NATO):** The possibility of a malicious attempt to damage or disrupt a computer network system.

[9] **Intelligence**: The product resulting from the collection, processing, analysis, integration and interpretation of available information concerning foreign states, hostile or potentially hostile forces or elements, geography and social and cultural factors that contributes to the understanding of an actual or potential operating environment.

Note: The term 'intelligence' also applies to the activities that result in the product and to the organizations engaged in such activities. DTB Record 738.

sponsored cyber espionage and disruptive cyber operations. This threat can be expected to grow in the coming years.

Adversarial cyber operations are posing significant threats to allied missions in or through cyberspace where adversaries are able to deny or manipulate operational capabilities, conduct rapid and sustained intelligence collection, and conduct deception activities. The operational challenge, therefore, is to ensure the CAF's freedom of action within cyberspace by defending CAF capabilities in support of military objectives. [R4]

In the military context, while the use of cyberspace has become crucial to operations, potential adversaries, including state proxies and non-state actors, are rapidly developing cyber means to exploit the vulnerabilities inherent in C4ISR systems on which militaries depend, as well as other operational technologies, such as combat systems. [R7]

The high rate of technological innovation, the dominance of commercial, off-the-shelf software, and the increasing proliferation of entities with embedded and unchangeable software means that cyber-attack potential will outpace defence capabilities. [R26]

a. The continued use of commercial technology means that system vulnerabilities can be known, traded and widely exploited. Interdependence based on linked networks makes important systems highly vulnerable to rapid and catastrophic collapse, requiring a prolonged repair stage. As the number of cyber transactions increases, the relative proportion of attacks may go down. However, the risk of catastrophic attacks is steadily increasing;

b. The proliferation of devices with embedded systems—the Internet of Things—adds a new danger. Devices will be long-lasting, vulnerable to attack, but unreachable for software fixes; and

c. The state use of cyber-attack weapons will not be restrained primarily due to its effectiveness and the anonymity cyberspace provides making some attacks virtually untraceable.

2.4. Concept of Operations

Given the complexities of modern operational environments there is an ongoing requirement for real-time situational awareness, information sharing, and collaboration, usually achieved through a Cyber – Battlespace Management Capability, more frequently referred to as Cyber – Common Operational Picture (COP). A Cyber – Battlespace Management Capability should include the ability to rapidly fuse, correlate, and display data from global network sensors to deliver a reliable picture of friendly, neutral, and adversary networks, including their physical locations and activities. In addition, the Cyber – Battlespace Management Capability should support near real-time threat and event data from myriad sources and improve commanders' abilities to identify, monitor, characterize, track, locate, and take action in response to cyber domain activity as it occurs both globally and within Areas of Responsibility (AOR).

> "The overall effectiveness of cyber operations is determined by the ability to rapidly integrate situational awareness, understanding and action across network operations and cyber operations activities. This implies a need to centralize the units and a desire to reduce the headquarters executing C2 to the minimum necessary. From a defensive perceptive, this is particularly important with respect to the development of cyber situational awareness, which is important to network operations, but the center of gravity for DCO. C2 should be as flat as possible and optimized to be responsive with adequate authorities delegated to take rapid action[10]. From a force structure perspective, this drives integrated DCO units responsible for building and maintaining broad cyber domain situational awareness and authorized to direct rapid action from dispersed network operations elements." [R4]

Forces conducting cyber operations may support several users simultaneously. This requires extensive coordination, planning, and early integration of requirements and capabilities. Supported and supporting commanders coordinate, as appropriate, the deployment and employment of forces conducting cyber operations required to accomplish the assigned mission, particularly for deployed weapon and platform systems. Most cyber operation forces will be geographically separated from a particular supported theatre of operations, thus all involved commanders are required to take extra measures to ensure the supported commander is continuously aware of the remote supporting forces' operational status.

With the CD-DAR system, Cyber Operators are the personnel tasked with Cyber security and DCO. These operators are on the front line of the CAF operations, supporting the Joint Force Cyber Component Commander (JFCCC). 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. Figure 2 below provides a high-level operational view of the desired system where the Cyber Operators are the personnel tasked with Cyber security and DCO.

[10] **This is an extract from the JDN Cyber Operations; the C2 Structure being "as flat as possible" means that Command authority should be delegated as close as possible to the tactical response execution, thereby enabling responsiveness of the Direct-Act segments of the OODA loop.**

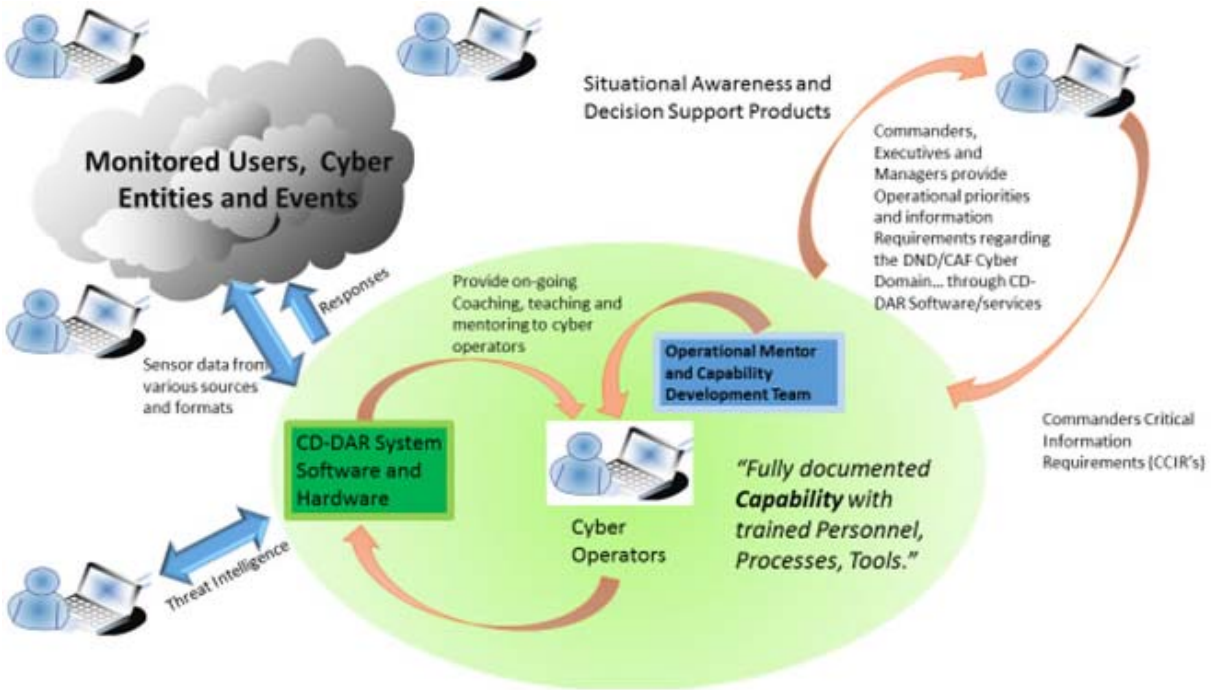


Figure 2 - Operational View: Cyber Operations Centre

The CD-DAR project will create, equip, organize and train CFNOC to operate a capability that defends DND/CAF networks in the current 24/7 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 view 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 (RCN), the Royal Canadian Air Force (RCAF), the Canadian Army (CA), the Canadian Joint Operations Command (CJOC), Canadian Special Operations Forces Command (CANSOFCOM) and the Strategic Joint Staff (SJS)) would be similarly enabled with the appropriate level of information for operational purposes. .

2.5. Concept of Support [R39]

This concept of support will state how In–Service Support (ISS) and evolution of the CD-DAR capability, as an operational system, will be done both from a technical and business (operational) perspective.

2.5.1. Technical Concept of Support

Technical ISS for CD-DAR denotes in-service support for IT Facilities and IT Assets impacted by CD-DAR.

For CD-DAR, this category includes:

a. Server Rooms where asset security information is collected, aggregated, analysed, reported and acted on; and

b. Cyber Integrated Test Environment (CITE).

IT Facility ISS is out of scope as it is assumed that existing IT facility processes will be used.

IT Asset ISS includes support for in-scope information systems, software and hardware and the information processed by them.

For CD-DAR, IT assets:

a. *Include* any information systems, hardware, software and supporting information upon which CD-DAR depends (e.g., for security-related and defence-related monitoring, detection, analysis, decision-making and responses)

b. *Exclude* any information systems, hardware and software that CD-DAR functionality acts on (e.g., the devices that it monitors).

Assistant Deputy Minister (Information Management) (ADM(IM)) will be responsible for supporting the facilities and assets, leveraging the organization implemented as part of the Information Technology Service Management (ITSM) Project or contracting services out, as appropriate.

Support to the system will follow the Information Technology Infrastructure Library[11] (ITIL) framework, which endorses alignment of IT services to the needs of the business. ITIL represents the industry best practises for IT System support. These best practises will be adapted to suit the unique environment and organizational structure of the DND/CAF.

Three lines of support are defined under ITIL:

a. First Line Support. First line support is responsible to register and classify received incidents and undertake an immediate effort to restore a failed service as quickly as possible. If an immediate solution cannot be achieved, first line support will refer the issue to second line support. First line support also processes service requests and keeps users informed about the status of resolution.

b. Second Line Support. Second line support takes over incidents which cannot be resolved immediately by first line support. Second line support will coordinate with external service

[11] ITIL, formally an acronym for Information Technology Infrastructure Library, is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

providers as required. Problems that cannot be resolved at this level will be passed to third line support.

c. Third Line Support (National). Third Line support is provided by hardware and software manufacturers or third party suppliers. Services are requested by second line support to solve an incident.

The table below outlines the lines of support within DND with response and repair times:

Table 4 - DND Support Times

Level of Support Facility	Response Time	Repair Time
First Line Support	Immediate (Helpdesk) Less than 1 hr	Continuous Effort
Second Line Support	To be Confirmed (TBC)	TBC
Third Line Support	TBC (based on contract or Service Level Agreement)	TBC

The detailed CONSUP will be developed during the Definition Phase of the project as system design, key performance measures and functional specifications are defined.

2.5.2. Business Concept of Support

An Operational Mentor and Capability Development (OMCD) capability, a small team comprised of military, public service and professional services cyber operations subject matter experts, will be co-located with the delivered capability during implementation and throughout its life-cycle. The role of OMCD is to coach, instruct 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. In collaboration with organizations impacted by CD-DAR, the OMCD will:

a. Support the business transformation of the CAF Cyber security and DCO capabilities to become a National Institute of Standards and Technology (NIST) 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.

Typical area of responsibility include:

a. Processes & organizations (Planning and Management, Research and Development, Concept and Doctrine, Organizational Design, Business Processes, Business Administration, Legal Services, Security Services);

b. Human Resource Management (Civilian Personnel Management, Military Personnel Management, Contractor Management, Training);

c. Physical Resource Management (Facilities, Physical Infrastructure Equipment, Supplies and Procurement); and

d. Financial Resource Management (Personnel, Operations and Maintenance (PO&M) funding).

For CD-DAR, this includes:

a. Organizations that govern CD-DAR operations such as the Cyber Force Commander; and

b. Organizations involved in the use of CD-DAR capabilities such as the Joint Cyber Operations Team (JCOT), DEFSOC and CFNOC.

2.6. Key Roles [R30]

a. CAF Commanders. Commanders across the CAF, up to and including the CDS, are responsible for C2 of assigned forces, including the Cyber Force.

b. Operational Support Staff. Operational support staff include all DND/CAF individuals who provide direct and indirect support to CAF strategic and operational commander's planning activities and mission execution. They are often located at headquarters.

c. Service Provider Staff. The staff that implements and manages delivery of CD-DAR to users. Included is CFNOC for operational support and for security event and incident handling. Also included is the Cyber Operator role.

d. Operational Authority (OA). The OA is defined as the person who has the authority to define requirements and operating principles, set standards and accept risk within his area of responsibility; the OA is responsible and accountable to the Chief of the Defence Staff [3]. Assuming no significant organizational and IT governance changes in the foreseeable future, DOS SJS will be the OA for the infrastructure within scope of CD-DAR.

e. Technical Authority (TA). The TA is defined as the person who has the authority to set technical specifications and standards, manage configurations, provide technical advice and monitor compliance within his area of responsibility[12]. Assuming no significant

[12] 2700-1 (SJS J6), 10 November 2017

organizational and IT governance changes in the foreseeable future, ADM(IM) will be the TA for the infrastructure within scope of CD-DAR.

f. Security Authority. The security authority is defined as the person who has the authority to identify risk, provide advice and security standards for endorsement by the operational authority and technical authority, and monitor compliance within his area of responsibility. Assuming no significant organizational and IT governance changes in the foreseeable future, ADM(IM)/Director Information Management Security (D IM Secure) will be the Security Authority for the infrastructure within scope of CD-DAR.

g. Training Authority. The training authority is defined as a formation commander or commander of a command who is responsible for a military occupation or branch, and who has command of a learning support centre and one or more training establishments or functional centres of expertise. Assuming no significant organizational changes in the foreseeable future, the Canadian Forces School of Communications and Electronics (CFSCE) will be the Training Authority for the capabilities delivered under this project.

h. Mentorship and Capability Development. Consists in mentoring Cyber Operators at all applied rank levels to improve skills and enhance CAF cyber operations in order to maintain proficiency. More specifically the mentor is to coach, teach and mentor cyber operators to achieve their mission through continuous business transformation, skills development, collective training development and coordination, and cyber tool development and sustainment.

2.7. Key Tasks

All Cyber Operators and other users (managers, executives, commanders and their staffs) perform their tasks through a single integrated environment. These tasks include: 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.

Cyber domain SA is aggregated at CFNOC (via CD-DAR) and pushed to key personnel such as departmental executives, commanders, managers and other operational elements of the DND/CAF network such as the RCN, RCAF, CA, CJOC, CANSOFCOM, and SJS.

CD-DAR supports a number of the Cyber Operations tasks and functions that were defined in the Cyber Operations Joint Doctrine Note [R4] to support Network Operations, Support Cyber Operations, Cyber Security, and Cyber Defence scenarios. DCO tasks and functions will be further analyzed at a later time.

2.8. User Characteristics

As discussed in Section 2.1, CD-DAR will provide a near real-time view into the Command Network and the assigned network's security status. CD-DAR will also help ensure that systems are not negatively

impacted by adverse effects by continuously monitoring the DND/CAF networks with the assistance of cyber operators. Cyber Operators are the personnel tasked with Cyber security and DCO.

2.8.1. Cyber Operators

Cyber Operators are the backbone of the Cyber Force. They are the personnel, at all rank levels, with the primary role to "detect, recognize and identify hostile or otherwise unauthorized cyber entities and to assist in the destruction, neutralization, suppression or otherwise elimination of the enemy in and through cyberspace."

Cyber Operators conduct DCO, liaise and work collaboratively with OGDs and agencies, as well as with Canada's allies to enhance the DND/CAF ability to provide a secure cyber environment. They monitor CAF digital communication networks to detect and respond to unauthorized network access attempts and provide cyber support to meet the operational requirements of the elements of the CAF Cyber Operator Skill Sets.

The Cyber Operators trade are not to be confused with the Aerospace Telecommunications and Information Systems Technicians (ATIS), Army Communication and Information System Specialists (ACISS), Naval Combat Information Operators (NCIOP), and Naval Communicators (NAVCOMM) trades. These military occupations are primarily concerned with the setup, installation, operation and maintenance of communications networks and ITI while Cyber Operators are focused on overseeing and protecting ITI from hostile threats and denying the use of cyberspace by hostile forces. All 26 jobs for the Cyber Operators (CYBER OP, 00378) can be performed by Regular or Reserve Force personnel except for the most senior job in the occupation: Cyber Advisor.

Cyber Operators are trained and educated in the art of Cyber Warfare with specific attention to:

a. The nature of Cyberspace and the Cyber Domain;

b. Threats, Threat Actors and their Impact on Cyberspace;

c. Principles and techniques in detection, recognition, identification and attribution of all natures of cyber entities;

d. Principles and techniques in DCO, including Internal Defensive Measures (IDM) and Response Actions (RA); and

e. Tactics, Techniques and Procedures for:

   i Cyber Support Coordination,

   ii Command and Control,

   iii Cyber Reconnaissance,

   iv Cyber Surveillance,

v Cyber Incident Handling,

vi Cyber Forensics,

vii Cyber Threat Identification, and

viii Cyber Operations Centre functions.

3. DESIGN AND CONCEPT GUIDANCE

CD-DAR will enable DND/CAF Cyber security operations and provide the CFNOC/DEFSOC with the ability to provide Cyber SA, defend DND/CAF network environments and conduct DCO. To this end, the capability must be able to perform several mandatory functions.

While it is expected that several Cyber security tools will be necessary to fulfill the requirements for CD-DAR, notionally, the key functional elements or components sought may be functionally represented as follows: [R31]

a. The ability to maintain situation awareness, through a Common Operating Picture, of alerts, threats, and remediation across the DND/CAF Command Network, and to feed situational awareness to processes for decision on, and execution of, responses through standardized interfaces and supporting automated workflows for the decision support to the command element, and the implementation of responses as directed;;
b. An ability to create and maintain an authoritative Cyber Data Repository (CDR) that includes multi-source cyber intelligence data to be integrated (hosted and interoperated with applications and a trusted repository) into the assigned Command Network as one cohesive system;
c. An ability to perform automated Cyber Entity and Event Discovery (CEED) to rapidly identify and track, all assets (authorized and non-authorized) connected to the Command Network and assess their attributes for vulnerability, configuration, risk and patch compliance;
d. An ability to perform automated Cyber Security Monitoring and Actions (CSMA) to rapidly identify and track, all assets (authorized and non-authorized) connected to the Command Network and assess their attributes for vulnerability, configuration, risk and patch compliance;
e. An ability to conduct Cyber Defence Analysis and implement Decision Support (CDADS) to continuously collect, retain, and analyze cyber threat information on the Command Network environment and detect and characterize suspicious activity, provide context for risk and vulnerability assessments in near real-time;
f. An ability to perform automated Task Management (TM) to adaptively and dynamically identify, contain and eradicate a threat; and
g. An ability to utilize an integrated Operational Training System (OTS) for cyber operators.

ANNEX A describes each of these notional functional elements and Figure 3 below provides functional components interrelationships.

