RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

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

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

Title - Sujet CD-DAR - ITQ Invitation to Qualify: Cyber Defence – Decision Analysis and Response	
Solicitation No. - N° de l'invitation W6369-20CY06/C	**Amendment No. - N° modif.** 001
Client Reference No. - N° de référence du client W6369-20CY06	**Date** 2021-04-28
GETS Reference No. - N° de référence de SEAG PW-$$QE-049-28197	
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 Eastern Daylight Saving Time EDT
on - le 2021-06-17 Heure Avancée de l'Est HAE

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

Address Enquiries to: - Adresser toutes questions à: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (873) 355-3543 ( )	**FAX No. - N° de FAX** ( ) -

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

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**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**

THIS SOLICITATION AMENDMENT 001 IS ISSUED TO:

1. Correct reference link errors in Annex A, the SOR and the CONOPS. The corrected documents are attached.

ALL OTHER TERMS AND CONDITIONS OF THE SOLICITATION REMAIN UNCHANGED.

Invitation to Qualify (ITQ)

FOR THE
CYBER DEFENCE – DECISION ANALYSIS AND RESPONSE

ITQ NO, W6369-20-CY06/C

Table of Contents

1. General Information 2
1.1 Introduction 2
1.2 Overview of the Project 2
1.3 Overview of the Planned Procurement Process 4
1.4 Debriefings 6
1.5 National Security Exception 6
1.6 Industrial and Technological Benefits 6
1.7 Consultants 7
1.8 Conflict of Interest or Unfair Advantage 7
1.9 Fairness Monitor 7
2. Instructions for Respondents 8
2.1 Standard Instructions, Clauses and Conditions 8
2.2 Teaming Terminology 8
2.3 Submission of Only One Response 9
2.4 Applicable Laws 11
2.5 Questions, Comments and Communications 11
2.6 Rights of Canada 12
2.7 Security Requirements 12
3. Preparing and Submitting a Response 14
3.1 Language for Future Communications 14
3.2 Content of Response 14
3.3 Respondent Core Team 15
3.4 Evaluation and Respondent Core Team 15
3.5 Composition of Core Team 16
3.6 Changes to the Respondent Core Team 16
3.7 Electronic-Submission of Response 16
4. Process for Evaluating Responses 18
4.1 Evaluation of Respondent Qualifications 18
4.2 Conduct of the Evaluation 18
4.3 Phased Bid Compliance Process (PBCP) 18
4.4 Technical Evaluation 21
4.5 Basis of Qualification 21
4.6 ITQ Second Qualification Round 22
Annex A: Mandatory Evaluation Criteria 23
Annex B: Security Requirements 40
Annex C: Response Submission Form 57
Annex D: Agile and Collaborative Procurement Process 59
Annex E: Query on In-Service Support 62
Attachment 1: Draft Statement of Requirements (DSOR) 63
Attachment 2: Draft Concept of Operations (CONOPS) 64

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 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 D.

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

1.2.1 **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

[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.

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.

1.2.2 **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 at the end of this documents in Attachment 1: Draft Statement of Operational Requirements (SOR) and Attachment 2: Draft Concept of Operations (CONOPS)

1.2.3 **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. The contract or components of it may be leveraged to meet additional or similar requirements within DND.

ii) **Leveraging of DND Resources:** As the project progresses it may leverage internal DND/CAF, Other Government Departments (OGDs) or Five Eyes (FVEY) Nations resources and other existing or new procurement instruments.

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

iv) **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. It is Canada's intention to have an iterative and phased approach to the implementation.

v) **In-Service Support:** To assist Canada in determining in-service support (ISS) contracting options early in the procurement process Canada requests bidders provide answers to the ISS questions in Annex E. *Note: Responses to these questions are not a requirement of this ITQ.*