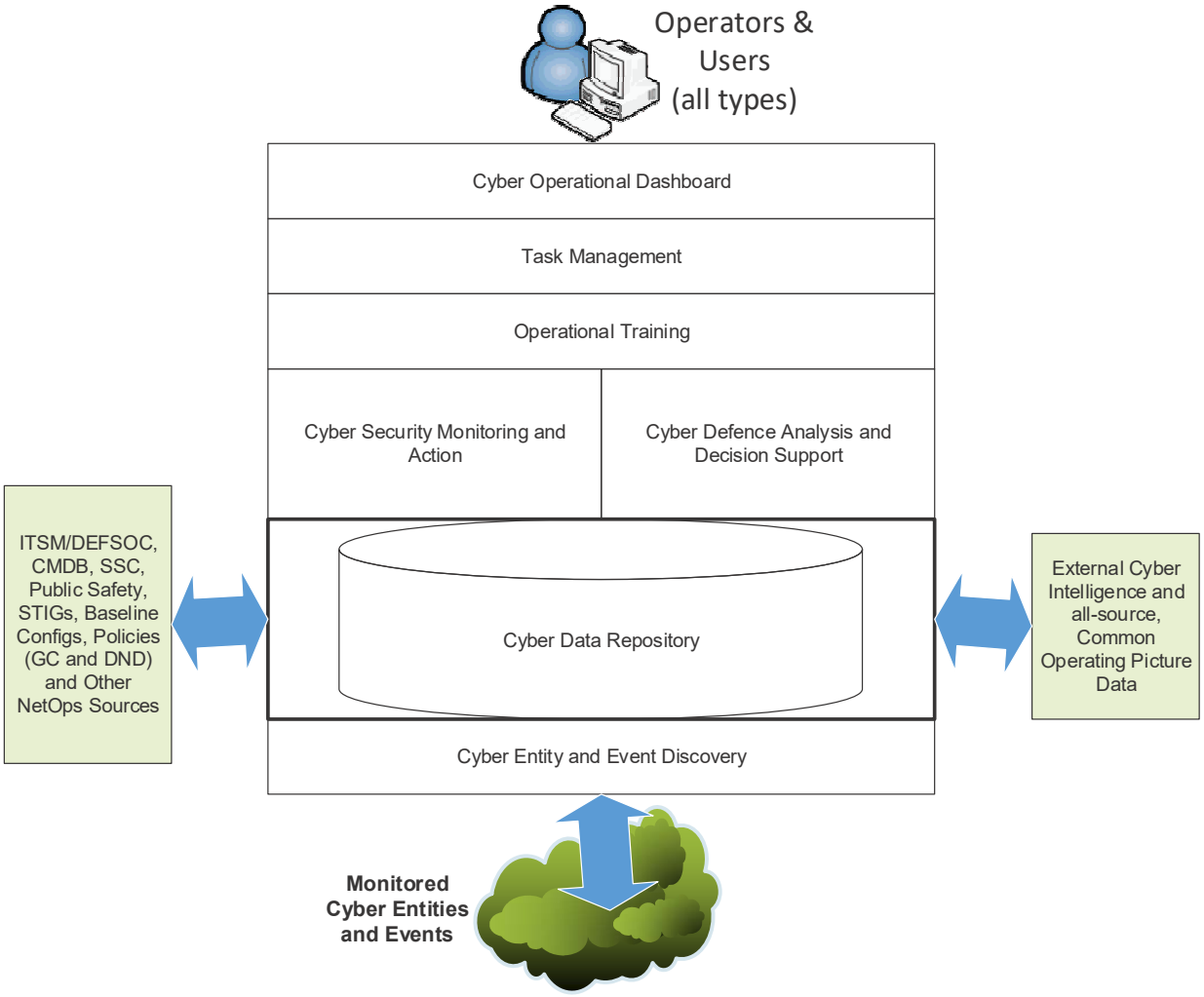


Figure 3 - CD-DAR Functional Components Interrelationships

4. SYSTEM EFFECTIVENESS REQUIREMENTS

4.1. General Requirements

This section defines the system effectiveness requirements for CD-DAR as understood at this point in project development. These requirements address the complete capability and must be further defined in concert with the development of the CONOPS, in order to balance the technological capabilities available at project implementation with the personnel and operating procedures. The System Effectiveness Requirements cover the following areas:

a. Operability;
b. Survivability;
c. Maintainability;
d. Availability;
e. Reliability;
f. Environmental Sustainability;
g. Safety and Health; and
h. Delivery Requirements.

The system effectiveness requirements have been captured in Chapter 8 – Requirements Table of this document, and complemented by the Performance Objective (PO) requirements presented in section 6.

4.1.1. Levels of Requirement / Performance Criteria

In specifying the different performance requirements, two levels of measurement will be used: Mandatory or Desirable.

4.1.1.1. Mandatory

A mandatory requirement is a criterion that must be met to ensure the CD-DAR solution will achieve the minimum acceptable performance and operational requirements. Performance thus designated, is deemed to be so important that even if a potential solution meets all other mandatory criteria and all desirable criteria, but fails to meet one mandatory criterion, that solution will be rejected. Within this document, the word "must" is considered synonymous with mandatory.

4.1.1.2. Desirable

Desirable requirements are used to promote more sensitive evaluations of solution items that meet all mandatory requirements. A Desirable requirement describes a performance requirement where performance better than the stated mandatory level is deemed to have significant operational value. The words "should" or "could" are to be considered synonymous with desirable.

4.1.2. Caveat on Levels of Measurement

The stipulation of a mandatory criterion presumes that it is achievable at reasonable cost. However, should any mandatory criterion subsequently be determined to be impractical for technical or budgetary reasons, then that criterion will be reassessed. Performance criteria set in the SOR can only be changed with the concurrence of the Project Director in consultation with the Project Manager.

4.2. Operability

CD-DAR will be considered operational when the functional requirements (Section 8), POs (Section 6) and user acceptance criteria (Section 4) have been met.

4.3. Survivability

The capability must be effective in all operating environments, as identified in section 2.2 of this SOR, as the CD-DAR solution will be integrated into the host network as an internal capability. The System must, to the greatest extent possible, be designed to survive the threats identified in section 2.3 of this SOR, through the use of adaptive technology and analytics incorporated into the CD-DAR solution.

4.4. Maintainability

As a primary and critical system for DCO, CD-DAR will be used by Cyber Operators, Managers, Executives and other Operators on a 24/7 basis. The System's reliability, availability, and maintainability requirements must support this operational need and must be supported and maintained in accordance with the CONSUP in section 2.5 outlined within this SOR.

The system must be repaired and operating as determined through the Security Categorization (formerly Statement of Sensitivity) and the Security Authorization and Accreditation (SA&A) process. Security Categorization Security categorization is a process to determine the expected injuries from threat compromise and the level of these expected injuries with respect to the security objectives of confidentiality, integrity, and availability and a first document iteration is completed during the Definition phase of the project, while the SA&A process defines IT security risk management of the information systems.

The System must make use of health monitoring and control functions[13] within the existing CAF infrastructure to monitor and maintain the nominal operation of CD-DAR.

The System architecture must be developed in such a way that individual equipment can be repaired, maintained, and/or replaced with minimal impact on the operation of the capability.

Planned outages, required for planned system maintenance and upgrades, must be relatively infrequent and of short duration. In order to maintain operational tempo, the system must be able to be restored to its minimal operational configuration (to be defined at a later time) rapidly. Therefore, every reasonable

[13] The term "health" here refers to the nominal operation of the CD-DAR system

attempt must be made to restore minimum operational configuration or better as a result of an unplanned outage and leading to full nominal operation.

The capability is expected to be deployed on standard commercial grade hardware platforms. As such, the System's hardware configuration must meet the maintainability requirements for this hardware. In addition, any developmental software must be developed using industry best practices to ensure a high level of reliability and ease of maintenance.

It is expected that both the user community and functionality of the System will need to evolve over time. To support the need to evolve, the System must apply industry best practices and guidelines to ensure that the capability's software and system are:

a. Scalable – The addition of users and/or endpoints must not result in unacceptable performance degradation;
b. Extensible – The integration of additional functionality must not require major changes to the architecture of the existing solution or its individual components/sub-components; and
c. Adaptable/Modifiable – Changes to existing functionality must not require major changes to the architecture of the existing solution or its individual components/sub-components.

4.4.1. Maintainer Acceptance

Maintainer acceptance must be achieved prior to final acceptance of the capability (as defined in section 4.4). Maintainer acceptance will be authorized by ADM(IM). As in the case of user acceptance, maintainer acceptance must occur in two phases:

a. IOC acceptance; and
b. FOC acceptance.

Maintainer acceptance at each phase will require the completion of a series of activities, as defined in the IOC and FOC Certificates (to be developed at a later time). Upon completion of all the activities for IOC or FOC, the Acceptance Authority (ADM(IM)) must either "Fully Accept", "Not Accept" or "Accept with Conditions" the CD-DAR solution. For anything other than "Fully Accept", the Acceptance Authority must provide direction as to the necessary corrective action in order to achieve full acceptance.

4.5. Availability

In order to maintain operational tempo, the system must be able to be restored to its minimal operational configuration (to be defined at a later time) rapidly. Therefore, every reasonable attempt must be made to quickly restore minimum operational configuration or better as a result of an unplanned outage and leading to full nominal operation. Planned outages, as required for planned maintenance and upgrades, also need to be of a short duration.

The CD-DAR must be able to perform localized monitoring, analysis, and support responsible decision-making within disconnected, intermittent, and geographically limited regional networks even when it is disconnected from a central management point. The deployed CD-DAR solution must render the same

availability level as the enduring capability while operating in disconnected, intermittent, and geographically limited environments.

4.6. Reliability

In order to meet the required operational availability, CD-DAR must be highly reliable as defined by the availability of the CD-DAR capabilities, with a relatively low failure rate.

4.7. Environmental Sustainability

The CD-DAR solution must meet the DND standards for environmental stewardship. The DND and the CAF adopted the following code of environmental stewardship [R40]. The DND and the CAF must:

1. integrate environmental concerns with other relevant concerns including those from operations, finance, safety, health and economic development in decision-making;
2. meet or exceed the letter and spirit of all federal laws;
3. improve the level of environmental awareness throughout the DND and the CAF through environmental awareness training, and encourage and recognize the actions of personnel leading to positive impacts on the environment;
4. recognize that the life cycle aspects of hazardous material management (initial selection, procurement, use, handling, storage, transportation and disposal) is an essential factor in all planning with particular emphasis on determining whether the material should even be acquired given its characteristics (see DAOD 4003-1, *Hazardous Materials Management*);
5. ensure that environmental considerations are integrated into procurement policies and practices;
6. practice pollution prevention in day-to-day activities and operations by seeking cost-effective ways of reducing the consumption of raw materials, toxic substances, energy, water, and other resources, and of reducing the generation of waste and noise; and
7. acquire, manage and dispose of lands in a manner that is environmentally sound, including the protection of ecologically significant areas.

4.8. Safety and Health

The solution must not generate health or safety concerns for the operators over and above those imposed by the operational environment. It must comply with all the DND/CAF health and safety codes.

4.9. Delivery Requirements

TBD

5. SUB-SYSTEM EFFECTIVENESS REQUIREMENTS

N/A - Sub-System Levels are not defined prior to the Definition phase of the project.

6. PERFORMANCE MEASURES

Performance measures are presented below in the form of System Performance Parameters using the following conventions:

a. ***Performance Indicator***: A title indicating the type of performance measure.

b. ***Performance Description***: A description of the performance indicator.

c. ***Quantity (Qty)***: The value of the indicator to be achieved.

d. ***Unit of Measure***: The unit in which the quantity is measured.

6.1. System Level Measures

This section identifies a series of performance indicators that will be quantified in the Definition project phase.

Table 5 - System Performance Parameters [R2]

ID (Performance Objective)	Performance Indicator	Description	Qty
PO.1	Entity Connection	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.)	TBD
PO.2	Automatic Attack Prevention	Automatically prevent an attack at the network or host through a protective tool such as Host Intrusion Prevention System	TBD
PO.3	SIEM Audit Entry and Console Display	Generate an audit entry and send it to a Security Information and Event Management (SIEM) console	TBD
PO.4	Automatic File Anomalous Activity Analysis	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	TBD
PO.5	Automatic IDS Alert and Console Display	Trigger an Intrusion Detection System (IDS) alert and send both the alert and the associated packets to the SIEM console	TBD
PO.6	Entity Attribute Detection	Recognize that a detected cyber entity within the DND/CAF cyberspace is either human or non-human, and discover its key attributes	TBD
PO.7	Entity Identification and Location	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)	TBD
PO.8	Intent Characterization	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	TBD

ID (Performance Objective)	Performance Indicator	Description	Qty
PO.9	Monthly System Log Data Queries and Collection	Query each month's log data for any system in the DND/CAF cyberspace and gather results	TBD
PO.10	Malicious Entity Correlation and Alerts	Generate pivot tables to assist cyber operators in identifying entities with similar or connected malicious behaviour and prompt the operator to initiate response actions	TBD
PO.11	Criteria-based Entity Packet Capture Retrieval	Retrieve a week's worth of indexed Packet Capture (PCAP) from online storage for any entity criteria such as set of Internet Protocol (IP) addresses, hostnames, ports, user accounts or content	TBD
PO.12	Event of Concern Recognition and Action	Recognize an event of concern and tag it as benign or fill out a case and escalate it to Tier 2	TBD
PO.13	Infected Host Isolation	Isolate an infected host	TBD
PO.14	Incident Owner Identification and Contact	Identify and contact a sysadmin, security officer or operations officer at a site whose system was involved in a potential incident	TBD
PO.15	IDS Life Cycle Deployment, to Fleet to Sensors	Develop, download, test and deploy IDS signatures to a fleet of sensors	TBD
PO.16	Multiple System or Account Response Plan Development	Identify, analyze, and develop a response plan to an intrusion involving multiple systems or accounts	TBD
PO.17	Tier 2 and 3 Malware Payload Analysis	Provide Tier 2 to Tier 3 analysis of the payload for a new strain of malware	TBD
PO.18	Downed Data Feed Identification and Recovery	Identify and recover from a downed sensor or data feed	TBD
PO.19	Stakeholder Major Incident Briefings	Gather stakeholders and brief them on details of a major incident in progress	TBD
PO.20	IDS Fleet Signature or SIEM Content Scrub	Do a monthly/quarterly scrub of all signatures deployed to an IDS fleet or content deployed to SIEM	TBD

ID (Performance Objective)	Performance Indicator	Description	Qty
PO.21	Major Patch Test and Recommendation	Test and recommend a major patch to the enterprise	TBD
PO.22	Serious Incident Content Analysis and Documentation	While adhering to legal chain-of-custody standards, analyze and document the contents system involved in a serious incident • Deploy an Incident Response Team • Recover data • Triage data	TBD
PO.23	Forensics Remote Analysis	Remotely extract Forensics Artifacts for analysis and evidence • Files • Processes • Memory • Registry • Logical hard drive image • Bit level hard drive image	TBD
PO.24	Adversarial Intent Assessment	Assess the actions and potential motives and intentions of an adversary operating on constituency networks	TBD
PO.25	Analysis Reporting and Presentation	Report analysis results and present legally admissible evidence	TBD
PO.26	Life Cycle Operationalization of Custom Analytics Tools	Develop, deploy, and make operational complex custom detection and analytics tools such as Perl scripts and SIEM use cases	TBD
PO.27	SOP Lifecycle DCO Baselining	Revise, review, and baseline an internal defensive cyber security operations standard operating procedure (SOP)	TBD
PO.28	New Procedure Exercising	Exercise Cyber Operator shifts on new procedures	TBD
PO.29	Emerging Threat and Vulnerability Notification	Inform Cyber Operators on new and emerging threats and vulnerabilities	TBD
PO.30	New Defence Technique Operationalization	Make new defense techniques operational with new tactics, techniques and procedures	TBD

ID (Performance Objective)	Performance Indicator	Description	Qty
PO.31	Tool-based New Defence Technique Operationalization	Make new defence techniques operational with new tools to address newly identified and prioritized threats	TBD
PO.32	Security Posture Evolution	Evolve the overall security posture (policy, processes, tools) of vulnerable DND/CAF cyberspace to address newly identified and prioritized vulnerabilities	TBD
PO.33	Data Loss	Zero packet loss at the monitoring points of presence.	TBD
PO.34	Data Loss	Zero event log loss.	TBD
PO.35	Data Loss	Zero information loss.	TBD
PO.36	Data Integrity	Verifiable data integrity.	TBD
PO.37	Data Monitoring	Prevent adversaries from detecting the presence of (and evading) monitoring capabilities.	TBD
PO.38	Data Event 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.	TBD
PO.39	Survivability	Support the survivability of the Cyber security and DCO capabilities, even when portions of the cyberspace are compromised or contested.	True
PO.40	Document Disclosure Protection	Protect from disclosure sensitive documents and records maintained by the defensive cyber security operations capability.	True

6.2. Sub-System Level Measures

N/A – Sub-System Levels are not defined prior to the Definition phase of the project.

7. PERSONNEL AND TRAINING REQUIREMENTS

In order to be effective, the System must be operated and supported by trained resources assigned to the key roles, as defined in Section 2.6 above.

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

7.1. Personnel – Staffing

Staffing of CD-DAR will include military personnel, public servants and contracted personnel.

7.1.1. Operational Staff

The system will be utilized by DND/CAF personnel who are assigned accredited user roles and authorities within CD-DAR. Additional temporary and permanent users will be added as required to meet the data entry requirements for operations and to meet mission mounting and mission closure materiel transfer and surge capacity. Operational staff for these positions will be filled through Cyber Uplift.

7.1.2. Maintenance Staff

For the purposes of Options Analysis, it is assumed the system will be maintained by DND/ CAF personnel who are assigned the respective support function in support of the CD-DAR. As part of the Definition Phase, an ISS analysis will be conducted, along with continued industry engagement, to determine a maintenance strategy that returns the best blend of performance, flexibility and value for money. Today, CFNOC is the de-facto Life Cycle Materiel Manager (LCMM) for most of the existing Cyber equipment and capability-specific software.

7.2. Training

In order to successfully operate and support CD-DAR, an effective training regime must be provided. Initial cadre training will be provided as part of the Project scope. However, recurrent training will be delivered as part of the capability's ISS, and will be the responsibility of the OA. The OA may delegate authority over maintenance and administrator training to the TA.

The CD-DAR training program must provide Incremental project-related content training, based on a train the trainer approach, integrated to the existing DND/CAF DCO training program [R32].

The solution must deliver the necessary training for appropriate users representing the OA, 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 IOC and a steady state training system to ensure FOC.

7.2.1. Training Environment

The vision for CD-DAR is 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.

The solution must provide an integrated OTS 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 CD-DAR 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; and

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.

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

7.2.2. Training Deliverables

Training deliverables will include, but may not be limited to:

a. 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, and

   ii. On-going continuous training, both individual and collective Cyber Operator focussed; and

b. OMCD capability is planned in order to mentor Cyber Operators to improve skills and enhance CAF cyber operations in order to maintain proficiency.

8. REQUIREMENTS TABLE

The requirement tables in this section describe the preliminary requirements to meet the objectives of the CD-DAR project. They are organized around the analysis framework depicted in Figure 4 below. The framework was originally developed in version 1 of the Technical Architecture Document (TAD) and employed to draft the High Level Mandatory Requirements (HLMR) for CD-DAR.

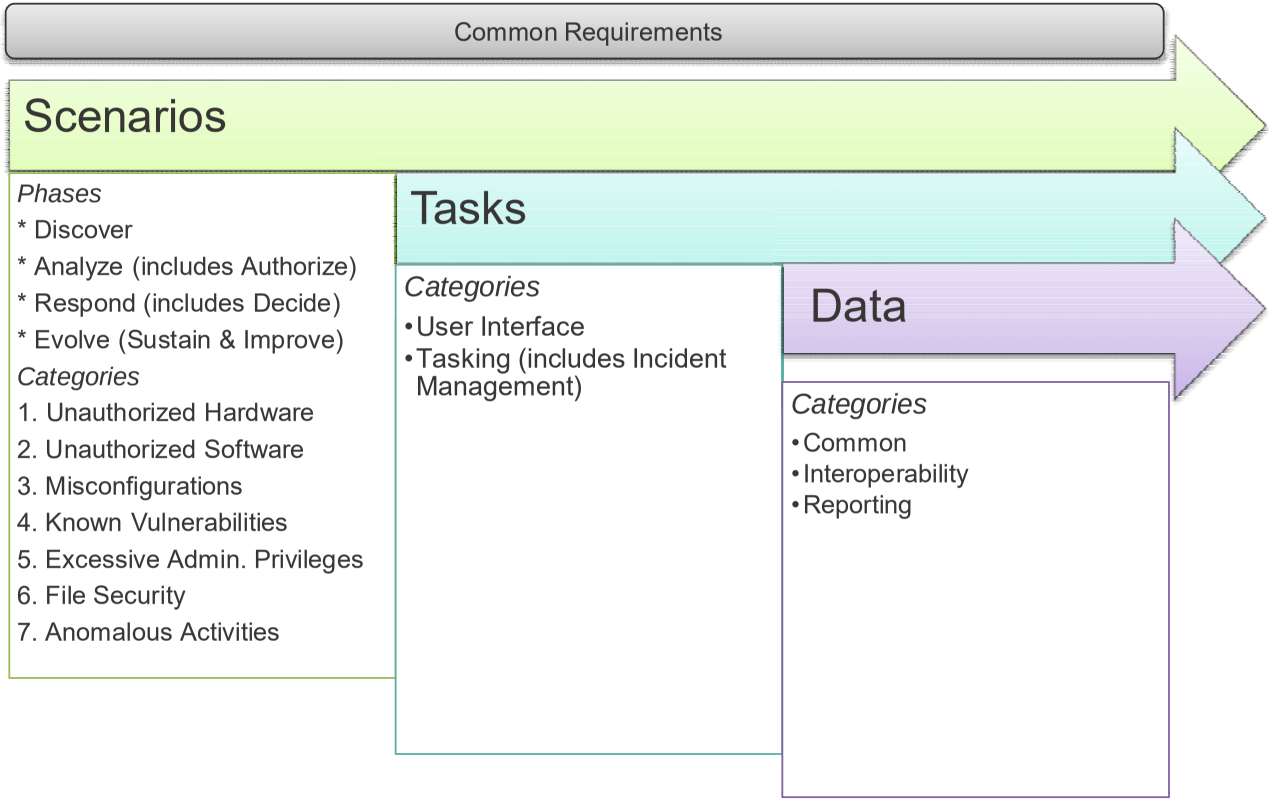


Figure 4 - CD-DAR Analysis Framework

Figure 5 - CD-DAR Framework Comparison

8.1. Operational Common Requirements

This table includes general requirements that do not logically fit into any of the other more specific categories of requirements.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OCR-001	Network Management	The system must support network locations that are managed by DND, CAF, third-parties, and where management is shared.	Mandatory	Mandatory	all
OCR-002	Security Controls	The capability must address CIS critical security control 1-5 in a rapid and a highly automated manner.	Mandatory	Mandatory	all
OCR-003	Cyber Domain Scenarios	The system must provide the capability to address the following cyber domain scenarios: unauthorized hardware, unauthorized software, misconfigurations, known vulnerabilities, unauthorized administrative privileges, file security and anomalous activities.	Mandatory	Mandatory	all
OCR-004	Life Cycle Phases	The system must provide functionality required for each of the life cycle phases of each cyber domain scenario, namely: discovery, analysis, response and evolution.	Mandatory	Mandatory	all
OCR-005	Integrated Implementation.	Project capabilities must be integrated with operational capabilities at the time of implementation. Examples include existing training environment [Health Monitoring and Control, OTS], decision support tasks, and data encryption.	Mandatory	Mandatory	all
OCR-006	Environmental Stewardship	The system must meet the DND/CAF standards relevant to CD-DAR. Examples include environmental stewardship and health and safety codes.	Mandatory	Mandatory	all

8.2. Operational Discovery Requirements

This table includes requirements to determine the current state of all cyber asset entities and network usage in the cyber environment, most of it automatically and rapidly processed. Note that Administrative Privilege requirements also cover Anomalous Activity requirements.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		Common Discovery			

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
ODR-001	Entity Discovery	The system must provide real-time continuous identification and tracking of cyber asset entities and network usage.	Mandatory	Mandatory	1,2
ODR-002	Actual State Discovery	The system must provide an automated process and tools to ingest existing and newly identified actual state data sets and metadata.	Mandatory	Mandatory	1,2
ODR-003	Discovery Timestamp	The system must have a date and time associated with each instance of actual state information and identify the collection source.	Mandatory	Mandatory	1,2
ODR-004	Discovery Context	The system must include the mechanism to define actual state dependent on context and scope.	Mandatory	Mandatory	1,2
		Hardware Discovery			
ODR-005	Hardware Discovery	The system must identify and track hardware devices (physical and virtual) that are on the network, authorization status and who (by individual, access group, or organization) manages each device.	Mandatory	Mandatory	1,2
ODR-006	Hardware Discovery Timing	The system must identify and collect hardware inventory information on all devices on the network on a scheduled and ad-hoc basis as specified by authorized users.	Mandatory	Mandatory	1,2
ODR-007	Hardware Identification	The system must provide a unique identifier (which may vary within device type) that supports device persistent of any network location changes for each device on the network.	Mandatory	Mandatory	1,2
ODR-008	Hardware Location	The system must collect data to enable staff to physically locate the hardware devices.	Mandatory	Mandatory	1,2
ODR-009	Hardware Validation Information	The system must collect additional hardware data (e.g., subcomponents, attached peripheral devices, local account information), for managed and properly configured devices and with credentials sufficient to validate actual inventory data.	Mandatory	Mandatory	1,2
ODR-010	Behaviour based Hardware type	The system should detect the type of each hardware device based upon its network behavior.	Desirable	Desirable	1,2
		Software Discovery			
ODR-011	Software Discovery	The system must identify and track software products that are on the device for each hardware device (physical and virtual) on the network within system boundaries, authorization status, and who (by individual, access group, or organization) manages each software product.	Mandatory	Mandatory	1,2
ODR-012	Software Identification	The system must provide a unique identifier (e.g., Common Platform Enumeration [CPE], Software Identification Tags) for each software product that is used to identify instances of installed software products and components, including version number, across devices on the network.	Mandatory	Mandatory	1,2
ODR-013	Software Discovery Timing	The system must identify and collect software inventory information on DND/CAF defined and scoped devices on the network on a scheduled and ad hoc basis as specified by authorized users.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
ODR-014	Software Discovery Details	The system must collect additional software data (e.g., software components, component digital fingerprints) for managed and properly configured devices, with credentials sufficient to validate actual inventory data.	Mandatory	Mandatory	1,2
ODR-015	Software Ownership and Status	The system must document and record software inventory information, including product name, owner/manager, and operational status.	Mandatory	Mandatory	1,2
		Configuration Discovery			
ODR-016	Configuration Discovery	The system must identify and collect configuration settings (including the actual values) for specific software and hardware products on DND/CAF defined and scoped devices on the network on a scheduled, event-driven, and ad hoc basis as specified by authorized users.	Mandatory	Mandatory	1,2
ODR-017	Configuration Identification	The system must support a unique identifier for each configuration setting collection across devices on the network.	Mandatory	Mandatory	1,2
		Vulnerability Discovery			
ODR-018	Vulnerability Discovery	The system must identify and collect vulnerability information, including time first detected and time remediated, on all devices on the network on a scheduled, event-driven, and ad hoc basis as specified by authorized users.	Mandatory	Mandatory	1,2
ODR-019	Vulnerability Mapping	The system must collect appropriate data to map actual vulnerabilities to the on-network hardware and software inventories.	Mandatory	Mandatory	1,2
ODR-020	Vulnerability Discovery Methods	The system must discover vulnerabilities on the network using unauthenticated or authenticated methods.	Mandatory	Mandatory	1,2
ODR-021	Vulnerability Patch Data Discovery	The system must provide a secure patch management process that will automatically identify and acquire patches for all products and systems (commercial or government).	Mandatory	Mandatory	1,2
ODR-022	Vulnerability Patch Scope Discovery	The patch management system must be accessible from authorized locations, assets and users.	Mandatory	Mandatory	1,2
		Administrative Privileged Discovery			
ODR-023	User Trust Information	The system must collect and report trust information on all users.	Mandatory	Mandatory	1,2
ODR-024	Actual User Trust Level	The system must determine the granted trust level for each authorized user.	Mandatory	Mandatory	1,2
ODR-025	Required User Trust Level	The system must determine the required operational trust level for each user.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
ODR-026	Actual Training Information	The system must collect and report training[14] information for each authorized user in the DND/CAF.	Mandatory	Mandatory	1,2
ODR-027	Actual Training Information Details	The system must include training completed, knowledge demonstrated, and/or certification obtained, depending on DND/CAF policy.	Mandatory	Mandatory	1,2
ODR-028	User Training Information	The system must support collection, monitoring, and reporting of general security-related training applicable to all users.	Mandatory	Mandatory	1,2
ODR-029	Role Training Information	The system must support collection, monitoring, and reporting for security-related training based on the roles authorized/assigned to the user.	Mandatory	Mandatory	1,2
ODR-030	Completed Training Information	The system must collect data associated with completed training and security-related behavior documentation required for security-related behavior requirements, for which the user is assigned or authorized, in order to provide measurable data elements for the creation of automated security checks.	Mandatory	Mandatory	1,2
ODR-031	Completed Process Level Training	The system must generate reports of successful completion of required training available to the systems and processes that can monitor/enforce access.	Mandatory	Mandatory	1,2
ODR-032	Employee Credential Information	The system must collect and report credential information associated with accounts and users credentials (e.g., X.509 certificates, user identifiers, public/private key pairs) issued to each user employed by the DND/CAF (including contractors).	Mandatory	Mandatory	1,2
ODR-033	Credential Changes	The system must collect and report credential information associated with accounts and users credential reissuance, revocation, and suspension enforcement mechanisms and their configuration for all applicable credential types.	Mandatory	Mandatory	1,2
ODR-034	Credential Password Complexity	The system must collect and report credential information associated with accounts and users password complexity enforcement mechanisms and their configuration for all in-scope accounts at the DND/CAF.	Mandatory	Mandatory	1,2
ODR-035	User and Account Privileges	The system must collect and report information on privileged and non-privileged accounts and users.	Mandatory	Mandatory	1,2
ODR-036	Physical Access Privileges	The system must collect and report physical access authorizations issued to each user employed by the DND/CAF.	Mandatory	Mandatory	1,2

[14] Training includes: training, knowledge and/or certification, depending on DND/CAF policy.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
ODR-037	Account Status	The system must collect and report account status (restrictions, enablement, revocation, in authorization time window, etc.) implemented for every in-scope account at the DND/CAF.	Mandatory	Mandatory	1,2
		File Discovery			
ODR-038	Document Control Discovery	The system must automatically monitor the network for DND/CAF data labels on specified file types to support inventorying of data holdings.	Mandatory	Mandatory	1,2
ODR-039	Digital Chain of Custody Discovery	The system technologies and processes must collect information regarding GC investigative requirements for digital chain of custody.	Mandatory	Mandatory	1,2
		Anomalous Activity Discovery			
ODR-040	User Activity Discovery	The system must provide real-time continuous monitoring of user activity.	Mandatory	Mandatory	1,2
ODR-041	Network Traffic Discovery	The system must provide real-time continuous monitoring of network traffic.	Mandatory	Mandatory	1,2
ODR-042	Packet Capture Data	The system must ingest PCAP data.	Mandatory	Mandatory	1,2
ODR-043	Out of Band Network Traffic Discovery	The system must provide out-of-band collection and retention of raw network traffic in CAF cyberspace (internal, in-bound, and out-bound).	Mandatory	Mandatory	1,2
ODR-044	Network Traffic Retention.	The system must meet the following data retention guidelines: IDS alerts and SIEM-correlated alerts:	Mandatory	Mandatory	1,2
ODR-045	Endpoint Discovery.	The system must provide an Endpoint Detection and Response (EDR) capability to identify the installation of malware in the form of APT on an endpoint device.	Mandatory	Mandatory	1,2
ODR-046	Endpoint Discovery Details	The system must 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).	Mandatory	Mandatory	1,2
ODR-047	Endpoint Data Discovery	The system must provide an ability to remotely gather memory images or files for forensics investigation.	Mandatory	Mandatory	1,2
ODR-048	Endpoint Hard Drive Discovery	The system must provide an ability to gather hard drive images (server, workstation or mobile) for forensics investigation.	Mandatory	Mandatory	1,2
ODR-049	Internetwork Data Discovery	The system must collect and report information related to the implementation of policies that control the flow of data between enclaves at one or more levels in the protocol stack. This information must support the enforcement of these policies.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
ODR-050	Open Source Intelligence Discovery	The system must ingest reputable, sustainable and adjustable cyber Open Source Intelligence (OSINT) service feed(s).	Mandatory	Mandatory	1,2

8.3. Operational Analysis Requirements

This table includes requirements to identify and recommend courses of action for unauthorized security and defensive conditions. The requirements are further grouped into the following sub-categories:

1. *Authorization*: requirements to distinguish between authorized and unauthorized conditions.
2. *Detection*: requirements to find unauthorized conditions and to recommend courses of action.
3. *Prioritization*: requirements to facilitate prioritization of responses.

Note that Administrative Privilege requirements also cover Anomalous Activity requirements.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		Common Analysis			
OAR-001	Decision Support Analysis	The system must provide an ability to perform Decision Support tasks.	Mandatory	Mandatory	1,2
		Common Authorization			
OAR-002	Authoritative State	The system must include the mechanism to define the desired state for an entity dependent on the entity context (e.g., Organizational Unit and system linkage) and the scope of the capability's attributes.	Mandatory	Mandatory	1,2
OAR-003	Enterprise Data Analysis	The system must be able to perform enterprise data analysis.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OAR-004	Authoritative SA&A Data	The system must ingest security assessment & authorization data.	Mandatory	Mandatory	1,2
OAR-005	Authorized Data Changes	The system must provide an automated process and tools to ingest existing and newly identified authoritative data sets and metadata.	Mandatory	Mandatory	1,2
OAR-006	Change Authorized Data	The system must develop authoritative data to support automated identification of changed entities.	Mandatory	Mandatory	1,2
		Hardware Authorization			
OAR-007	Authorized Hardware	The system must document and record DND/CAF approved (i.e., authorized devices) hardware inventory information, including device type (e.g., router, workstation, firewall, printer), owner/manager, and operational status.	Mandatory	Mandatory	1,2
OAR-008	Authorized Hardware Input Methods	The system must allow manual or batch creation of DND/CAF approved device data (e.g., through integration with external asset information repositories or through business rules).	Mandatory	Mandatory	1,2
		Software Authorization			
OAR-009	Authorized Software Data	The system must establish and maintain a software inventory, unique identifiers for software, and other properties such as the manager of the software.	Mandatory	Mandatory	1,2
OAR-010	Authorized Software Input Methods	The system must allow manual or batch creation of authorized software data (e.g., through integration with external asset information repositories or through business rules).	Mandatory	Mandatory	1,2
		Configuration Authorization			
OAR-011	Authorized Configuration	The system must create, update, and maintain the security configuration settings benchmarks for target hardware devices and software products.	Mandatory	Mandatory	1,2
OAR-012	Authorized Configuration Details	The system must store, process, maintain, track changes, and distribute security configuration benchmarks, including DND/CAF exceptions (including the justification and compensating countermeasures), as determined by authorized users (with authorization being granted per benchmark).	Mandatory	Mandatory	1,2
OAR-013	Authorized Configuration Information	The system must permit authorized users to select and compose a set of security configuration benchmarks to establish an authorized security configuration baseline for a cyber asset entity or group of assets.	Mandatory	Mandatory	1,2
OAR-014	Authorized Asset Level Configurations	The system must record authorized security configuration settings that are set and managed by authorized users within benchmarks for specific software and hardware products.	Mandatory	Mandatory	1,2
		Vulnerability Authorization			

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OAR-015	Authorized Vulnerabilities	The system must provide authoritative vulnerability data through complete coverage of the CVEs identified by the National Vulnerability Database (NVD) and equivalent vulnerability information from other useful sources.	Mandatory	Mandatory	1,2
		Administrative Privilege Authorization			
OAR-016	Authorized Administrator Identity	The system must ingest accredited administrator identity data.	Mandatory	Mandatory	1,2
OAR-017	Authoritative User Identity	The system must ingest accredited user identity data.	Mandatory	Mandatory	1,2
	Departmental Authoritative Authentication Data	The system must leverage departmental authentication and credential capabilities.	Mandatory	Mandatory	1,2
OAR-018	Access Authorization Trust Level	Make key trust level authorization attributes available to the systems and processes that monitor access.	Mandatory	Mandatory	1,2
OAR-019	User Access Trust Requirements	Provide, to control systems and processes that monitor access, key trust attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility or an account on a system.	Mandatory	Mandatory	1,2
OAR-020	Unauthorized User Behaviour	The system must provide collection mechanisms or processes to detect and record/report information to identify when an authorized user does not meet attribute-based security-related behavior requirements, and when an authorized user's security-related behavior requirements have expired.	Mandatory	Mandatory	1,2
OAR-021	User Access Training Requirements	The system must provide, to control systems and processes that monitor access, key training attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility or an account on a system.	Mandatory	Mandatory	1,2
OAR-022	User Access Credentials Requirements	The system must provide, to control systems and processes that monitor access, key credential attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility or an account on a system.	Mandatory	Mandatory	1,2
OAR-023	Data Credential Types	The system must employ an approved process for issuing different credential types and defining authentication requirement policies for access to various facilities, systems, and information.	Mandatory	Mandatory	1,2
		File Authorization			
OAR-024	Authorized Document Control	The system must provide authorized data for DND/CAF data labelling on specified file types to support security policy compliance checks.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		Anomalous Activity Authorization			
OAR-025	Internetwork Encryption Discovery	The system must collect data associated with the boundary encryption policy and the encryption policy required for a network flow across a boundary to provide measurable data elements for the creation of automated security checks.	Mandatory	Mandatory	1,2
		Common Detection			
OAR-026	Unauthorized Asset Detection	The system must detect unauthorized cyber asset entity conditions (i.e., unauthorized hardware and software, misconfigurations, known vulnerabilities and unauthorized administrative privileges) and anomalous activities.	Mandatory	Mandatory	1,2
OAR-027	Multiple Source Analysis	The system must be able to correlate multiple data sources and supporting assessment processes through pre-made and custom-made reports and queries.	Mandatory	Mandatory	1,2
OAR-028	Decision Point Analysis	The system must support the correlation of cyber asset entity and network usage information, in conjunction with decision points, specific to the determination of actual versus desired state function of the decision point.	Mandatory	Mandatory	1,2
OAR-029	Authoritative Data Correlation	The system will provide an automated means to relate authoritative data from multiple sources in pre-defined ways.	Mandatory	Mandatory	1,2
OAR-030	Threat Integration	The system must provide an automated, effective and reliable threat intelligence fusion capability that enables multi-source and multi-caveat analytics.	Mandatory	Mandatory	1,2
OAR-031	Change Data Detection	The system must automatically identify changed entities.	Mandatory	Mandatory	1,2
OAR-032	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.	Mandatory	Mandatory	1,2
OAR-033	Cyber Analysis Alerts	The system must provide a method to create, modify, remove, view and send alerts.	Mandatory	Mandatory	1,2
OAR-034	Authorized SIEM Data	The system must ingest SIEM data for all cyber domain scenarios.	Mandatory	Mandatory	1,2
OAR-035	Misconfiguration Compromises	The system must have the ability to detect indicators of compromise.	Mandatory	Mandatory	1,2
OAR-036	Decision Point Assessment	The system must include decision point capabilities to support the ingestion of machine-readable policies to measure the actual state against the desired state for ongoing assessment of security controls.	Mandatory	Mandatory	1,2
OAR-037	Authoritative Threat Intelligence Data	The system must ingest threat intelligence data.	Mandatory	Mandatory	1,2
OAR-038	Interface Assessment Scheduling	The system must permit scheduled or on-demand assessment.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OAR-039	Interface Assessment Requests	The system must provide an automated process and tools to request tailored assessments.	Mandatory	Mandatory	1,2
OIR-040	Assessment Results Retention	The system must retain assessment results for a DND/CAF-defined period to enable enterprise security posture reporting and trending.	Mandatory	Mandatory	1,2
OAR-041	Retrospective Analysis and Audits	The system must support retrospective analysis and audit functions.	Mandatory	Mandatory	1,2
OAR-042	Historical Reporting	The system must provide tailored analysis of short-term historical data (e.g. crafted queries, use case modelling) that supports the ability to log findings, trigger alerts, and generate reports.	Mandatory	Mandatory	1,2
OAR-043	Historical Correlation	The system must provide correlation of historic events, trends and behaviours to real-time events and reconstruct activities based on context.	Mandatory	Mandatory	1,2
OAR-044	Historical Audits	The system must provide audit tools that support manual and automated (scheduled and ad hoc) queries and reports.	Mandatory	Mandatory	1,2
OAR-045	Physical Access Control Systems Integration	The system must integrate with IP-addressable Physical Access Control Systems (PACS) components to support all CD-DAR capabilities.	Mandatory	Mandatory	1,2
		Hardware Detection			
OAR-046	Hardware Analysis	The system must collect appropriate data to match actual to authorized DND/CAF approved (i.e., authorized devices) hardware inventory, including when detected and if the device is in desired state.	Mandatory	Mandatory	1,2
		Software Detection			
OAR-047	Software Analysis	The system must detect for unauthorized software execution by blocking based on an authorized software list specific to each hardware device. At a minimum, resident executables must be blocked.	Mandatory	Mandatory	1,2
OAR-048	Software Change Detection	The system should detect for whitelist changes and software installation actions.	Desirable	Desirable	1,2
OAR-049	Software Source Integrity Verification	The system should provide source integrity verification for all tool components, such as digital fingerprints for each software file used within the system.	Desirable	Desirable	1,2
OAR-050	Malware Detection and Protection	The system should execute detect/protect for malware (including, as configured, all on whitelisted software, and software not behaving as expected) at a rate comparable to existing anti-virus products, and provide a means for removing malware in time to prevent it from executing.	Desirable	Desirable	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		Configuration Detection			
OAR-051	Security Configuration Analysis	The system must enumerate differences from the security configuration benchmark, including differences that provide greater protection or reduce risk further than the benchmark.	Mandatory	Mandatory	1,2
		Vulnerability Detection			
OAR-052	Vulnerability Impacts	The system must provide an automated process and tools to assess the impact of known vulnerabilities (e.g. CVE data) on cyber asset entities.	Mandatory	Mandatory	1,2
OAR-053	Vulnerability Impact Scope	The system vulnerability impact assessment must include cyber asset entity type and configuration to a complete system or service perspective.	Mandatory	Mandatory	1,2
OAR-054	Vulnerability Kill Chain	The system vulnerability impact assessment must consider the entire cyber kill chain.	Mandatory	Mandatory	1,2
OAR-055	Vulnerability Compromise Probability	The system vulnerability impact assessment must identify the likelihood of a compromise.	Mandatory	Mandatory	1,2
OAR-056	Patch Analysis	The system vulnerability impact assessment must automatically assess the need for installation of patches on network assets.	Mandatory	Mandatory	1,2
OAR-057	Vulnerability Detection	The system must update tools in a timely manner to be able to detect vulnerabilities that have been identified by the Government CVEs.	Mandatory	Mandatory	1,2
OAR-058	Vulnerability Reports	The system must generate vulnerability assessment reports.	Mandatory	Mandatory	1,2
		Administrative Privileges Detection			
OAR-059	User Trust Analysis	The system must determine when a user issued a credential does not meet trust level requirements and when that user's trust level has expired.	Mandatory	Mandatory	1,2
OAR-060	User Trust Level Screening	The system must employ an established screening/indoctrination process before granting access to various levels of sensitive material.	Mandatory	Mandatory	1,2
OAR-061	Security Checks Automation	Have security checks that provide the basis for automating the monitoring, reporting, and prioritizing of trust deficiencies in DND/CAF cyber environment.	Mandatory	Mandatory	1,2
OAR-062	Authorized User Behaviour	The system must collect and report security-related behavior indicators for each authorized user in the DND/CAF.	Mandatory	Mandatory	1,2
OAR-063	User Training Policy Validation	The system must validate the existence of DND/CAF training policies and report on their enforcement. DND/CAF training policies must document how long a training/knowledge/certification activity is valid before it expires and the user is required to repeat the training/knowledge/certification.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OAR-064	User Activity Task Automation	The system must utilize automated security checks to provide the basis for automatically identifying, monitoring, reporting, prioritizing, and reviewing security-related behavior deficiencies in DND/CAF cyber environment.	Mandatory	Mandatory	1,2
OAR-065	Training Grace Period	The system should define appropriate grace periods for training associated with each security-related behavior requirement.	Desirable	Desirable	1,2
OAR-066	User Authentication	The system must verify authentication mechanisms implemented for every in-scope account at the DND/CAF.	Mandatory	Mandatory	1,2
OAR-067	User Account Verification	The system must verify default accounts/passwords are NOT enabled on in-scope systems.	Mandatory	Mandatory	1,2
OAR-068	User Credentials Process Validation	The system must continuously monitor key outputs from the credential issuance and authentication definition processes to detect when a credential or authentication action deviates from established standard(s).	Mandatory	Mandatory	1,2
OAR-069	Policy Authentication	The system must verify that all authentication mechanisms deployed on in-scope systems across the DND/CAF implement the appropriate authentication policy.	Mandatory	Mandatory	1,2
OAR-070	User Credential Type Validation	The system must verify that all credential types have appropriate expiration, reissuance, and revocation policies.	Mandatory	Mandatory	1,2
		File Detection			
OAR-071	Data Label Authorization	The system must assess data label information on specified file types to support security policy compliance checks	Mandatory	Mandatory	1,2
OAR-072	Digital Chain of Custody Process	The system technologies and processes must assess compliance with GC investigative requirements for digital chain of custody.	Mandatory	Mandatory	1,2
		Anomalous Activity Detection			
OAR-073	Anomalous Activity Detection	The system must provide the capability to detect anomalous activities.	Mandatory	Mandatory	1,2
OAR-074	Anomalous Activity Authorization	The system must ingest baseline data that enables the detection of acceptable and unacceptable network traffic conditions and user activity.	Mandatory	Mandatory	1,2
OAR-075	Historical Anomaly Analysis	The system must provide an analysis of enterprise data to detect suspicious and anomalous activity.	Mandatory	Mandatory	1,2
OAR-076	Advanced Threat Detection	The system must provide features and data supporting the hunt for Advanced Persistent Threats (APTs), insider threats, and indicators.	Mandatory	Mandatory	1,2