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

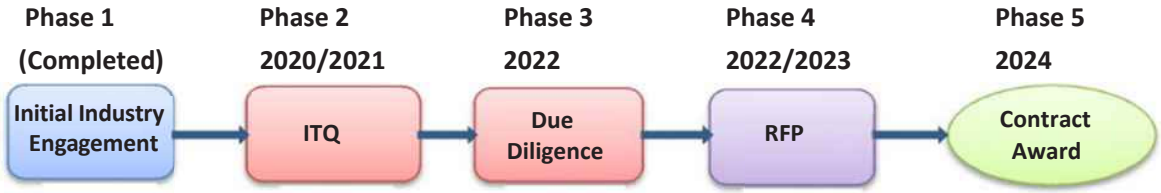
1.2.5 **Foreign Ownership, Control and Influence (FOCI):** A FOCI assessment will be required prior to contract award. The Contractor must complete and submit a Foreign Ownership, Control and Influence (FOCI) Questionnaire and associated documentation identified in the FOCI Guidelines for Organizations prior to contract award to identify whether a third party individual, firm or government can gain unauthorized access to COMSEC, NATO CLASSIFIED or FOREIGN CLASSIFIED information/assets.

1.2.6 **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	**Formal ITQ**	**Bidders Conference**	
Industry Day		**One-on-one Meetings**	
One-on-one Meetings			

1.3.1 **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

1.3.2 Phase 2 – Invitation to Qualify

Draft ITQ: The Draft ITQ was the commencement of the second phase in the procurement for the CD-DAR project. Suppliers were invited to submit written questions and comments on the Draft ITQ.

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.

1.3.3 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 B. Pre-qualified Supplier not meeting the security requirements will only have access to the non-classified components of the draft RFP. To the greatest extent possible while safeguarding national security 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 B.

1.3.4 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 B. 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. To the greatest extent possible while safeguarding national security 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.

1.3.5 **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

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

1.7.2 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.

1.7.3 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 (2020-05-28), 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;
v. Stuart Morrison; and
vi. Bethany Allen

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

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

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

2.1.3 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)”;

2.1.4 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;

2.1.5 Delete subsection 01 – Integrity Provisions – Bid;

2.1.6 Delete subsection 14 – Price Justification; and

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

2.1.8 The Phased Bid Compliance Process applies to this requirement.

2.2 Teaming Terminology

The following terms are defined in order to assist Respondents with the organization of their team in response to this ITQ:

2.2.1 "Association of Entities" means separate legal entities within a formally organized professional services network, where all members of the network operate using a common brand, with shared access to intellectual property, talent resources, integrated technology, methodology, strategies and policies across the network. It does not include unrelated affiliates of the Respondent with whom the Respondent is partnering through a Respondent Core Team or Joint Venture (as applicable).

2.2.2 “Entity” refers to any individual, corporation, partnership, firm, Joint Venture, syndicate, association, trust or other form of legal entity.

2.2.3 “Joint Venture” refers, collectively, to the Joint Venture Participants that comprise the Respondent.

2.2.4 “Joint Venture Participant” refers to an Entity that has entered into an arrangement with one or more other Entities, either contractually or by forming a new Entity, to combine money, property, knowledge, expertise or other resources in a joint endeavour.

2.2.5 “Prime Respondent” refers to the Core Team Member that will become the Contractor if the Respondent is selected as a Contractor during any stage of the Procurement Process.

2.2.6 "Respondent" means the Entity, Prime Respondent and its Core Team Members, or Joint Venture submitting a response to this ITQ.

2.2.7 “Respondent Representative” refers to the individual who has been authorized by the Respondent to represent and bind the Respondent, including all Core Team Members and Joint Venture Participants comprising the Respondent.

2.2.8 “Respondent Core Team” refers to, collectively, the Prime Respondent and its Core Team Members that comprise the Respondent.

2.2.9 “Team Member” refers to each Entity that is a member of a Respondent Core Team.

2.2.10 “Qualified Supplier and Pre-qualified Supplier” refers to a Respondent who has been selected by Canada under this ITQ.

2.3 Submission of Only One Response

2.3.1 A response may be submitted by:

i) a single Entity as the Respondent;
ii) a Prime Respondent and its Core Team Members together as the Respondent; or
iii) a Joint Venture as the Respondent.

2.3.2 For the purposes of this ITQ only, Respondents are not required to create a legal entity in order to submit a Response as a Respondent Core Team or a Joint Venture, but Canada anticipates this will be required prior to responding to the subsequent solicitation.

2.3.3 Canada requires that each Response, at the closing date of this ITQ or upon request from the Contracting Authority, be signed by the Respondent Representative, all Core Team Members and Joint Venture Participants, as applicable. Canada request signatures be provided through the Response Submission Form at Annex C. Respondents who submit a Response agree to be bound by the instructions, clauses and conditions of this ITQ.