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OAR-077	Endpoint Detection Capabilities	The system must provide an Endpoint Detection and Response (EDR) capability to analyze the presence of malware in the form of APT on an endpoint device.	Mandatory	Mandatory	1,2
OAR-078	Forensics Data	The system must ingest forensic data.	Mandatory	Mandatory	1,2
OAR-079	Endpoint Forensics Data	The system must provide an ability to gather forensics data about endpoint devices (such as processes ran, files accessed and created, applications/commands/scripts used, user accounts used, and applications installed).	Mandatory	Mandatory	1,2
OAR-080	User Activity Analysis	The system must provide real-time continuous analysis of contextualized user activity.	Mandatory	Mandatory	1,2
OAR-081	User Activity Correlation	The system must correlate user activity across domains/caveats.	Mandatory	Mandatory	1,2
		Common Prioritization			
OAR-082	Task Prioritization	The system must provide an indicator for priorities of current mitigation tasks.	Mandatory	Mandatory	1,2
OAR-083	Risk Management	The system must support processes and tools to continuously identify, define, integrate and automate Risk Management of the DND/CAF cyber domain.	Mandatory	Mandatory	1,2
OAR-084	Risk Management Details	The Risk Management processes and tools must include: information categorization, security control selection, safeguard evaluation, configuration compliance check, and risk calculation.	Mandatory	Mandatory	1,2
OIR-085	Risk Management Scores	The system must include the mechanism to define risk scores for the difference between actual and desired states (including scores that reflect a reduction in risk).	Mandatory	Mandatory	1,2
OAR-086	Asset Criticality	The system must support prioritizing remediation actions by identifying critical cyber asset entities.	Mandatory	Mandatory	1,2

8.4. Operational Response Requirements

This table includes requirements to respond to unauthorized security and defensive conditions.
Note that Administrative Privilege requirements also cover Anomalous Activity requirements.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		Common Response			
ORR-001	Contingency Plan Response	The system must have a contingency plan to restore and reconstitute full information system functionalities and the capability to apply new or additional security safeguards to prevent future compromise.	Mandatory	Mandatory	3
ORR-002	Risk Management Response	The system must support processes and tools for automated Risk Management response actions.	Mandatory	Mandatory	3
ORR-003	Event Responses	The system must be able to set automatic event response.	Mandatory	Mandatory	3
ORR-004	Predetermined Response Automation	The system must enable pre-determined technical responses to be automatically actioned for documented events which exceed documented thresholds.	Mandatory	Mandatory	3
ORR-005	Predetermined Response Override	The system must provide a manual override option for pre-authorized responses.	Mandatory	Mandatory	3
ORR-006	Infrastructure Segmentation Response	The system must include automated tools to segment portions of the infrastructure with newly identified security vulnerabilities in a timely manner.	Mandatory	Mandatory	3
ORR-007	Filtering Response	The system must enforce one or more filtering policies using one or more decision points. These filtering policies control what data can enter or exit the systems.	Mandatory	Mandatory	3
		Hardware Response			
ORR-008	Unauthorized Hardware Response	The system must provide an automated process and tools to respond to the detection of unauthorized cyber hardware conditions.	Mandatory	Mandatory	3
		Software Response			
ORR-009	Unauthorized Software Response	The system must provide an automated process and tools to respond to the detection of unauthorized cyber software conditions.	Mandatory	Mandatory	3
ORR-010	Whitelist Change Response	The system must protect against whitelist changes and software installation actions.	Mandatory	Mandatory	3
ORR-011	Unauthorized Software Execution Response	The system must protect against unauthorized software execution by blocking based on an authorized software list specific to each hardware device. At a minimum, resident executables must be blocked.	Mandatory	Mandatory	3
		Vulnerability Response			
ORR-012	Response Documentation	The system should provide text for system administrators to explain clearly and simply how to correct the vulnerability.	Desirable	Desirable	3

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
ORR-013	Authoritative Patch Data	The system must provide a secure patch management process that will automatically install and verify patches for all products and systems (commercial or government).	Mandatory	Mandatory	3
ORR-014	Vulnerability Response	The system must identify and collect vulnerability information, including time first detected and time remediated, on all devices on the network on a scheduled, event-driven, and ad hoc basis as specified by authorized users.	Mandatory	Mandatory	3
		Administrative Privileges Response			
ORR-015	User Trust Level Response	The system must enforce access using available key trust level authorization attributes.	Mandatory	Mandatory	3
ORR-016	User Training Response	The system must enforce user access to a facility or an account on a system based on key training authorization requirements.	Mandatory	Mandatory	3
ORR-017	Behaviour Deficiency Response	The system should utilize automated security checks to provide the basis for automatically correcting security-related behavior deficiencies in the DND/CAF cyber environment.	Desirable	Desirable	3
ORR-018	User Credentials Response	The system must enforce user access to a facility or an account on a system based on key credential authorization requirements.	Mandatory	Mandatory	3
		File Response			
ORR-019	Document Control Response	The system must enforce the use of DND/CAF labeling on specified file types to support inventorying of data holdings.	Mandatory	Mandatory	3
ORR-020	File Security Response	The system must provide protection to the confidentiality, integrity, and authenticity of data at rest, in transit, or in process via cryptography.	Mandatory	Mandatory	3
		Anomalous Activity Response			
ORR-021	Endpoint Response	The system must provide an Endpoint Detection and Response (EDR) capability to respond to the installation of malware in the form of APT on an endpoint device.	Mandatory	Mandatory	3

8.5. Operational Evolve Requirements

This table includes requirements to sustain and improve the overall security and defensive capabilities delivered by this project at the performance levels implemented at FOC.

The requirements are further grouped into the following sub-categories:

4. *In Service Support*: general requirements regarding sustainment of project capabilities after implementation.

5. *Availability*: requirements regarding uninterrupted access to operational capabilities.
6. *Capability Distribution*: requirements regarding overall capability configurations.
7. *Scalability*: requirements regarding capability capacities.
8. *Flexibility*: requirements regarding the operational ability to expand and reconfigure capabilities.
9. *Capability Development*: requirements regarding best practice improvements.
10. *Training*: requirement regarding competency development.
11. *Change Acquisition*: requirements regarding customized and commercial acquisition of capabilities.
12. *Change Testing;* requirements to verify compliance of capabilities to requirements prior to implementation.
13. *Change Implementation*: requirements regarding the implementation of capabilities into operations.
14. *Resilience*: requirements regarding recovery of capabilities from disruption to operations.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		In Service Support			
OER-001	Capability Lifespan	The capability must remain effective, adaptive and in service throughout its 10-year life-cycle.	Mandatory	Mandatory	7,9
		Availability			
OER-002	Type of Sites	The system must support reliably available and contested sites.	Mandatory	Mandatory	7,9
		Capability Distribution			
OER-006	Central Processing	The system must provide the ability to centrally monitor, analyze, decide and respond to IT infrastructure conditions.	Mandatory	Mandatory	7,9
OER-007	Central Processing Organization	The System core component must be Centrally installed at the Canadian Armed Forces Network Operations Centre (CFNOC) in Ottawa, Ontario.	Mandatory	Mandatory	7,9
OER-008	Ownership Distribution	The system must maximize functionality and performance using locations that are managed by DND, CAF or third-parties or where management is shared.	Mandatory	Mandatory	7,9
OER-009	Deployment Enablement	The System deployable components must be delivered, entered in DND/CAF inventory and ready for deployment on an as required basis.	Mandatory	Mandatory	7,9
		Scalability			

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OER-010	Scalability	To support the need to evolve, the System must apply industry best practices and guidelines to ensure that the capability's software and system are: Scalable – The addition of users and/or endpoints must not result in unacceptable performance degradation.	Mandatory	Mandatory	7,8,9
OER-011	Site Capacity	The system must support high, medium, and small scale capacity sites.	Mandatory	Mandatory	7,8,9
OER-012	Capacity Impact	The system must minimize the use of network bandwidth and end point system resources to limit potential impact to mission/business operations.	Mandatory	Mandatory	7,8,9
OER-013	Data Capacity	The system must store, process, and provide data for large Federal organizations (using the threshold of up to one million devices) while maintaining adequate timeliness, completeness, and accuracy for applicable capabilities	Mandatory	Mandatory	7,8,9
OER-014	Temporary Capacity	The system must be able to provide temporary increases in computing, networking and/or storage capabilities to meet surge requirements without negatively impacting the rest infrastructure.	Mandatory	Mandatory	7,8,9
		Flexibility			
OER-015	Extensibility	To support the need to evolve, the system must apply industry best practices and guidelines to ensure that the capability's software and system are: Extensible – The integration of additional functionality must not require major changes to the architecture of the existing solution or its individual components/sub-components.	Mandatory	Mandatory	7,8,9
OER-016	Adaptability	To support the need to evolve, the system must apply industry best practices and guidelines to ensure that the capability's software and system are: Adaptable/Modifiable – Changes to existing functionality must not require major changes to the architecture of the existing solution or its individual components/sub-components.	Mandatory	Mandatory	7,8,9
		Capability Development			
OER-017	Capability Development Functions	The OMCD must train users to perform system functionality with initial training, on-going training, professional development, mentoring and coaching.	Mandatory	Mandatory	7,8,9
OER-018	Capability Development Support	OMCD team(s) must support Cyber security operations.	Mandatory	Mandatory	7,8,9

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OER-019	Capability Development Structure	The capability must provide DND/CAF and professional services in the form of OMCD team(s) to coach, teach and mentor the cyber operators at all applied rank levels.	Mandatory	Mandatory	7,8,9
OER-020	Capability Development Location	The OMCD capability must train users to operate wherever cyber operations occurs, such as Cyber Security Operations Centres and deployed missions.	Mandatory	Mandatory	7,8,9
OER-021	Capability Development Co-location	The OMCD team(s) must be co-located with the delivered capability during implementation and throughout its life-cycle.	Mandatory	Mandatory	7,8,9
OER-022	Capability Development Levels	The OMCD team(s) must mentor Cyber Operators at all levels to improve skills and enhance CAF cyber operations in order to maintain proficiency.	Mandatory	Mandatory	7,8,9
OER-023	Capability Development Maturity	The OMCD team(s) must support the business transformation of the delivered capabilities to achieve NIST Level 5 security operations capability.	Mandatory	Mandatory	7,8,9
OER-024	Capability Development Environment	The OMCD capability must train users to perform capabilities in domestic, international, centralized and deployed environments.	Mandatory	Mandatory	7,8,9
		Training			
OER-025	Training Scope	The system must provide a training capability to capture best practices and learn from previous operations.	Mandatory	Mandatory	7,9
OER-026	Training Simulation Capability	The system must provide a training simulation capability to support collective operational training in a customizable operational context.	Mandatory	Mandatory	7,9
OER-027	Training Simulation Scope	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.	Mandatory	Mandatory	7,9
		Change Acquisition			
OER-028	Developmental Software Practices	Any developmental software must be developed using industry best practices.	Mandatory	Mandatory	7,8,9
OER-029	Development Threat Information	The system must collect and report information related to the implementation of modeling threats to information systems, including identifying vulnerabilities and corresponding countermeasures.	Mandatory	Mandatory	7,8,9
OER-030	Development Security Information	The system must collect and report information related to the implementation of methods for secure information system development and enforce secure information system development policies.	Mandatory	Mandatory	7,8,9

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OER-031	Development Deployment Security Information	The system must collect and report information related to the implementation of methods for secure information system deployment and enforce secure information system deployment policies.	Mandatory	Mandatory	7,8,9
OER-032	Development Policy Vulnerability	The system should identify relevant regulations, governance processes, compliance polices, and security CONOPS that malicious actors could exercise to compromise the information and information system, and perform risk assessment to evaluate impact to information and information systems.	Desirable	Desirable	7,8,9
OER-033	Development Vulnerability Mitigation	The system should implement methods to minimize vulnerabilities or weakness during information system design activities.	Desirable	Desirable	7,8,9
OER-034	Development Coding Security	The system should implement secure coding practices (including fail-safe coding, critical code and data protection, and secure code re-use) during information system development.	Desirable	Desirable	7,8,9
OER-035	Development Components Acquisition and Disposal	The system should execute secure acquisition (e.g., verify procurement supply chain, chain-of-custody) and disposal of components and data as part of information system deployment.	Desirable	Desirable	7,8,9
OER-036	Development Components SCRM	The system should follow Supply Chain Risk Management (SCRM) policies and procedures for baselining, tracking, and auditing the provenance of information system components (to include mitigation of counterfeits, reputation scoring, and chain of custody) for the acquisition/development of the information system.	Desirable	Desirable	7,8,9
OER-037	Development SCRM Integration	SCRM should be an integral part of the overall risk management process and include risk assessment guidance and the use of security related controls to mitigate identified risk.	Desirable	Desirable	7,8,9
OER-038	Development Component Distribution Risks	SCRM should establish a process for identifying, preventing, assessing, reporting and mitigating the risks associated with the global and distributed nature of CD-DAR product and service supply chains. The range of countermeasures selected should include appropriate risk reduction strategies and the best way to implement them.	Desirable	Desirable	7,8,9
		Change Testing			
OER-039	Capability Assessment Purpose	The Cyber Capability Assessment and Evaluation Facility (CCAEF) must research, exercise current, and test and evaluate new cyber defense and security practices and solutions within a simulated environment.	Mandatory	Mandatory	7,8,9

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OER-040	Capability Assessment Scope	The CCAEF must simulate the functionality and performance of all DND/CAF Cyber Domains and caveats within the scope of the Project.	Mandatory	Mandatory	7,8,9
OER-041	Capability Assessment Network	The CCAEF must provide a configuration managed baseline representation of each facet of all DND/CAF Cyber Domains and caveats within the scope of the Project.	Mandatory	Mandatory	7,8,9
OER-042	Capability Assessment Performance	The CCAEF must provide functional and performance evaluations of new hardware and software.	Mandatory	Mandatory	7,8,9
OER-043	Capability Assessment Configurations	The CCAEF must provide configuration changes to existing installed hardware and/or software.	Mandatory	Mandatory	7,8,9
OER-044	Capability Assessment Users	The CCAEF must provide additions or changes to the nature and number of authorized users.	Mandatory	Mandatory	7,8,9
OER-045	Capability Assessment Locations	The CCAEF must provide additions or changes to points of presence and their locations.	Mandatory	Mandatory	7,8,9
OER-046	Capability Assessment Effects	The CCAEF must provide effects on data throughput and/or bandwidth at any point within the networks.	Mandatory	Mandatory	7,8,9
OER-047	Capability Assessment Data	The CCAEF must provide the collection of system log data and SIEM data.	Mandatory	Mandatory	7,8,9
OER-048	Capability Assessment Integration	The CCAEF must integrate with existing or planned Information Technology Infrastructure test and evaluation systems.	Mandatory	Mandatory	7,8,9
		Change Implementation			
OER-049	Proposed Change Purpose	The system must provide an automated process and tools to analyze the impact of proposed DND/CAF cyberspace changes for all cyber domain scenarios except Proposed Changes.	Mandatory	Mandatory	7,8,9
OER-050	Proposed Change Scope	The system must provide an automated means to report on the impact of proposed cyberspace changes for all cyber domain scenarios except Proposed Changes.	Mandatory	Mandatory	7,8,9
OER-051	Proposed Change Policy	Proposed changes must include changes to security policy, including those needed to satisfy the requirements of this project.	Mandatory	Mandatory	7,8,9
OER-052	Proposed Change Conditions	The system must include response to threats, net new, update or removal of software, hardware, configuration or design in Proposed Changes	Mandatory	Mandatory	7,8,9
OER-053	Proposed Change Processes	The system must process all Request for Change (RFC) and Configuration Management updates.	Mandatory	Mandatory	7,8,9
		Resilience			

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OER-054	Disruption Minimization	The system must employ features that minimize the disruption to system operation.	Mandatory	Mandatory	7.9
OER-055	Disconnected, Intermittent, and Limited Environments Deployability	The system must provide a rapidly deployable, local assessment capability to support Disconnected, Intermittent, and Limited environments (e.g. ships, aircraft and austere deployments).	Mandatory	Mandatory	7.9
OER-056	Disconnected, Intermittent, and Limited Environments Recovery	The system must provide a centralized assessment capability in Disconnected, Intermittent, and Limited environments.	Mandatory	Mandatory	7.9
OER-057	Disconnected, Intermittent, and Limited Environments Bandwidth Constraints	The system must operate in Disconnected, Intermittent, and Limited environments.	Mandatory	Mandatory	7.9
OER-058	Disconnected, Intermittent, and Limited Environments Alternate Channel	The system must provide an alternate information transfer method to facilitate Disconnected, Intermittent, and Limited environments.	Mandatory	Mandatory	7.9
OER-059	Disconnected, Intermittent, and Limited Environments Alternate Channel	The system must integrate locally collected information when normal operation is restored, while not compromising information.	Mandatory	Mandatory	7.9
OER-060	Data Backup	The system must include backup capabilities for data stored over the network.	Mandatory	Mandatory	7.9
OER-061	Unplanned Outages	Unplanned outages must be of a relatively short duration (time limit not to be exceeded to be defined).	Desirable	Mandatory	7.9
OER-064	Recovery Principle	The system must be developed in such a way that individual equipment can be repaired, maintained, and replaced with minimal impact on the operation of the capability.	Mandatory	Mandatory	7.9
OER-065	Repair Timing	The system must be repaired, repaired, maintained, replaced and operating in a timely manner as determined through the Statement of Sensitivity and the Security Assessment & Authorization process.	Mandatory	Mandatory	7.9

8.6. Operational Task Requirements

This table includes requirements for working-level delivery of CD-DAR capabilities to stakeholders in the form of tasks and workflows.

The requirements are further grouped into the following sub-categories:

15. *User Interface*: requirements to make capabilities accessible to stakeholders.
16. *Tasks*: requirements to make capabilities available to stakeholders.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		User Interface			
OTR-001	User Interface Capability	The system must provide an integrated user interface to access the functionality delivered by CD-DAR.	Mandatory	Mandatory	4
OTR-002	Interface Activation Principle	The automated functionality provided by the system must be activated by users and, wherever possible by the system.	Mandatory	Mandatory	4
OTR-003	Role Based Interface Configurability	The system must provide a user-friendly configurable interface suitable to the user roles, functions and tasks.	Mandatory	Mandatory	4
OTR-004	User Optimized Interface	The system must optimize the use of the Cyber Operator's time.	Mandatory	Mandatory	4
OTR-005	NCR User Access	The system must support and permit all users (Commanders, Cyber Operators and Support Staff) concurrently located and operating within the geographic and IT Service Locale bounded by the National Capital Region	Mandatory	Mandatory	4
OTR-006	DND/CAF and SSC User Access	The system should support and permit all users (Commanders, Cyber Operators and Support Staff) concurrently located and operating within DND/CAF and SSC.	Desirable	Desirable	4
OTR-007	Canada-Bound User Access	The System must support and permit access to all users (Operational Authorities, Cyber Operators, Managers, Executives and Support Staff) concurrently located and operating outside the geographic and Service Locale bounded by the NCR but within Canada.	Desirable	Mandatory	4
OTR-008	Disadvantaged User Access	The System must support and permit access to all users (Operational Authorities, Cyber Operators, Managers, Executives and Support Staff) concurrently located and operating outside the geographic and Service Locale bounded by the NCR but internationally deployed in disadvantaged Service Locales with limited Bandwidth capabilities.	Desirable	Mandatory	4

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OTR-009	Web Based Interface	The system should be delivered in a web-based application.	Desirable	Desirable	4
		Tasking			
		Task Common			
OTR-010	Task Management Capability	The system must provide a user accessible task management capability that identifies, defines and automates tasks, processes and workflows to perform all CD-DAR functionality.	Mandatory	Mandatory	4
OTR-011	Task Incident Workflow	The system must have an automated Incident Response Workflow.	Mandatory	Mandatory	4
OTR-012	Enterprise Task Management	The system must provide a unified task management database data that relates task participants, capabilities, timing, assignment and activity data.	Mandatory	Mandatory	4
OTR-013	Task Notes	The system must provide the ability to enter and maintain notes against all types of information to address non-standard content.	Mandatory	Mandatory	4
OTR-014	Task Input Methods	The system must permit manual and batch entry of information.	Mandatory	Mandatory	4
OTR-015	Task Interoperability	The system must permit data interchange with other related systems (e.g., ticket systems, submission systems)	Mandatory	Mandatory	4
OTR-016	Task Participants	The system must uniquely identify and relate authoritative and informal roles, organizations, organizational units, teams, organizational positions, individuals and other participants involved in the tasking capability.	Mandatory	Mandatory	4
OTR-017	Task Participant Details	The system must include additional participant data such as unique identifiers; titles; reporting structure and other relationships; classification and other codes; permanent and temporary participants; and required skills, skillsets, profiles and templates.	Mandatory	Mandatory	4
OTR-018	Task Participant Functions	The system must permit searching, selecting, opening, copying attributes from another user, changing and closing of subordinate members by authorized users.	Mandatory	Mandatory	4
OTR-019	Task Participant Availability	The system must permit adding and deleting of availability of subordinate members by authorized users.	Mandatory	Mandatory	4
OTR-020	Task Participant Preferences	The system must be able to reset preferences to system defaults by authorized users.	Mandatory	Mandatory	4
OTR-021	Task Participant Work Details	The system must be able to add, modify and remove member work details (skillsets, capacity, availability) by authorized users.	Mandatory	Mandatory	4
OTR-022	Task Participant Workload Adjustments	The system must provide the ability to adjust workloads to address changing circumstances.	Mandatory	Mandatory	4

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OTR-023	Task Participant Workload Issues	The system should automatically provide alerts and warnings regarding Analyst or Workload issues.	Desirable	Desirable	4
OTR-024	Task Participant Competency Development	The system should implement coaching or training where required to address workload issues.	Desirable	Desirable	4
OTR-025	Task Participant Team Functions	The system must be able to create, move, merge and delete teams by authorized users.	Mandatory	Mandatory	4
OTR-026	Task Participant Team Composition	The system must be able to add and remove members from a team by authorized users.	Mandatory	Mandatory	4
OTR-027	Task Capabilities	The system must define the authoritative and actual type of work that can be conducted by participants and the conditions under which work is conducted.	Mandatory	Mandatory	4
OTR-028	Task Capability Details	The system must include additional tasking capability data such as accountabilities, entitlements (identity, authentication, and authorization), preferences (language, accessibility, preferred channels, and application defaults), assignments (work, non-work, assignment rules), distribution (multi-site, multi-partner), channels (immediate, deferred, single rotation) skills (activities, proficiency level and capacity) and availability (calendar, hours and shifts).	Mandatory	Mandatory	4
OTR-029	Task Activity	The system must uniquely define authoritative and track all actual interaction among participants, its content, its relationship to other interactions (requests, communications, assignments, issues, incidents, problems, workarounds, and orders) and cross-references to associated systems and processes (e.g., partner requests, tickets, services, problems, incidents, workarounds.	Mandatory	Mandatory	4
OTR-030	Task Activity Details	The system must include additional activity data such as status, participants, services requested, identification, description, classification, prioritization, assignment reason, timing, relationship with other requests and partner systems.	Mandatory	Mandatory	4
OTR-031	Task Timing	The system must include data to support the targeted and actual timing of tasks.	Mandatory	Mandatory	4
OTR-032	Task Timing Details	The system must include additional timing data such as targeted and actual start time and dates, finish time and dates, notification time and dates and durations.	Mandatory	Mandatory	4
OTR-033	Task Alerts	The system must provide an automated tasking and workflow capability for responding to a trigger or alert.	Mandatory	Mandatory	4
		Task Receipt			
OTR-034	Task Receipt Context	The system must relate tasks to define context (e.g., by symptom, root cause, response, participants, other systems).	Mandatory	Mandatory	4

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OTR-035	Task Receipt Identification Interoperability	The system should permit access to Identify Management solution to confirm entitlement.	Desirable	Desirable	4
		Task Analysis			
OTR-036	Repetitive Analysis Tasks	The system must automate repetitive analysis tasks.	Mandatory	Mandatory	4
OTR-037	Task Analysis Interoperability	The system should permit interoperability with the knowledge systems used by providers to analyze and resolve activities.	Desirable	Desirable	4
		Task Assignment			
OTR-038	Task Assignment Functions	The system must be able to view, delete, complete, reactivate and reassign activities by authorized users.	Mandatory	Mandatory	4
OTR-039	Task Function Conditions	The system must limit reassignments, deletions and completions to open activities; Reactivations to closed activities by authorized users.	Mandatory	Mandatory	4
OTR-040	Task Assignment Automation	The system must maximally automate assignments through an assignment engine driven by Participant and Capability data.	Mandatory	Mandatory	4
OTR-041	Task Assignment Resourcing	The system must traverse the Participant Structure according to Assignment Logic to find the most appropriate resources to execute and complete the work assignment.	Desirable	Desirable	4
OTR-042	Task Assignment Strategies	The system must support various assignment strategies (e.g., by participant topology, skill-requirements, resource availability, channel, priority, timing).	Desirable	Desirable	4
OTR-043	Multiple Task Assignments	The system must support multiple assignments.	Desirable	Desirable	4
OTR-044	Task Assignment Logic Interoperability	The system should permit access to other systems that support assignment logic.	Desirable	Desirable	4
OTR-045	Task Assignment Override	The system must permit manual override of assignments.	Desirable	Desirable	4
OTR-046	Task Assignment Prioritization	The system must be able to create, activate, deactivate, increase priority and decrease priority of routing rules by authorized users.	Mandatory	Mandatory	4
OTR-047	Task Assignment Administrative Adjustments	The system must permit temporary changes to assignment logic to deal with short-term administrative requirements (e.g., personnel reassignments, local infrastructure failures).	Mandatory	Mandatory	4

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OTR-048	Task Reassignment Options	The system must permit various reassignment options such as specified member (by dropdown list, by partial name search), next available member, self, profile characteristic (complexity, language, etc.).	Mandatory	Mandatory	4
OTR-049	Task Reassignment Justification	The system must require a reason for reassignment.	Mandatory	Mandatory	4
OTR-050	Task Assignment Tracking	The system must track the assignment of work based on the nature of the work and the availability of skilled resources to address it.	Mandatory	Mandatory	4
OTR-051	Task Assignment Events	The system must record and relate all assignments, events and states in the activity database for unified viewing.	Mandatory	Mandatory	4
OTR-052	Task Assignment Notifications	The system must provide notifications regarding assignment progress, especially alerts and warnings that notify Agents of potential or actual threats to service standards (e.g., deadline warnings to permit adjustments prior to service impacts; expected delays, completion of task).	Mandatory	Mandatory	4
OTR-053	Task Progress	The system must provide a capability to track and monitor progress of workflow tasks.	Mandatory	Mandatory	4
OTR-054	Task Traceability	The system must report on progress/findings back to the process [or sub-system or module] that originated the tasking.	Mandatory	Mandatory	4
		Task Reporting			
OTR-055	Task Reporting	The system must provide the ability to handle information from various views to support efficient data handling (e.g., by Role, by Individual, by various attributes such as Language, Types).	Mandatory	Mandatory	4
OTR-056	Task Reporting Views	The system must permit viewing of performance information from a number of views (e.g. Member, Activity, Status) and levels (Agent, Team) to determine performance levels.	Mandatory	Mandatory	4
OTR-057	Task Reporting Modes	The system must permit online viewing and printing of performance information. Custom reporting and standard reporting must be supported.	Mandatory	Mandatory	4
OTR-058	Task Document Functions	The system must be able to view, move, modify, delete and reinstate associated documents by Authorized users.	Mandatory	Mandatory	4
OTR-059	Task Reporting Queries	The system must be able to flexibly search for and retrieve relevant activities based on various criteria related to Activity and Assignment (e.g., Person, Skill Required, Availability, Request, Type of Work, Performance, Level in the Assignment Database).	Mandatory	Mandatory	4
OTR-060	Task Reporting Criteria	Will permit multiple value and multiple criteria searches.	Mandatory	Mandatory	4
OTR-061	Task Reporting Organization	Will permit sorting, grouping and filtering of searched results.	Mandatory	Mandatory	4

8.7. Operational Information Requirements

This table includes common requirements to handle the information needed by CD-DAR.

The requirements are further grouped into the following sub-categories:

17. *Common Data*: requirements regarding the general management of information.
18. *Interoperability*: requirements regarding the flow of information between functions and locations.
19. *Reporting*: requirements regarding the output and display of information to stakeholders.

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
		Common Data			
OIR-001	Enterprise Data Management	The system must provide a unified data repository that acts as the authoritative cyber entity and event data source for all CD-DAR data.	Mandatory	Mandatory	5,6
OIR-002	Enterprise Data Management Details	The system must 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.	Mandatory	Mandatory	5,6
OIR-003	Data Identification	The system must use a standard naming convention to classify and uniquely define all cyber entities.	Mandatory	Mandatory	5,6
OIR-004	Data Asset Identification Details	The system entity data must include as a minimum of: entity type(s), networks, virtual/physical entity, applications/software, configuration, border devices, entity criticality, logical and physical state and location, physical zone, Cross Domain Solution info, administrative accounts, and ownership (refer to Appendices 2 and 3 in RFI).	Mandatory	Mandatory	5,6
OIR-005	Data Currency and Coverage	The system must ensure that attribute information associated with an object is current within xx-hours coupled with the xx% coverage for all objects.	Mandatory	Mandatory	5,6
OIR-006	Data Input Method	The system must allow manual or batch creation of DND/CAF data (e.g., through integration with external asset information repositories or through business rules).	Mandatory	Mandatory	5,6
OIR-007	Data Logging	The system must perform logging.	Mandatory	Mandatory	5,6
		Data Interoperability			

Requirement ID	Requirement Name	Requirement Detail	IOC Level	FOC Level	HLMR #
OIR-008	Partner Interoperability	The system must provide automated data exchange capabilities with partners.	Mandatory	Mandatory	5,6
OIR-009	Common Interoperability	The system must support data interchange and sharing between all CD-DAR capabilities using standard interfaces and/or API, standard formats and CD-DAR standard data structures including those for assets, users, analysis and boundaries	Mandatory	Mandatory	5,6
OIR-010	Intelligence Sharing Standards	The system must support data interchange and sharing between all CD-DAR capabilities and external capabilities using standard interfaces and/or API, standard formats and CD-DAR standard data structures.	Mandatory	Mandatory	5,6
OIR-011	Cross Domain Workstations Data	The system must operate in DND/CAF user-based Cross-Domain Solution environment (e.g. multiple security domains on a single workstation).	Mandatory	Mandatory	5,6
OIR-012	Cross Domain Servers Data	The system must operate in DND/CAF server-side Cross Domain Solution environment.	Mandatory	Mandatory	5,6
		Reporting			
OIR-013	Reporting Distribution	The system must provide a customizable method to generate reports, view report results and send reports.	Mandatory	Mandatory	5,6
OIR-014	Asset Maps Formats	The system must provide a network map of all cyber asset entities in various formats, including visual.	Mandatory	Mandatory	5,6
OIR-015	Asset Maps Distribution	The system must provide IT Asset Maps for monitored Cyber Asset Entities to the Commanders: through email, through an appropriate software tool, or through an appropriate method within the JBMC, and in accordance with the requirements of the Security Assessment & Authorization process.	Mandatory	Mandatory	5,6
OIR-016	Status Reports Schedule	The system must provide Cyber Status Reports on demand or on a pre-defined schedule.	Mandatory	Mandatory	5,6
OIR-017	Status Reports Scope	The system must provide Cyber Status Reports to the Commanders for monitored Cyber Asset Entities: such as telephone calls, SMS Text messaging, email, through an appropriate software tool, or through an appropriate method within the JBMC.	Mandatory	Mandatory	5,6
OIR-018	Status Reports Process	The system must provide Cyber Status Reports defined by the Commanders to be delivered through an automated process based on a notification subscribers list.	Mandatory	Mandatory	5,6

9. PROJECT REFERENCES

URL Address	Hyper Link Text	Link
https://finland.emc.com/collateral/white-papers/rsa-advanced-soc-solution-sans-soc-roadmap-white-paper.pdf	Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, May 2015, SANS Institute:	R2
https://collaboration-img.forces.mil.ca/sites/DGCyber/D_Cyber_FD/SSO_CRD/Shared Documents/121018-UU-3136-4-PL-CD-DAR-Project Brief Draft V1.2.docx	CD-DAR Project Brief, v1.2, 12 October 2018	R3
	Joint Doctrine Note - Cyber Operations, Article 0608, February 2017	R4
http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf	Canada's Defence Policy: Strong, Secure, Engaged (SSE)	R6
\\dcs-prk-pv02890\imgdiv$\0_DG_C~1\0_DCYB~1\SSO&CR~1\05-PRO~1\000-OP~1\00-BUS~1\CURREN~1	CD-DAR Business Case Analysis (BCA), v1.9	R7
https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/lead-security-agencies.html	Lead security Agencies	R9
http://collaboration-admpa.forces.mil.ca/sites/DI/Departmental%20management/project-pad.pdf	Project Approval Directive, Department of National Defence, 16 December 2014	R12

http://collaboration-admpa.forces.mil.ca/sites/DI/Departmental%20management/project-pad.pdf	Definition of the Project Approval Process, PGM 1/13, 13 August 2013	R13
https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html	Government of Canada Cyber Security Event Management Plan	R18
https://www.hsdl.org/?view&did=734860	DoD Cyber Operations Lexicon 2010-2011, Page 8, Section 16	R24
http://pubs.drdc-rddc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3DSYSNUM=532776	CF Cyber Operations in the Future Cyber Environment Concept, DRDC CORA TM 2009-058, December 2009, pg. 2.	R25
http://publications.gc.ca/collections/collection_2016/scrs-csis/PS73-2-2016-06-03-eng.pdf	CSIS 2018 Security Outlook Potential Risks and Threats, 2016	R26
ttp://www.forces.gc.ca/en/about-reports-pubs-report-plan-priorities/2016-section-i-organizational-expenditure-overview.page	2016-17 Report on Plans and Priorities	R27
http://cid-bic.forces.mil.ca/Cid/Data/Documents/3349/Draft%20Preliminary%20SOR%20-%20ITI%20in%20Sp%20of%20C2,%20v0.1,%2016%20Nov%2018.pdf	Information Technology Infrastructure in Support of Command and Control (ITI in Sp of C2) Preliminary SOR, 16 November 2018	R30
https://buyandsell.gc.ca/cds/public/2017/12/18/637ad14072ef720ed0c51146992cca46/ABES.PROD.PW__QE.B049.E26594.EBSU000.PDF	CD-DAR RFI	R31
https://collaboration-img.forces.mil.ca/sites/DGCyber/D_Cyber_FD/SSO_CRD/Shared%20Documents/1	CD-DAR Project Charter	R32