2.3.4 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.

2.3.5 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.

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

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

2.3.8 **Respondent Representative:** A Respondent Representative must be appointed, and identified by name in the Response, to provide documentation and information to the Contracting Authority and to receive instructions and notices for and on behalf of the Respondent or any and all Core Team Members or Joint Venture Participants, as applicable.

2.4 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 C). If no other province or territory is specified, the Respondent agrees that the laws of Ontario are acceptable to it.

2.5 Questions, Comments and Communications

2.5.1 **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
Patti Wight / Laurie Stewart

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

2.5.2 **Deadline for Asking Questions:** All questions and comments regarding the solicitation must be submitted by email to the Contracting Authority no later than 10 calendar days before the ITQ closing date. Questions received after that time may not be answered.

2.5.3 **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.

2.5.4 **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.

2.6 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.

2.7 Security Requirements

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

2.7.1 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.

2.7.2 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 B, Section 1.2 Security Requirements for Phase 3 – Due Diligence.

2.7.3 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.

2.7.4 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 B. Pre-qualified Suppliers that

do not meet the security requirements for the Final RFP as detailed in Annex B Section 1.2 on the date the final RFP is released will be removed from the list of Pre-qualified Suppliers.

2.7.5 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 B, 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:

i. Response Submission Form at Annex C - Requested at ITQ Closing

Respondents are requested to include the Response Submission Form, found at **Annex C**, 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, the Core Team Members 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 Response Submission Form information when requested during the evaluation period is mandatory.

ii. Responses to the Qualification Requirements at Annex A – 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 and point rated criteria that are subject to evaluation in Annex A - Evaluation Criteria. Each of the Mandatory and Point Rated 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.

Note: Respondents are cautioned not to include, in their bid, any known classified information or a collection of information that when aggregated would become classified.

3.3 Respondent Core Team

3.3.1 A Respondent must identify each member of the Respondent Core Team in its Technical Bid.

3.3.2 When submitting a response as a Respondent Core Team, Unless otherwise stated specifically in the Technical Evaluation Criterion, the Respondent may submit information pertaining to the Respondent itself or to a member of its Core Team in demonstrating how they meet the Technical Evaluation Criterion. The Respondent must identify which member of its Core Team they are referring to in the information provided with each criterion.

3.3.3 Only the capabilities and experience of the Respondent Core Team will be considered when evaluating the response submitted to this ITQ. The capabilities and experience of subcontractors will not be evaluated unless such subcontractors are members of the Respondent Core Team as provided below.

3.4 Evaluation and Respondent Core Team

3.4.1 Except as expressly provided otherwise in this ITQ, a Respondent may meet the Technical Evaluation Criteria itself and bid as a corporation or other such single legal entity, or may meet the Technical Evaluation Criteria as a Respondent Core Team, if the Prime Respondent and the members of the Core Team together meet the Technical Evaluation Criteria.

3.4.2 A Respondent may rely on the experience of one of its Core Team members to meet any Technical Evaluation Criterion of this ITQ, unless otherwise stated specifically in the Technical Evaluation Criterion.

Example: A Respondent has a Core Team of X, Y and Z. If a solicitation requires: (a) that the Respondent have 3 years of experience providing maintenance service, and (b) that the Respondent have 2 years of experience integrating hardware with complex systems, then each of these two requirements can be met by a different member of the Core Team. However, for a single Technical Evaluation Criterion, such as the requirement for 3 years of experience providing maintenance services, the Respondent cannot indicate that each of Core Team members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive. Core Team members cannot pool their experience with other Core Team members or with the Bidder to satisfy a single Technical Evaluation Criterion of this bid solicitation.

Any Respondent with questions regarding the way in which a Core Team bid will be evaluated should raise such questions through the Enquiries process as early as possible during the ITQ bid solicitation period.

3.5 Composition of Core Team

3.5.1 Only a Respondent that has pre-qualified pursuant to the ITQ phase, will become a pre-qualified supplier and able to bid on any subsequent solicitation.

3.5.2 Respondents that become pre-qualified suppliers are advised that any change in name, corporate structure, legal status, corporate reorganization or sale or other transfer of its assets after the date of qualification under the ITQ may result in its disqualification from bidding, including disqualification from bidding as a Joint Venture Bidder.