61129-UU-3136-1-PJT-DG%20Cyber-CSA%20Project%20Charter-Final_as_signed.docx		
	Project Management Principles and Policies for DND, May 1999	R34
https://www.canada.ca/en/treasury-board-secretariat/services/information-technology-project-management/project-management/outcome-management-guide-tools.html	Outcome Management Guide and Tools	R37
https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf	Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee	R38
	CD-DAR CONSUP, V1.1	R39
http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-4000/4003-0.page	DAOD 4003-0, Environmental Protection and Stewardship	R40
	CD-DAR Project Interdependency Management	R41

10. GLOSSARY

Glossary Term	Glossary Description
Artificial Intelligence	Artificial Intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions) and self-correction.
Asset Entity	Actual and desired Hardware, Software identity, Configuration, known vulnerabilities and administrative privileges.
Command Network	Communications network that connects an echelon of command with some or all of its subordinate echelons for the purpose of command and control. Consolidated Secret Network Infrastructure (CSNI) is a part of the Command Network within DND/CAF. Included under the Command Network are Comd-Net Extensions and Interfaces, and Deployable DWAN systems. Throughout this document "Command Network" will be used to include the above terms.
Computer Network Attack	A military operation to disrupt, deny, degrade, or destroy information resident in Information Technology System (ITS) or the ITS themselves. [Source: Interim DND/CF Policy on CF Computer Network Operations, 21 November 2013]
Computer Network Defence	Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within information systems or networks. Also - an activity undertaken to protect against, monitor for, analyze, detect and respond to unauthorized activity within or directed against ITS. [Source: Interim DND/CF Policy on CF Computer Network Operations, 21 November 2013]

Glossary Term	Glossary Description
Computer Network Exploitation	An intelligence collection activity intended to access, gather data from or control an ITS of an adversary, potential adversary or other Government of Canada approved party. [Source: Interim DND/CF Policy on CF Computer Network Operations, 21 November 2013]
Computer Network Operations	Comprised of computer network attack, computer network defence and computer network exploitation. [Source: Interim DND/CF Policy on CF Computer Network Operations, 21 November 2013]
Cyber Asset	Programmable electronic devices and communication networks including hardware, software, and data. [Source: North American Electric Reliability Corporation, Glossary of Terms Used in Reliability Standards 14 (May 25, 2012)]
Cyber Domain	All areas, entities and activities related to, or affecting, cyberspace. Definition note: The Cyber Domain includes the dependent infrastructure and people/users of cyberspace. [Source: Cyberspace Operations, Joint Doctrine Note v6]
Cyber Entity	Cyber Entity is defined as "any distinct thing or actor that exists within the cyber infrastructure [cyberspace]."
Cyber Environment (or Cyber Terrain)	The interdependent networks of IT structures, including the Internet, telecommunications networks, computer systems and embedded controllers, as well as the software and data that reside within them. [Source: CAF Cyber Operations Primer, February 2014.]
Cyber Kill Chain	Collection of processes related to the use of cyberattacks on systems.
Cyber Operations	The conduct of offensive cyber, defensive cyber and cyber support operations where the primary purpose is to achieve objectives in or through the Cyber Domain. [Source: Cyberspace Operations, Joint Doctrine Note v6]
Cyber Security	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". [Source: TERMIUM Plus®, The Government of Canada's terminology and linguistic data bank, 9 Oct 2014.]

Glossary Term	Glossary Description
Cyber Threat	A Cyber Threat is any potential event or act, deliberate or accidental, that could result in the compromise of a GC ITS. [Source: Government of Canada Cyber Security Event Management Plan (GC CSEMP), 4 August 2015 [R18]]
Cyberspace	The interdependent networks of IT structures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers, as well as the software and data that reside within them. [Source: Cyberspace Operations, Joint Doctrine Note v6]
Defensive Cyber Operation	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. [Source: Cyber Operations, Joint Doctrine Note v6; DTB record 693742]
Destroy	Destroy is a Mission Task Verb and means to damage an object or an enemy force so that it is rendered useless to the enemy until reconstituted. In a cyber context, this can be offensive actions against data/information confidentiality, integrity or availability that are essential to enemy operations and render enemy operations useless until they have been reconstituted. (Examples include deleting all files from a server, flashing basic input-output, system or firmware, or causing physical, damage to industrial control systems, etc.)
Detection	Detection means the discovery by any means of the presence of a person, object or phenomenon of potential military significance. In a cyber context, the focus of detection is on cyber entities and the discovery, capturing, recording, tracking and maintenance of their key attributes
Digital Chain of Custody	Preservation of the integrity of digital evidence as well as a procedure for performing documentation chronologically toward evidence.
Forensic analysis	Forensic analysis is a term for in-depth analysis, investigation whose purpose is to objectively identify and document the culprits, reasons, course and consequences of a security incident or violation of state laws or rules of the organization.
Host Computer	In a computer network, a computer that provides end users with services such as computation and database access and

Glossary Term	Glossary Description
	that may perform network control functions, [Source: Defence Terminology Bank, Record 13461]
Identification	Identification means the process of attaining an accurate characterization of a detected entity by any act or means so that high confidence real-time decision, including weapons SA&A engagement, can be made. In a cyber context, this means completing the analysis of a cyber entity in sufficient detail and with legal chain of evidence support to permit cyber force commanders to make operational decisions and plans to take appropriate action when and where necessary. In some cases, this task may involve detailed forensic analysis of hardware and software artefacts guided by deep understanding of threat intelligence.
Information Management	A discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal or long-term preservation. [Source: Treasury Board of Canada Secretariat, Policy Framework for Information and Technology, 1 July 2007]
Information System	Assembly of equipment, methods and procedures and, if necessary, personnel organized to accomplish information processing functions. Note: An information system may also transfer information in support of the processing function, for example, over a local area network interconnecting a number of computers which are part of the information system. [Source: Defence Terminology Bank, Record 20171]
Information Technology	Includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation, and implementation of information systems and applications to meet business requirements. [Source: Treasury Board of Canada Secretariat, Policy Framework for Information and Technology, 1 July 2007]
Information Technology Infrastructure	The set of computers, communications, systems software, utility programmes, and management tools which support the automation of information management throughout an organization. Infrastructure does not include applications and their associated databases. [Source: Defence Terminology Bank, Record 1837]

Glossary Term	Glossary Description
Information Technology Infrastructure Library	Set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.
Information Technology Service	The discrete points of interaction between information technology and people, both internal and external to an organization. [Source: New Definition for the purposes of the CD-DAR Project]
Information Technology Service Locale	The actual desktop, office, building, or similar geographic area within a Service Delivery Area where people establish their discrete points of interaction with information technology. [Source: New Definition for the purposes of the CD-DAR Project]
Information Technology Systems	An assembly of computer hardware, software or firmware, either stand-alone or interconnected that is used to process or transmit data, or to control mechanical or other devices. [Source: Defence Terminology Bank #48262]
Intelligence	The product resulting from the collection, processing, analysis, integration and interpretation of available information concerning foreign states, hostile or potentially hostile forces or elements, geography and social and cultural factors that contributes to the understanding of an actual or potential operating environment. Note: The term 'intelligence' also applies to the activities that result in the product and to the organizations engaged in such activities. [Source: Defence Terminology Bank, Record 738]
Internal Defensive Measures	Internal Defensive Measures are measures and activities conducted within one's own cyberspace to ensure freedom of action.
Machine Learning	The process by which a functional unit improves its performance by acquiring new knowledge or skills, or by reorganizing existing knowledge or skills. [Source: Defence Terminology Bank, Record #21880.]
Neutralize	Neutralize is a Mission Task Verb and means to render an enemy element temporarily incapable of interfering with a particular operation. The task must make clear exactly what must be neutralized; it is ambiguous to simply state

Glossary Term	Glossary Description
	"neutralize enemy preparation" or "neutralize enemy security forces". In a cyber context, this can be offensive actions against data/information confidentiality, integrity or availability that prevents enemy force units from using its offensive or defensive cyber capabilities (Example: interrupt the sensor feeds from a target domain to the responsible cyber defense unit).
Offensive Cyber Operation	Offensive Cyber Operation. An offensive operation intended to project power in or through cyberspace to achieve effects in support of military objectives. [Source: Cyber Operations, Joint Doctrine Note v6; DTB record 693752]
Operational Authorities	These are the commanders and their staffs (such as the MND, CDS, Comd CJOC, DOS SJS and other Strategic and Operational commanders/staffs) who actively rely upon IT Services for the successful conduct of their missions, operations and tasks, be they domestic, international, expeditionary or corporate services/administrative functions. These are the end consumers of the Situational Awareness Products of CD-DAR. [Source: New Definition]
Operational Authority	The person who has the authority to define requirements and operating principles, set standards and accept risk within their area of responsibility. [Source: Defence Terminology Bank, Record 43435]
Outcome	An outcome is "something that follows as a result or consequence." [Source: Outcome Management Guide and Tools [R37]]
Recognition	Recognition means the determination by any means of the friendly or enemy character or of the individuality of another, or of objects such as aircraft, ships, or tanks or of phenomena such as communications-electronics patterns. In a cyber context this means analyzing the key attributes of cyber entities and their activities (understanding that the data on many attributes may be false, out of date, incomplete, or misleading, etc.) in the holistic context of global and joint operations/information domain, to determine whether the activities being observed are the result of Natural or Deliberate threats and estimate the impacts of these threats.

Glossary Term	Glossary Description
Response Action	In defensive cyber operations, measures and activities conducted in or through cyberspace, outside of one's own cyberspace, against ongoing or imminent threats to preserve freedom of action. [Source: Record of Decisions – Joint Terminology Panel meeting held at the Canadian Forces Warfare Centre from 26-29 April 2016]
Signals Intelligence (SIGINT)	Intelligence derived from electromagnetic communications, communication systems and electromagnetic non-communication transmissions, by those who are not the intended recipients of the information. [Source: Record of Decisions – Joint Terminology Panel meeting held at the Canadian Forces Warfare Centre from 26-29 April 2016]
Situational Awareness	Situational Awareness is the knowledge of the elements in the operational environment necessary to make well-informed decisions. [Source: Defence Terminology Bank, Record 41441]
Support Cyber Operation	A network operation tasked by, or under direct control of, a commander to support offensive and defensive cyber operations. [Source: Record of Decisions – Joint Terminology Panel meeting held at the Canadian Forces Warfare Centre from 26-29 April 2016]
Suppress	Suppress is a Mission Task Verb and means to temporarily degrade an enemy capability to enable a friendly action. The effect is temporary and usually only lasts while the friendly force is firing. In a cyber context, this can be a series of offensive cyber actions that degrade or neutralize the ability of a belligerent force to use cyberspace. (Example: Denial of service attacks).
Statement of Sensitivity	A description of the confidentiality, integrity or availability requirements associated with the data or other assets stored or processed in or transmitted by an information system. Source: Terminum

11. ACRONYMS & ABBREVIATIONS

Acronym / Abbreviation	Description
ADM(IM)	Assistant Deputy Minister (Information Management)
AI	Artificial Intelligence
AOR	Area of Responsibility
APT	Advanced Persistent Threats
BCA	Business Case Analysis
C Cyber	Chief of Cyberspace Staff
C2	Command and Control
C4ISR	Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance
CAF	Canadian Armed Forces
CANSOFCOM	Canadian Special Operations Forces Command
CDADS	Cyber Defence Analysis and implement Decision Support
CD-DAR	Cyber Defence - Decision Analysis and Response
CDR	Cyber Data Repository
CDS	Chief of the Defence Staff
CEED	Cyber Entity and Event Discovery
CFNOC	Canadian Forces Network Operations Centre
CITE	Cyber Integrated Test Environment
CJOC	Canadian Joint Operations Command
COA	Course of Action
COD	Cyber Operational Dashboard
Comd-NET	Command Network
CONOPS	Concept of Operations
CONSUP	Concept of Support

Acronym / Abbreviation	Description
COP	Common Operational Picture
CORA	Centre for Operational Research Analysis
CPE	Common Platform Enumeration
CPU	Central Processing Unit
CSA	Cyber Security Awareness
CSC	Critical Security Controls
CSE	Communication Security Establishment
CSMA	Cyber Security Monitoring and Actions
CVE	Common Vulnerabilities and Exposures
Cyber Op	Cyber Operator
DAR	Decision Analysis Response
DART	Disaster Assistance Response Team
DCB	Defence Capability Board
DCSFA	Director Corporate Submissions and Financial Arrangements
DCO	Defensive Cyber Operations
DCO-DS	Defensive Cyber Operations – Decision Support
DEFSOC	Defence Service Operations Centre
DG Cyber	Director General Cyber
DGGC	Director General level Governance Committee
DGIMO	Director General Information Management Operations
DGIMPD	Director General Information Management Project Delivery
DIL	Disconnected, Intermittent, Limited (Low Bandwidth)
DIM Secur	Director Information Management (Security)
DND/CAF	Department of National Defence and the Canadian Armed Forces

Acronym / Abbreviation	Description
DoD	Department of Defence (US)
DPS	Defence Procurement Strategy
DRDC	Defence Research and Development Canada
DWAN	Defence Wide Area Network
EDR	Endpoint Detection and Response
FOC	Full Operational Capability
FVEY	Five Eyes
FY	Fiscal Year
GC	Government of Canada
GC CSEMP	Government of Canada Cyber Security Event Management Plan
HLMR	High-Level Mandatory Requirements
HST	Harmonized Sales Tax
IDM	Internal Defensive Measures
IDS	Intrusion Detection System
IOC	Initial Operational Capability
IP	Internet Protocol
IPCP-IA	Investment Plan Change Proposal – Impact Assessment
IRMC	Investment and Resource Management Committee
IRPDA	Independent Review Panel for Defence Acquisition
ISS	In-Service Support
IT	Information Technology
ITI	Information Technology Infrastructure
ITIL	Information Technology Infrastructure Library
ITI in Sp of C2	Information Technology Infrastructure in Support of Command and Control

Acronym / Abbreviation	Description
ITS	Information Technology System
ITSM	Information Technology Service Management
JCOT	Joint Cyber Operations Team
JFCCC	Joint Force Cyber Component Commander
KML	Keyhole Markup Language
ML	Machine-Learning
MND	Minister of National Defence
MTBF	Mean Time between Failures
MTTR	Mean Time to Repair
NAG	Network Access Gateway
NATO	North Atlantic Treaty Organization
NAVCOMM	Naval Communicators
NCIOP	Naval Combat Information Operators
NCR	National Capital Region
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defence Command
NP	National Procurement
NSA	National Security Agency
NSE	National Security Exemption
NSMC	National Service Management Centre
NSMO	National Service Management Office
NS-SCC	National Security – Special Contracting Caveat
NVD	National Vulnerability Database
NVG	NATO Vector Graphics

Acronym / Abbreviation	Description
OA	Operational Authority
OGD	Other Government Department
OMCD	Operational Mentor and Capability Development
OSINT	Open Source Intelligence
OTS	Operational Training System
PA(Def)	Project Approval (Definition)
PA(Imp)	Project Approval (Implementation)
PACS	Physical Access Control Systems
PAD	Project Approval Directive
PB(ID)	Project Brief (Identification)
PCAP	Packet Capture
PGM	Program Guidance Memorandum
PIP	Project Implementation Plan
PMB	Programme Management Board
PO	Performance Objective
PO&M	Personnel, Operations and Maintenance
PORA	Project Opportunity and Risk Assessment
PSPC	Public Services and Procurement Canada
Qty	Quantity
RA	Response Actions
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy
RFI	Request for Information
RFP	Request for Proposals

Acronym / Abbreviation	Description
RSD	Regional Service Desk
SA	Situational Awareness
SA&A	Security Authorization and Accreditation
SANS	SysAdmin, Audit, Network and Security
SIEM	Security Information and Event Management
SIGINT	Signals Intelligence
SJS	Strategic Joint Staff
SOP	Standard Operating Procedures
SOR	Statement of Operational Requirement
SRB	Senior Review Board
SSC	Shared Services Canada
SSE	Strong, Secure, Engaged
TA	Technical Authority
TAD	Technical Architecture Document
TBC	To Be Confirmed
TBD	To Be Determined
TBS	Treasury Board of Canada Secretariat
TM	Task Management
UK	United Kingdom
UN	United Nations
US	United States

ANNEX A – CYBER FUNCTIONAL COMPONENTS DESCRIPTION

Id	Component	Description
1	Cyber Operational Dashboard	Visualization and Reporting The COD provides various dashboards, dynamic views and reporting features in order to support all required use cases for relevant users. The dashboard allows key users (such as managers, executives, analysts, etc.) sitting at their desk to visualize the status of cyber entities. The COD 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. User Interface The term "dashboard" refers to a single screen information display that is used to monitor the status of cyber entities and their behaviour. 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 (i.e. workflows, event monitoring, work tickets, analysis, CDR data entry and management, etc.) are conducted and managed. 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. Data Access and Integration The COD is the visual interface for all human users to access the information stored in the CDR, in order to improve Cyber Defence SA and to support incident handling. The COD provides standard data feeds that may be consumed by existing Battlespace Management Capabilities and C2 applications, using standard data formats such as Keyhole Markup Language (KML), and NATO Vector Graphics (NVG), in order to visualize the Cyber Defence situation together with other layers of the military situation such as land, air and maritime units. Analysis The COD presents the graphical analysis tools and view into the underlying CEED, CSMA, CDR, CDADS and TM system components.
2	Task Management	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.

Id	Component	Description
3	Operational Training	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 focused 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; and d. A collective training component for the Decision Analysis and Response capability. It is a replication of the set of operational systems with offline datasets allowing complete range of functionalities and running realistic scenarios for training purposes.
4	Cyber Security Monitoring and Action	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 mandatory CSCs are: CSC-1 Inventory of authorized and unauthorized devices CSC-2 Inventory of authorized and unauthorized software CSC-3 Secure configuration of end-user devices CSC-4 Continuous vulnerability assessment and remediation CSC-5 Controlled use of Administrative privileges.
5	Cyber Defence Analysis and Decisions Support	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:

Id	Component	Description
		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 (COA), and assess their effectiveness, costs and side effects with respect to mission objectives; c. Cyber intelligence and OSINT analysis; d. Hunt and advanced analytics; e. Forensics analysis; f. Incident handling; g. Incident response with COA analysis; h. Network security monitoring and reporting; and i. Operational planning.
6	Cyber Data Repository (CDR)	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	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

Id	Component	Description
		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.

ANNEX B – OPERATIONAL DRIVERS

Serial	Driver	Need	Outcome
1	Awareness The ability to gather, fuse and display quality, timely information across cyber domain.	Cyber domain awareness is paramount in decision making for Cyber security and Defence. Data from multiple sources is necessary to visualize the DND/CAF Cyber domain, in order to facilitate command and control of the Cyber Force. This provides the capability to identify anomalies or patterns that may be overlooked if restrained by a single domain focus.	An unobstructed, persistent and manageable visualization of DND/CAF cyberspace that enables analysis and decision making.
2	Responsiveness The ability to anticipate and take action when and where required.	DND/CAF requires the ability to exercise authoritative control over cyberspace (CAF internal networks included in scope for the CD-DAR Project, Cyber space is defined in the BCA Glossary), across the tactical, operational and strategic levels.	In order to identify and mitigate threats, attacks and vulnerabilities, DND/CAF will have a proactive capability which continuously analyzes cyberspace and supports response actions.
3	Flexibility and Scalability The ability to respond to enemy and support friendly courses of action (COAs) and to maintain the freedom of manoeuvre within the DND/CAF cyberspace.	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.	A capability that is effective, scalable and sustainable across all CAF operational scenarios and functional within the DND/CAF Cyber security and defence environment.
4	Resilience The ability to recover from or adjust to, network change, attack,	A capacity that can readily recover from, or adjust to, the operational situation while maintaining quality	A resilient capability that can continuously support network operations, Cyber security,

Serial	Driver	Need	Outcome
	damage, or destabilizing effects in cyber, operational and natural environments.	Cyber security and defence capability.	and DCO within a highly contested environment.
5	Innovative The ability to modify the capability in keeping with the current pace of changing technology	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. There is a need to implement a solution that can keep pace with that rapid change, including, but not limited to, using relational contracting methodologies that leverage the ability of industry suppliers to provide solutions in a timely fashion, via continual conversation.	Throughout its life-cycle, a best in-class capability that can be easily implemented to address the changing environment, mission and threat.
6	Interoperability All force entities seamlessly connect, or provide information to and from each other.	A joint capacity for multiple data sources to be fused and/or exchanged across DND/CAF domains, with key allies and amongst partners' cyberspace infrastructure. (GC, US, Five Eyes, North Atlantic Treaty Organization (NATO), Public Safety, Shared Services Canada, the Communications Security Establishment (CSE) and the private sector).	A technical and informational capability that enables seamless operations within DND/CAF and with our key allies and partners, and contributes to the broader GC cyber security.

a. Discovery of cyber assets – Discovering and keeping track of all network assets and distinguishing the known from the new (and the unknown) is currently challenging. Software flaws and improper configuration of system components are significant vulnerabilities of information systems that allow for system exploitation. There are minor capabilities deployed

sporadically throughout DND/CAF but nothing that produces or aligns with an enterprise solution for the DND/CAF Cyber Force;

b. Cyber analysis – Distinguishing regular traffic coming from known devices from suspicious traffic or traffic coming from new and unknown devices is currently challenging. Current Defensive Cyber Operations (DCO) capabilities are mostly manual and are insufficient for the complexity of the DND/CAF cyber domain and/or the tactics used by our potential adversaries. Sensors are insufficient, and when they detect indications of possible malicious activities, analysts must manually piece the data together and try to understand the extent of the breach, identify the malicious actor and the targeted item or location, and identify the operational impacts. DND/CAF have some Solutions but none have been specially designed to conduct analysis on the scale and of the type that CD-DAR will be designed to provide;

c. Cyber response – The ability to respond to unknown traffic and to eliminate threats is challenging. Current DND/CAF cyber domain systems cannot provide the data with current operational information and intelligence that supports the Command decision-making processes; this makes current processes cumbersome, insufficiently integrated and lacking responsiveness. CD-DAR will allow the Cyber Commander and the Cyber Force the option of more autonomous solutions so that they have full control over responsive actions when dealing with cyber events;

d. Cyber command and control – The command and control of cyber actions within the DND/CAF cyber domain environment is challenging. Current capabilities do not allow for the command and control of defensive cyber actions across the breadth of our most important networks. DND/CAF cyber domain systems cannot provide the data with operational information and intelligence that helps the command decision processes. CD-DAR will improve our ability to perform command and control of cyber elements within the DND/CAF cyber domain environment, through standardized interfaces and supporting automated workflows;

e. Integration – DND/CAF DCO information is not currently integrated in the enterprise system. The integration of cyber specific information for the Cyber Commander and the Cyber Force is currently possible but CD-DAR capabilities will enable a more seamless process and faster integration;

f. Interoperability – It is challenging to exchange cyber threat vectors and analyze information between internal departments, external domains, or with other countries. Key actions in cyber defence such as cyber threat vector exchange, access to external friendly data sources, and access to analysis information with internal systems[15] need to be done in a seamless fashion.

[15] As well as the systems and assigned network environments of specified Other Government Departments & Agencies (OGD&As), Five Eyes (FVEY) nations, North Atlantic Treaty Organization (NATO) nations, and other external organizations

All force entities must be able to connect and provide the required information sharing between each other. Capabilities, such as Cyber Incident and Information Coordination System or the Malware Information Sharing Platform are not interoperable to the capacity in which CD-DAR will provide to the Cyber Commander and Force;

g. Resilience – It is challenging or not possible to monitor Disconnected, Intermittent, and Limited (DIL) environments. The current model is manual, organization-centric and has limited responsiveness. Our networks do not have any designed Cyber Resilience, such as ability to perform localized monitoring, analysis, and support responsible decision-making within disconnected, intermittent, and geographically limited regional networks even when it is disconnected from a central management point. CD-DAR will be resilient and capable of operating in disconnected, intermittent, and geographically limited environments;

h. Continuous evolution – Any changes in policy, technology, scope, business workflows, collective training, cyber tool development, or threats, greatly impact connected systems, infrastructures and policies, which reduces or disables functionality. Therefore, ensuring ongoing joint Cyber security and defence capabilities provide the ability to exploit joint operating functions. This must take place within the cyber environment, while at the same time ensuring that improvements or additions to these cyber capabilities are implemented without impacting the IT infrastructure baseline; and

Flexibility – There is no effective scalability or sustainable capacity across all CAF operational engagements that is functional within the DND/CAF Cyber security and defence environments.

Annex B: Mandatory Evaluation Criteria

1. Mandatory Technical Criteria

The respondent must meet the mandatory technical evaluation criteria specified in Table 1 of Annex B of the ITQ. All evaluation criteria listed in Table 1 are mandatory and all are subject to the Phased Bid Compliance process. The Respondent must provide the necessary documentation to support compliance with this requirement. Each Mandatory Technical Criterion must be addressed separately.

Projects: Where the respondent must include a description of projects:

(i) a project must have been completed by the Respondent itself and cannot include the experience of any proposed subcontractor or any affiliate of the Respondent

(ii) a project must have been completed by the ITQ closing date

(iii) more than one (1) reference project may be used to meet the evaluation criteria

(iv) a project must be in operations, not in Research and Development (R&D) or test environments

(v) a project must be recent within the last five (5) years

(vi) a project may be done as a joint venture, but the Respondents must identify the components for which they were responsible

(vii) a project may be used for multiple criteria

(viii) the Respondents have to clearly identify their role, responsibilities, and deliverables of their contract in as much detail as possible

(ix) the Respondent should identify what were the outcomes achieved, deliverables accomplished, as part of their contract and whether they were achieved within scope, budget, and schedule.

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

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

a. Project name
b. Short description of project objective
c. Project Value
d. Joint Venture or Single Vendor
e. Contract Value (with the Vendor)
f. Duration of Project (month/year)
g. Duration of Contract (month/year)
h. Project Level of Effort (Person Years (PYs) = Project Management Office (PMO) and Subject Matter Experts (SMEs)
i. Contract Level of Effort (PYs = PMOs and SMEs)

j. Capability capacity (number of users and *Endpoints*)
k. Statement of Requirements of the project and scope
l. Security Classification of the Project
m. References and contact information

2. Form 2 – Project Reference Check Form

Instructions to Suppliers:

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

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

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

Form 2 - Project Reference Check Form

#	Response		
(a)	Mandatory Requirement Number (from Table 1 of Annex B)		
(b)	Supplier Full Legal Name (if the Supplier is a joint venture, the full legal name of the joint venture member for the referenced project)		
(c)	Description of the project and contract (specific to Respondent), values in Canadian dollars, duration (list month and year), security classification of the referenced project.		
(d)	Name of client organization for the referenced project		
(e)	Name of client contact for the referenced project		
(f)	Client organization and client contact affiliation with the Supplier (or joint venture member)		
	Please indicate accordingly:	Are not affiliated	Are affiliated
(g)	Name of organization the client contact is currently working for (if the client contact is no longer working for the client organization identified for the referenced project)		
(h)	Title of client contact (while working on the referenced project)		
(i)	Current telephone number of client contact		
(j)	Current e-mail address of the client contact		
(k)	Role of the client contact in the referenced project		
(l)	Provide the maximum number of users and Endpoints of the reference project for which only the Respondent has worked on.		
	Number of Users:	Number of Endpoints:	
(m)	Identify the components for which you were responsible: (If the reference project was a joint venture, please identify only the components the Respondent was responsible for)		
(n)	Identify the level of effort (PYs – PMO and SMEs) on the reference project components for which you were responsible for		
(o)	Confirm reference project is in the Operations environment (Yes/No)		
(p)	If the reference project is used for multiple criteria, please provide breakdown of percentage for given criteria allocated within project timeline		
(q)	For the Contract that the referenced project falls under, identify clearly the Respondent's role, responsibilities, and deliverables in as much detail as possible		

3. Table 1 - Mandatory Technical Evaluation Criteria

Terms or words in Italics are defined in Table 2 - Definitions

Serial	Criteria	Evaluation	**Proof Required** (in the last 5 years before date of ITQ closing)
1	The Respondent must have *Successfully Implemented* at least one (1) *Complex Information Management/Information Technology (IM/IT) Project* in the last five (5) years, which included the design, development, integration, implementation, and delivery of Commercial off the Shelf (COTS)/Government off the Shelf (GOTS) *Cyber Security* and *Cyber Decision Analysis and Response* solutions, complete with the provision of at least 12 months of *Stabilization Support*, deployed on: **a. *Complex IM/IT Networks* of 10,000 or more *Endpoints; and*** **b. For one or more of the Five Eyes (FVEYs) nations (AUS/CAN/NZ/UK/US) or NATO member countries.**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented* COTS/GOTS–based *Cyber Security* and *Cyber Decision Analysis and Response* solutions for criterion 1.
2	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* in the last five (5) years, which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Cyber Decision Analysis and Response* of COTS/GOTS solutions that provide capabilities to: **a. Identify and track all (authorized and non-authorized) IM/IT assets within a designated *Complex IM/IT Network* environment of 10,000 or more *Endpoints*;** **b. Assess asset vulnerabilities, configuration, risk and patch compliance;** **c. Collect, retain and analyze cyber threat information;** **d. Detect and assess suspicious activity and provide context for risk and vulnerability assessments;** **e. Execute responses to threat and remediation actions in *near real-time*;** f. **Provide *Cyber Decision Analysis and Response* of *Command and***	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS solutions for criterion 2.

Serial	Criteria	Evaluation	**Proof Required** (in the last 5 years before date of ITQ closing)
	Control (C2) Networks **systems through an integrated** ***Common Operating Picture (COP)*****; and** g. **Provide at least 12 months of** ***Stabilization Support*****.**		
3	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions **that demonstrate ALL of the following within a** ***Complex IM/IT Network*** **environment of 10,000 or more** ***Endpoints,*** **complete with the provision of at least 12 months of** ***Stabilization Support*****, in the last five (5) years:** **a. Continuous data collection, retention, detection, analysis and provide context for risk and vulnerability assessments in** ***near real-time*****;** **b. Data feeds of cyber threat and analysis information from multiple sources of varied data formats must be normalized and be integrated into a common format for analysis and to provide a** ***Common Operating Picture (COP);*** **and** **c.** ***Advanced Data Analytics*** **utilizing:** **i. Integrated** ***Cyber Security*** **alerts from:** **1) Threat intelligence,** **2) External entity information,** **3) Internal asset information,** **4) Information from Event Detection and Response (EDR),**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS solutions for criteria 3.

Serial	Criteria	Evaluation	**Proof Required** (in the last 5 years before date of ITQ closing)
	5) Information from network traffic analysis, **6) Activity history, and** **7) User and Entity behavior analytics (UEBA), and** **ii. Integrated *Cyber Security* incident analysis from:** **1) Threat intelligence,** **2) Past incidents,** 3) **Similar incidents, and** 4) **Signature and heuristic-based detection.**		
4	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions and provision of at least 12 months of *Stabilization Support* – **utilizing *Adaptive* and *Dynamic* identification, containment and eradication of threats using advanced Cyber Defence capabilities in *near real-time* within a *Complex IM/IT Network* of 10,000 or more *Endpoints* in the last five (5) years.**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS solutions for criteria 4.
5	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* in the last five (5) years, which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions and provision of at least 12 months of *Stabilization Support* – **establishing a data repository that supports the storage, retrieval and processing of structured and unstructured data for a *Complex IM/IT Network* of 10,000 or more *Endpoints* and the performance of *Tier 2 Analysis* in order to enable decision support through automated and assisted execution of**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS solutions for criteria 5.

Serial	Criteria	Evaluation	**Proof Required** (in the last 5 years before date of ITQ closing)
	responses.		
6	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* in the last five (5) years, which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions and provision of at least 12 months of *Stabilization Support* – **For *Complex IM/IT Networks* of 10,000 or more *Endpoints* within globally distributed network components on two (2) or more continents where:** a. **Connectivity is unavailable, unreliable or has low capacity (bandwidth) (e.g. Satellite Communications (Mbps), Ships (Kbps)); and** b. **Re-synchronization of data with enduring environment is automatic once connectivity is re-established.**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS solutions for criteria 6.
7	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions and provision of at least 12 months of *Stabilization Support* – **For *Complex IM/IT Networks* of 10,000 or more *Endpoints* that provide the following interoperability functionalities within OGDSs of Government of Canada and Five Eyes (allies) in the last five (5) years, but not limited to:** **a. The ability to share information seamlessly, such as threat vectors, analyses information, etc., with key partners such as OGDs and Allies;** **b. Central collection of Threat Intelligence;** **c. Fusion and deduplication of Threat Intelligence;**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS solutions for criteria 7.

Serial	Criteria	Evaluation	**Proof Required** (in the last 5 years before date of ITQ closing)
	d. Search and graph analysis of indicators; **e. Storage of machine-readable and non-structured Threat Intelligence;** f. **Distribution of Threat Intelligence to external tools; and** g. **Interfaces and mechanisms for sharing Threat Intelligence with other organizations (in formats including SCAP, STIX, and JSON).**		
8	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* for which the *Respondent* has implemented the following emerging technologies as part of the core *Cyber Security* and *Decision Analysis and Response* solutions **for 10,000 or more *Endpoints* within the last five (5) years:** **a. *Artificial Intelligence (AI)*;** **b. *Machine-Learning*;** **c. *Cloud Computing*;** **d. *Behavioural Pattern Analysis*; and** **e. *Big Data*.** **The *Respondent* may identify additional emerging technologies Government of Canada should consider in its implementation.**	Pass/Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has integrated with *Cyber Security* and *Decision Analysis and Response* solutions for criteria 8.
9	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* which included **the design, development and delivery of integrated exercise and training solutions for operators and maintainers of *Cyber Security* and *Decision Analysis and Response* of *Complex IM/IT Network* systems (hardware & software) of 10,000 or more *Endpoints* in**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has developed and delivered exercise and training solutions for criteria 9.

Serial	Criteria	Evaluation	**Proof Required** (in the last 5 years before date of ITQ closing)
	the last five (5) years.		
10	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions and provision of at least 12 months of *Stabilization Support* – **For *Complex IM/IT Networks* of 10,000 or more *Endpoints* in the last five (5) years across:** **a. Multi-level security (Designated, Secret and Top Secret) environments; and** **b. Multi-caveat (within the same security level) security environments.**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS solutions for criteria 10.
11	The *Respondent* must have *Successfully Implemented* at least one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions and provision of at least 12 months of *Stabilization Support* – **For the administration and management of data collection from *heterogeneous* sources and Configuration Management for large collections of data in *Complex IM/IT Networks* of 10,000 or more *Endpoints* in the last five (5) years.**	Pass / Fail	The *Respondent* must provide a minimum of one (1) reference project in the last five (5) years for which the *Respondent* has *Successfully Implemented Cyber Security* and *Decision Analysis and Response* COTS/GOTS solutions for criteria 11.

Table 2 Definitions

Term	Definition
Adaptive	Ability to evolve, adjust or modify accordingly.
Advanced Data Analytics	The autonomous or semi-autonomous examination of data or content using sophisticated techniques and tools, typically beyond those of traditional business intelligence (BI), to discover deeper insights, make predictions, or generate recommendations.
Artificial Intelligence	The capability of a computer to perform such functions that are associated with human logic such as reasoning, learning, and self-improvement.
Behavioural Pattern Analysis	Behavioural analysis uses machine learning, artificial intelligence, big data, and analytics to identify malicious, stealth behavior by analyzing subtle differences in normal, everyday activities in order to proactively stop cyberattacks before the attackers have the ability to fully execute their destructive plans. Behavioral pattern analysis starts with behaviour monitoring, which in a cybersecurity context consists of: Recording the events and activities of a system and its users. The recorded events are compared against security policy and behavioral baselines to evaluate compliance and/or discover violations. Behavioral monitoring can include the tracking of trends, setting of thresholds and defining responses. Trend tracking can reveal when errors are increasing requiring technical support services, when abnormal load levels occur indicating the presence of malicious code, or when production work levels increase indicating a need to expand capacity. Thresholds are used to define the levels of activity or events above which are of concern and require a response. The levels below the threshold are recorded but do not trigger a response. Responses can be to resolve conflicts, handle violations, prevent downtime or improve capabilities.
Big Data	Large amount of data sets whose size is growing at a vast speed making it difficult to handle such large amount of data using traditional software tools available.
Cloud Computing	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Command and Control (C2) Networks	The network upon which a commander exercises authority and direction over assigned, allocated and attached forces in the accomplishment of a mission.

Term	Definition
Common Operating Picture (COP)	A shared and *Dynamic* representation of information that can be tailored to facilitate situational awareness, collaborative planning, decision-making, and response. Additionally, the operational picture must be tailored to the user's requirements, based on common data and information shared by more than one command.
Complex IM/IT Network	IM/IT Networks that are “complex” have distinct properties that arise from the interaction of the *complex systems* they comprise, such as sizeable, globally distributed, *Dynamic*, *adaptable*, *heterogeneous* (legacy / modern, various suppliers) network equipment, *heterogeneous* applications (software version, licensing, vendors), *heterogeneous* data (structured / unstructured) sources, *self-healing* (a system, which is always expected to be up and running as designed), intermittent connectivity, low bandwidth (e.g. Satellite Communications (Mbps), Ships (Kbps), etc.) and latency.
Complex Project	Complex projects are projects that are characterized as having many different social and technical elements on many different levels that are interconnected and interdependent. In contrast to simpler projects that are standardized, well-defined endeavors within predictable and stable environments, complex projects typically involve a high degree of uncertainty in defining end objectives, they often take place within a changing environment and may involve the input of many diverse stakeholders.
Complex System	Complex systems are systems whose behavior is intrinsically difficult to model due to the dependencies, competitions, relationships, or other types of interactions between their parts or between a given system and its environment. Systems that are "complex" have distinct properties that arise from these relationships, such as nonlinearity, emergence, spontaneous order, adaptation, and feedback loops, among others.
Contractual Relationship	A letter of support from a Joint Venture member would be acceptable evidence of a 'Contractual Relationship'.
Cyber-asset	All assets – software, hardware and users (authorized and non-authorized) connected to the Command Network (not including identity, credential, and access management for users).
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.
Decision Analysis and Response	Attaining an accurate characterization of a cyber-asset or usage weakness or threat and implementing approved security and defensive cyber actions to maintain freedom of action.
Deployed	A capability supporting an expeditionary (geographically dispersed, most often operated in a threat environment) base that employs and sustains task

Term	Definition
	forces for missions.
Dynamic	Pertaining to a data attribute, whose values can only be established during the execution of all or part of a programme.
Endpoint	An endpoint is a remote computing device that communicates back and forth with a network to which it is connected. Laptops, desktops, mobile phones, tablets, servers, and virtual environments can all be considered endpoints.
Freedom of Action	Once a task or mission has been established and the necessary orders have been given, subordinate commanders must be permitted maximum freedom of action to take initiative and exercise their skills and knowledge of the local situation in the planning and conduct of the operation with little or no constraints.
Heterogeneous	• Network equipment from various vendors, or different technological generations (legacy / modern) • Software applications: from varied vendors, of diverse versions or patch levels • Miscellaneous structured / unstructured data sources
Lines of Communication	All the land, water, and air routes that connect an operating military force with one or more bases of operations, and along which supplies and reinforcements move.
Machine Learning	The process by which a functional unit improves its performance by acquiring new knowledge or skills, or by reorganizing existing knowledge or skills.
Near Real-Time	Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that delays are limited to the data transport medium’s capabilities.
Respondent	Invocations of the term 'Respondent(s)' refer to the Prime System Integrator, Joint Venture, or Joint Venture member proposed for the Cyber Defence – Decision Analysis and Response (CD-DAR) procurement.
Self-healing	In the IT world, self-healing systems are described as “any device or system that has the ability to perceive that it is not operating correctly and, without external assistance, make the necessary adjustments to restore itself to normal operation”. A system, which is always expected to be up and running as designed.
Situational Awareness	The knowledge of the elements of the operational environment necessary to make well-informed decisions.