3.5.3 Changes described above, including failure to maintain the Respondent Core Team, throughout the procurement process (unless approved in writing by the Contracting Authority) may, at the discretion of Canada, result in the Respondent becoming ineligible for continued participation in the CD-DAR .

3.6 Changes to the Respondent Core Team

3.6.1 As stated a Respondent must identify each member of the Respondent Core Team in its Technical Bid. The Respondent Core Team must continue to consist of the Core Team identified in the response to this ITQ throughout the process of this procurement.

3.6.2 Failure to maintain the Respondent Core Team throughout the procurement process (unless approved in writing by the Contracting Authority) may, at the discretion of Canada, result in the Respondent becoming ineligible for continued participation in the CD-DAR procurement process.

3.7 Electronic Submission of Response

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.

In light of the current COVID-19 pandemic, bids transmitted to PWGSC by facsimile or by any method other than e-post Connect will not be accepted.

Bidders must submit only using epost Connect to the Bid Receiving Unit in the National Capital Region (NCR). The email address is:

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

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

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 Respondent must submit 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.

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

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

4.2.2 **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.

4.2.3 **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.

4.2.4 **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.

4.4 Technical Evaluation

Mandatory Technical Criteria

The Phased Bid Compliance Process will apply to all mandatory technical criteria. The mandatory technical criteria are described in Annex A – Technical Evaluation Criteria, Table 1

Point-Rated Technical Criteria

The Phased Bid Compliance Process will apply to all Point-Rated Technical Criteria and the mandatory overall minimum threshold score. The point rated technical criteria and mandatory overall minimum threshold score are described in Annex A - Technical Evaluation Criteria, Table 2.

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

4.5 Basis of Qualification

4.5.1 Each Respondent whose response

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

ii. meets all the mandatory evaluation criteria at Annex A; and

iii. obtains the required minimum of 80 points overall for the technical evaluation criteria at Annex A which are subject to point rating. The rating is performed on a scale of 160 points

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

4.5.2 Responses not meeting (i) or (ii) or (iii) will be declared non-responsive.

4.5.3 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.

4.5.4 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.

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

4.6 ITQ Second Qualification Round

4.6.1 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.

4.6.2 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.

4.6.3 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: Mandatory Evaluation Criteria

1. Technical Evaluation Criteria

1.1 Mandatory Technical Criteria

The Respondent must meet the mandatory technical evaluation criteria specified in Table 1. 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.

1.2 Point Rated Technical Criteria

Responses which meet all of the Mandatory Technical Criteria will be evaluated and scored based on the Point-rated criteria specified in Table 2. All evaluation criteria listed in Table 2 are subject to the Phased Bid Compliance process. The Respondent must provide the necessary documentation to support compliance with this requirement. Each Point Rated Technical Criterion must be addressed separately.

1.3 Projects

1.3.1 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 that are not part of the Respondent Core Team.

(ii) a project must have been successfully implemented within the last seven (7) years of the ITQ closing date.

(iii) more than one (1) reference project may be used to meet all the evaluation criteria, however, not more than one (1) reference project can be used to meet an individual evaluation criteria.

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

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

(vi) a project may be used to meet multiple criteria.

(vii) the Respondent has to clearly identify their role, responsibilities, and deliverables of their contract in as much detail as possible.

(viii) 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.

1.3.2 Respondents are cautioned not to include in their bid any known classified information or a collection of information that when aggregated would be classified.

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

Respondents should only provide the required reference project(s) as indicated in each mandatory and point rated 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 or point rated requirement(s).

1.3.4 Respondents **must** detail the following for each referenced project:

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. Work on Classified Projects

If any project experience relevant to the mandatory or rated criteria was obtained in a classified environment, and for which a non-disclosure or Security of Information Act (SOIA) agreement was signed, it may not be possible to divulge pertinent details required to substantiate the experience called for in the criteria. Should the Respondent choose to include these classified projects, the following procedure is to be followed:

The Respondent is to identify the classified project as "Project A, B, C" etc., as applicable, and identify the start/end dates and duration of the project. The Respondent must also provide a client reference, such as the project lead, with their contact information. This reference must be able to provide the information needed to verify compliance with the evaluation criteria.

The evaluation team, including a Contract Authority with appropriate security clearance, will verify with the project leads the work completed as specified in the criteria.

The results of the reference check will be used in the determination of the mandatory and rated criteria. Should the Respondent's reference be unable to provide the information needed to verify compliance with the evaluation criteria, the response will be deemed to have failed to meet the criteria.

3. Form 2 – Project Reference Check Form

Instructions to Respondents:

a) Respondents are requested to submit a Project Reference Check Form for each project referenced in response to each mandatory and point rated requirement in Tables 1 and 2 of Annex A 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 provided.

Form 2 - Project Reference Check Form

#	Response		
(a)	Mandatory/Point Rated Requirement Number (from Table 1 or 2 of Annex A)		
(b)	Respondent or Core Team Member Full Legal Name (if the Respondent 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 Respondent (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 (if applicable).		
	Number of Users:	Number of Endpoints:	
(m)	Identify the components for which the Respondent was 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 the respondent was 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		

Table 1 - Mandatory Technical Evaluation Criteria

Terms or words in Italics are defined in Table 3 - Definitions

Serial	Mandatory Criteria	Evaluation	**Proof Required** (in the last 7 years before date of ITQ closing)
M1	The Respondent must have Successfully Implemented one (1) Complex Information Management/Information Technology (IM/IT) Project in the last seven (7) years, which included the design, development, integration, implementation, and delivery of Commercial off the Shelf (COTS)/Government off the Shelf (GOTS)/Military Off-the-Shelf (MOTS) Cyber Security and Cyber Decision Analysis and Response integrated solutions, complete with the provision of at least 12 months of Stabilization Support, deployed on: **a. *Complex IM/IT Networks* of 8,000 or more *Endpoints; and*** **b. For one or more of the Five Eyes (FVEY) nations (AUS/CAN/NZ/UK/US).**	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented* COTS/GOTS/MOTS–based *Cyber Security* and *Cyber Decision Analysis and Response* integrated solutions within FVEY nations for Criteria 1.
M2	The Respondent must have *Successfully Implemented* one (1) *Complex IM/IT Project* in the last seven (7) years, which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Cyber Decision Analysis and Response* of COTS/GOTS/MOTS integrated solutions for **8,000 or more *Endpoints*** within FVEY nations that provided the capabilities listed at (a) and (b) and least five (5) of the capabilities listed from (c) to (h) below: **a. Provide *Cyber Decision Analysis and Response* of *Command and Control (C2) Networks* through an integrated Common Operating Picture (COP); and** b. **Provide *Cyber Decision Analysis and Response* of *Command and Control (C2) Networks* through Cloud Security;** **c. Identify and track all (authorized and non-authorized) IM/IT assets;** **d. Assess asset vulnerabilities, configuration, risk and patch compliance;** **e. Collect, retain and analyze cyber threat information;** **f. Detect and assess suspicious activity and provide context for risk and vulnerability assessments;** **g. Execute prevention and response to threats and remediation actions in *near real-time*;**	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 2.

	h. **Provide at least 12 months of *Stabilization Support*.**		
M3	The Respondent must have *Successfully Implemented* one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* integrating multiple (at least 5 or more) COTS/GOTS/MOTS solutions within FVEY nations **that demonstrate ALL of the following within a *Complex IM/IT Network* environment of 8,000 or more *Endpoints,* complete with the provision of at least 12 months of *Stabilization Support*, in the last seven (7) years:** **a. Continuous data collection, retention, detection, analysis (all in *near real-time*) and provide context for risk and vulnerability assessments; and** 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*);***	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 3.
M4	The Respondent must have *Successfully Implemented* one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* integrating multiple (at least 5 or more) COTS/GOTS /MOTS solutions within FVEY nations **that demonstrate ALL of the following within a *Complex IM/IT Network* environment of 8,000 or more *Endpoints,* complete with the provision of at least 12 months of *Stabilization Support*, in the last seven (7) years performing Advanced Data Analytics and response utilizing:** **a. Integrated *Cyber Security* incident analysis from:** **i. Threat intelligence,** **ii. Past Incidents,** **iii. Similar Incidents across networks, and** **iv. Signature and heuristic-based detection** **b. Integrated Cyber Security data analysis from:** **i. Security Incident and Event Management (SIEM),** **ii. End Point Detection and Response (EDR),** **iii. Full Packet Capture (FPC),** **iv. Intrusion Detection and Intrusion Prevention System (IPS/IDS), and**	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 4.