Term	Definition
Stabilization Support	Continuous support for at least 12 months duration from when the client group(s) began using the cyber capability to, at a minimum, when the cyber capability was fully implemented.
Status of Assets	Through the assessment of the asset's attributes for vulnerability, configuration, risk and patch compliance.
Successfully Implemented	Achieved when the *Respondent* has designed, developed, integrated, implemented, delivered and provided *Stabilization Support* for a project that has achieved successful completion where the requirements have been met and proof of acceptance from the clients provided; alternatively a Letter of Support from the (Federal) client would be acceptable.
Third (3rd) Line Support	Support capabilities provided to a military force within a theatre of operations or at installations established along the strategic lines of communication.
Tier 2 Analysis	**Tier 2 Analysis provides a further in-depth analysis** and focus on incident support and alert handling from Tier 1. Tier 2 Analysts coordinate security monitoring findings with the Threat Intelligence team, vendor partners, and with specific points of contact to obtain a wider analysis of event data and its impact on designated environments.

Annex C: Security Requirements

The following three sections detail the Security Requirements for each phase of the procurement process including the contract. These are the anticipated Security Requirements based on the Security Requirements Check Lists (SRCLs) included in this Annex. Canada reserves the right to modify the Security Requirements as required.

1.1 Security Requirements for the ITQ

a) There are no security requirements for the ITQ.

b) A Supplier is not required to have security clearance in order to become a Qualified Supplier.

c) There are security requirements for the Due Diligence Phase, the RFP and the Contract.

d) For information purposes, Suppliers are hereby informed that the amount of time to obtain required security clearance levels may be lengthy and is contingent upon the specific clearance levels required. Suppliers are solely responsible for obtaining such clearances. Suppliers that do not currently have personnel and organization security clearances through the Canadian federal government or their respective domestic Industrial Security Program, or Suppliers that do not meet the anticipated security requirements outlined in Sections 1.2 and 1.3 of this Annex, should begin the clearance process early by contacting the Industrial Security Program (ISP) of PWGSC (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

1.2 Security Requirements for Phase 3 – Due Diligence and Phase 4 – RFP

a) The following security requirements (Security Requirements Check List (SRCL) and related clauses provided by the Contract Security Program) apply to and are required for full participation in the Due Diligence Phase and RFP Phase. Pre-qualified Suppliers that do not meet these security requirements on the date the final RFP is released will be removed from the list of qualified suppliers.

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:

PWGSC FILE No. W6369-20-CY06 / RFP CLAUSES

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Facility Security Clearance at the level of NATO SECRET, with approved Document Safeguarding at the level of SECRET and NATO SECRET, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

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

3. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or sensitive site(s) must EACH hold a valid personnel security screening at the level of RELIABILITY STATUS, granted or approved by the CSP, PWGSC.

4. The Contractor personnel requiring access to CLASSIFIED or PROTECTED information and/or assets bearing the caveat “CANADIAN EYES ONLY” must be citizens of Canada and EACH hold a valid personnel security screening at the level of SECRET or RELIABILITY STATUS, as required, granted or approved by the CSP, PWGSC.

5. The Contractor/Offeror personnel requiring access to RESTRICTED CANADIAN CLASSIFIED or PROTECTED information, assets or sensitive site(s) must be citizens of Canada, United States, United Kingdom, Australia, or New Zealand and must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required, granted or approved by the CSP, PWGSC.

6. The Contractor/Offeror personnel requiring access to NATO UNCLASSIFIED information or assets must be citizens of Canada, United States, United Kingdom, Australia, or New Zealand, but do not require to hold a personnel security clearance; however, the Contractor must ensure that the NATO Unclassified information is not releasable to third parties and that the "need to know" principle is applied to personnel accessing this information.

7. The Contractor personnel requiring access to NATO RESTRICTED information or assets must be citizens of Canada, United States, United Kingdom, Australia, or New Zealand and EACH hold a valid RELIABILITY STATUS or its equivalent, granted or approved by the appropriate delegated NATO Security Authority.

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

9. The Contractor/Offeror personnel requiring access to FOREIGN CLASSIFIED or PROTECTED information, assets or sensitive site(s) must be a citizen of Canada, United States, United Kingdom, Australia, or New Zealand and must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required, granted or approved by the CSP, PWGSC.

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

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

12. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the CSP, PWGSC.

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

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

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

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

    (a) Security Requirements Check List and security guide (if applicable), attached at Annex _____;

    (b) Industrial Security Manual (Latest Edition).

1.3 Security Requirements for Phase 5 – Contract

a) The following security requirements (Security Requirements Check List (SRCL) and related clauses provided by the Contract Security Program) apply to the Contract.

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:

PWGSC FILE No. W6369-20-CY06 / CONTRACT CLAUSES

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Facility Security Clearance at the level of TOP SECRET and NATO SECRET, with approved: Document Safeguarding at the level of TOP SECRET and NATO SECRET issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC) as well as Communications-Electronic Security (COMSEC) account at the level of TOP SECRET, issued by the Communications Security Establishment Canada (CSEC).
2. This contract includes access to Controlled Goods. Prior to access, the contractor must be registered in the Controlled Goods Program of Public Works and Government Services Canada (PWGSC).
3. The Contractor/Offeror personnel requiring access to NON RESTRICTED CANADIAN PROTECTED information, assets or sensitive site(s) must EACH hold a valid personnel security screening at the level of RELIABILITY, granted or approved by the CSP, PWGSC.
4. The Contractor personnel requiring access to PROTECTED information and/or assets bearing the caveat “CANADIAN EYES ONLY” **must be citizens of Canada** and EACH hold a valid personnel security screening at the level of RELIABILITY, granted or approved by the CSP, PWGSC.
5. The Contractor/Offeror personnel requiring access to RESTRICTED CANADIAN CLASSIFIED or PROTECTED information, assets or sensitive site(s) **must be citizens of Canada, United States, United Kingdom, Australia, or New Zealand and** must EACH hold a valid personnel security screening at the level of TOP SECRET, SECRET, or RELIABILITY STATUS, as required, granted or approved by the CSP, PWGSC.
6. The Contractor personnel requiring access to TOP SECRET SIGINT information, assets or sensitive site(s) **must be citizens of Canada** *and* must EACH hold a valid personnel security screening at the level of TOP SECRET SIGINT issued by the Contract Security Program (CSP) of Public Works and Government Services (PWGSC).
7. The Contractor/Offeror personnel requiring access to NATO UNCLASSIFIED information or assets **must be citizens of Canada, United States, or United Kingdom**, but do not require to hold a personnel security clearance; however, the Contractor must ensure that the NATO Unclassified information is not releasable to third parties and that the "need to know" principle is applied to personnel accessing this information.
8. The Contractor personnel requiring access to NATO RESTRICTED information or assets **must be citizens of Canada, United States, or United Kingdom** and EACH hold a valid RELIABILITY STATUS or its equivalent, granted or approved by the appropriate delegated NATO Security Authority.
9. The Contractor/Offeror personnel requiring access to **NATO CLASSIFIED** information, assets or sensitive site(s) **must be citizens of Canada, United States, or United Kingdom** and EACH hold a valid personnel security screening at the level of NATO SECRET, granted or approved by the appropriate delegated NATO Security Authority.
10. The Contractor/Offeror personnel requiring access to FOREIGN CLASSIFIED or PROTECTED information, assets or sensitive site(s) **must be a citizen of Canada, United States, United Kingdom, Australia, or New Zealand** and must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required, granted or approved by the CSP, PWGSC.

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

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

13. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the CSP, PWGSC.

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

15. The contractor must at all times during the performance of the contract possess a letter from PWGSC identifying the results of the FOCI assessment with a FOCI designation of *Not Under FOCI* or *Not Under FOCI through Mitigation*.

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

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

(a) Security Requirements Check List and security guide (if applicable), attached at Annex C;

(b) *Industrial Security Manual* (latest edition) and the *IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector* (ITSD-06A).

1.4 Security Requirements Check Lists (SRCLs)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-RFP
Security Classification / Classification de sécurité
UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organizati Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD/DPDCC
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

In this RFP phase, qualified suppliers will be required to access and store one or more classified Annexes that will be provided; information is classified up to SECRET and releasable only to Canadian citizens.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non	Yes / Oui ✓
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	No / Non ✓	Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non	Yes / Oui ✓
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	No / Non ✓	Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	No / Non ✓	Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

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

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

PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ✓	PROTECTED A / PROTÉGÉ A ✓
PROTECTED B / PROTÉGÉ B ✓	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ✓	PROTECTED B / PROTÉGÉ B ✓
PROTECTED C / PROTÉGÉ C	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET ✓	CONFIDENTIAL / CONFIDENTIEL
SECRET / SECRET ✓	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET ✓
TOP SECRET / TRÈS SECRET		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-RFP

Security Classification / Classification de sécurité
UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No / Non ☐ Yes / Oui ☑
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité : SECRET

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No / Non ☑ Yes / Oui ☐
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☑ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux :

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No / Non ☑ Yes / Oui ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non ☐ Yes / Oui ☐
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No / Non ☐ Yes / Oui ☑
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No / Non ☑ Yes / Oui ☐
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No / Non ☑ Yes / Oui ☐
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No / Non ☐ Yes / Oui ☑
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No / Non ☑ Yes / Oui ☐
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-RFP

Security Classification / Classification de sécurité
UNCLASSIFIED

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-CONTRACT
Security Classification / Classification de sécurité
UNCLASSIFIED

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organizati... Ministère ou organisme gouvernemental d'origine: Department of National Defence	2. Branch or Directorate / Direction générale ou Direction: ADM(IM)/DGIMPD/DPDCC
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

In this Contract Award phase, the winning Bidder may require access to information that is collectively classified up to TOP SECRET - SIGINT as well as access to COMSEC assets, releasable to Canadian citizens only. The winning Bidder will also be required to store, process and exchange information with DND/CAF up to SECRET. Selected supplier personnel may also require access to designated restricted/classified areas and equipment to perform work as part of the contract fulfillment.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	No / Non	✓ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	✓ No / Non	Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No / Non	✓ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	✓ No / Non	Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	✓ No / Non	Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

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

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

PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ✓	PROTECTED A / PROTÉGÉ A ✓
PROTECTED B / PROTÉGÉ B ✓	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ✓	PROTECTED B / PROTÉGÉ B ✓
PROTECTED C / PROTÉGÉ C	NATO CONFIDENTIAL / NATO CONFIDENTIEL	PROTECTED C / PROTÉGÉ C
CONFIDENTIAL / CONFIDENTIEL	NATO SECRET / NATO SECRET ✓	CONFIDENTIAL / CONFIDENTIEL
SECRET / SECRET ✓	COSMIC TOP SECRET / COSMIC TRÈS SECRET	SECRET / SECRET ✓
TOP SECRET / TRÈS SECRET ✓		TOP SECRET / TRÈS SECRET
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ✓		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
W6369-20-CY06-CONTRACT
Security Classification / Classification de sécurité
UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No / Non: ☐ Yes / Oui: ✓
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité : TOP SECRET - SIGINT, SECRET

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No / Non: ✓ Yes / Oui: ☐
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

✓ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	✓ SECRET / SECRET	✓ TOP SECRET / TRÈS SECRET
✓ TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	✓ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux :

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No / Non: ✓ Yes / Oui: ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — No / Non: ☐ Yes / Oui: ☐
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No / Non: ☐ Yes / Oui: ✓
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No / Non: ☐ Yes / Oui: ✓
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No / Non: ✓ Yes / Oui: ☐
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No / Non: ☐ Yes / Oui: ✓
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No / Non: ☐ Yes / Oui: ✓
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

✓ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

✓ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Annex D: Response Submission Form

Invitation to Qualify No. W6369-20CY06/A Response Submission Form				
Respondent's full legal name *In the case of a joint venture, please identify all members.*				
Authorized Representative of Respondent for evaluation purposes (e.g., clarifications)	Name			
	Title			
	Address			
	Telephone #			
	Email			
Respondent's Procurement Business Number (PBN): _____ *Please see PWGSC Standard Instructions. Please make sure that your PBN matches the legal name under which you have submitted your response. If it does not, the Respondent will be determined based on the legal name provided, not based on the PBN, and the Respondent will be required to submit the PBN that matches the legal name of the Respondent.*				
If submitting a response to the ITQ as a joint venture, the Respondent must provide the joint venture member's full legal name and address [Respondent to add more rows if more than two (2) joint venture members]	Joint venture member full legal name:			
	Joint venture member address:			
	Joint venture member full legal name:			
	Joint venture member address:			
Former Public Servants *Please see the Section of PWGSC Standard Instructions entitled "Former Public Servants" for more information.* *If you are submitting a response as a joint venture, please provide this information for each member of the joint venture.*	Is the Respondent a Former Public Servant in receipt of a pension as defined in PWGSC Standard Instructions? **If yes, provide the information required by the Section in PWGSC Standard Instructions entitled "Former Public Servant"**	Yes		
		No		
	Is the Respondent a Former Public Servant who received a lump sum payment under the terms of the work force adjustment directive? **If yes, provide the information required by the Section in PWGSC Standard Instructions entitled "Former Public Servant"**	Yes		
		No		
Federal Contractors Program for Employment Equity Certification *Please see the section of PWGSC Standard Instructions entitled "Federal Contractors Program for Employment Equity" for more information.* *Please check one of the boxes or provide the required information. If you are submitting a response as a joint venture, please provide this information for each member of the joint venture.*	The Respondent certifies having no work force in Canada.			
	The Respondent certifies being a public sector employer.			
	The Respondent certifies being a federally regulated employer subject to the *Employment Equity Act.*			
	The Respondent certifies having a combined work force in Canada of fewer than 100 permanent full-time, part-time and temporary employees.			
	The Respondent has a combined workforce in Canada of 100 or more permanent full-time, part-time and temporary employees.			
	Valid and current Certificate number.			
	The Respondent certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour.			
Requested language for future communications regarding this procurement process – *please indicate either French or English*				
Requested Canadian province or territory for applicable laws				
Security Clearance Level of Respondent	Clearance Level			
	Date Granted			

Please ensure that the security clearance matches the legal name of the Respondent. If it does not, the security clearance is not valid for the Respondent.	Issuing Entity (PWGSC, RCMP, etc.)	
	Legal name of entity to which clearance issued	

On behalf of the Respondent, by signing below, I confirm that I have read the entire ITQ, including the documents incorporated by reference into the ITQ, and I certify and agree that:

1. The Respondent considers itself and its products able to meet all the mandatory requirements described in the ITQ;
2. All the information provided in the response is complete, true and accurate; and
3. The Respondent agrees to be bound by all the terms and conditions of this ITQ, including the documents incorporated by reference into it.

Respondent Authorization: Authorized Representative of Respondent

Name:
Address:
Email:
Signature of authorized representative of Respondent:
Telephone:
Date:

If submitting a response to the ITQ as a joint venture, the Respondent must complete section (h) below. [Respondent to add more rows if more than two (2) joint venture members]

Name:
Address:
Email:
Signature of authorized representative of Respondent:
Telephone:
Date:

Annex E: Agile and Collaborative Procurement Process

1.1 Introduction

a) Canada is taking an agile and collaborative approach to the procurement process for CD-DAR by bringing together government and industry to design and refine the procurement in an iterative manner in order to achieve results.

b) The ITQ Phase of the CD-DAR project as well as the Due Diligence Phase will continue to follow an agile and collaborative procurement process that will facilitate robust dialogue and two-way communication, quality feedback, and disclosure of information right up until the RFP is issued.

c) Canada recognizes that engagement and collaboration throughout a procurement process can help reduce the overall rework burden on potential bidders, help ensure vendors make a reasonable return on their investments and that the overall process delivers solid benefits to Canadians.

1.2 Prior to this ITQ

a) Prior to the ITQ, the Industry Collaboration Process started with the publication on Buy and Sell in December 2016 Letters of Interest (LOI) for both the Cyber Security Awareness (CSA) and Defensive Cyber Operations – Decision Support (DCO-DS) projects to determine if an existing solution was available in the market place. The results of the LOIs indicated that an off-the-shelf solution did not exist, but it demonstrated industry's strong interest in working with the DND/CAF to address its requirement. As the results of the LOI did not provide sufficient information to DND to move the project forward it was determined a more detailed Request for Information was required. The DCO- DS and CSA file number are as listed below. Although now inactive, both may be accessed on Buy and Sell.

DCO-DS LOI

Buy and Sell Reference number: PW-$$QE-049-26100

Solicitation number: W6369-17DE25/A

CSA LOI

Buy and Sell Reference number: PW-$$QE-049-26099

Solicitation number: W6369-17DE26/A

b) A RFI was posted in December 2017 on buyandsell.gc.ca under the DCO-DS project and provided more project information to industry and solicited detailed industry feedback on the operational and technical requirements, cost and schedule.

DCO-DS RFI

Buy and Sell Reference number: PW-$$QE-049-26594

Solicitation number: W6369-17DE25/B

c) An Unclassified Industry Day was held in February of 2018 to present Industry with an overview of the requirements and the intended engagement process and solicit Industry feedback. Questions and Answers and feedback resulting from that dialogue with attendees were posted on Buy and Sell.

d) Following the Industry Day classified one-on-one meetings were held in March of 2018 to present and discuss the classified Annex of the DCO-DS RFI. All suppliers were invited to request a one-on-one meeting with the only criteria being that they met the meeting Security Requirements detailed in the RFI. Classified question and answers were distributed upon request to the suppliers that attended the meetings or who met the Security Requirements and requested a copy by the deadline specified in the RFI. All unclassified questions and answers coming from the one-on-one meetings were posted on Buy and Sell.

1.3 During the ITQ Phase

a) Draft ITQ: A draft ITQ will be posted on Buy and Sell allowing for Industry to provide feedback prior to issuing the final ITQ. Suppliers will be invited to provide written comments and questions on the draft ITQ. Responses will be posted on Buy and Sell.

b) Formal ITQ: The formal ITQ will be posted on Buy and Sell. This is the first phase of the qualification process in order to be eligible to bid on the RFP for the CD-DAR Project.

c) Respondents will be required to submit responses by the time and date indicated in the ITQ.

d) The Government of Canada (GoC) will notify the vendors of the results of the evaluation.

1.4 During the Due Diligence Phase

a) The GoC intends to release a complete Draft RFP, which will include a classified component, to Pre-qualified Suppliers.

b) To keep all of industry informed of the requirements the GoC will post the unclassified components of the Draft RFP on Buy and Sell through a Request for Information (RFI).

c) In order to seek feedback on the complete draft RFP the GoC may hold a classified Bidders Conference and classified one-on-one meetings with Pre-qualified Suppliers,

d) When and where appropriate the GoC will provide feedback as to how it is using, or not using, the feedback received.

e) The GoC may make modifications to the requirements and terms of the RFP as per feedback from industry.

f) When possible, throughout the process, the GoC plans on addressing and publishing questions and answers submitted by other suppliers (not Pre-qualified Suppliers) on Buy and Sell.

g) When possible, throughout the process, unclassified questions asked by Pre-qualified Suppliers will be answered and posted on Buy and Sell.

h) Classified questions and answers will only be provided to Pre-qualified Suppliers who meet the required security requirements

j) The GoC plans on publishing questions and answers, when possible, throughout the process.

1.5 RFP

a) The GoC will provide the complete RFP, which will include classified components, to the Pre-qualified Suppliers and invite the Pre-qualified Suppliers to bid on the solicitation.

b) To keep all of industry informed, the GoC will post the unclassified components of the RFP on Buy and Sell, however only Pre-qualified Suppliers will be invited to bid on the solicitation.