	v. Vulnerability Assessments, and **vi. Workflow Management** **c. Integrated *Cyber Security* alerts from 3 out of 6 below:** **i. Threat intelligence,** **ii. External entity information,** **iii. Internal asset information,** **iv. Information from network and end points,** **v. Activity history, and** **vi. Information from Network Traffic Analysis**		
M5	The Respondent must have *Successfully Implemented* 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/MOTS integrated solutions within FVEY nations and provision of at least 12 months of *Stabilization Support* – **utilizing *Adaptive* and *Dynamic* identification, containment and eradication of threats (insider and external) using advanced Cyber Defence capabilities in *near real-time* utilizing standardized platforms within a *Complex IM/IT Network* of 8,000 or more *Endpoints* in the last seven (7) years.**	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 5.
M6	The Respondent must have *Successfully Implemented* one (1) *Complex IM/IT Project* in the last seven (7) years, which included the design, development, integration, implementation, and delivery of *Cyber Security* and *Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations and provision of at least 12 months of *Stabilization Support* - **establishing a data repository that supports the storage, integration, retrieval, analysis, and processing of structured and unstructured data (including Packet Capture (PCAP), Netflow, Common Event Format (CEF)) of a geographically dispersed network (10 or more nodes) and the performance of *Tier 2 Analysis* in order to enable decision support through automated and assisted execution of responses for a *Complex IM/IT Network* of 8,000 or more *Endpoints*.**	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 6.
M7	The Respondent must have *Successfully Implemented* one (1) *Complex IM/IT Project* which included the design, development, integration, implementation, and delivery of	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the

	Cyber Security and *Decision Analysis and Response* COTS/GOTS/MOTS solutions within FVEY and provision of at least 12 months of *Stabilization Support* - **For *Complex IM/IT Networks,* of 8,000 or more *Endpoints* and must have provided all of the interoperability functionalities below within FVEY nations in the last seven (7) years:** **a. The ability to integrate feeds seamlessly, such as threat vectors, analyses information, etc., with key partners such as OGDs, FVEY nations, or industry;** **b. Central collection of Threat Intelligence;** **c. Fusion and deduplication of Threat Intelligence;** **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).**		Respondent has *Successfully Implemented Cyber Security* and *Cyber Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 7.
M8	The Respondent must have *Successfully Implemented* 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 8,000 or more *Endpoints* within FVEY nations in the last seven (7) years**. This must include-the development of operational and support scenarios which can be created, modified, maintained, and executed by Cyber Operators within an exercise/training environment.	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has developed and delivered exercise and training solutions within FVEY nations for Criteria 8.
M9	The Respondent must have *Successfully Implemented* 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/MOTS integrated solutions within FVEY nations and provision of at least 12 months of *Stabilization Support* **– For the administration and management of data collection (such as but not limited to IT and Cyber assets, configuration, etc.)from *heterogeneous* sources and developing Configuration Management solutions for large collections of data in *Complex IM/IT Networks* of 8,000 or more *Endpoints* in the last seven (7) years.**	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented Cyber Security* and *Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 9.

M10	The Respondent must have *Successfully Implemented* 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/MOTS integrated solutions within FVEY nations **for which the Respondent have provided 3rd line technical support for a period of at least 12 contiguous months in the last seven (7) years where technical support met or exceeded each of the following:** **a. operated 5 days per week;** **b. 8 hours per day; and,** **c. 52 weeks per year**	Pass / Fail	The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has *Successfully Implemented Cyber Security* and *Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions within FVEY nations for Criteria 10.

Table 2 – Point Rated Technical Evaluation Criteria

Responses which meet all of the Mandatory Technical Criteria will be evaluated and scored based on the following Point-rated criteria.

Req #	Point Rated Evaluation Criteria	Scoring	Score	Proof Required (in the last 7 years before date of ITQ closing)
R1	The Respondent has *Successfully Implemented* Complex IM/IT Project which included the design, development, integration, implementation, and delivery of *Cyber Security and Cyber Decision Analysis and Response* COTS/GOTS/MOTS integrated solutions and re-synchronization within FVEY nations and provision of at least 12 months of S*tabilization Support* in the last seven (7) years for *Cyber Security and Cyber Decision Analysis and Response* utilizing the following emerging technologies as part of the core *Cyber Security and Cyber Decision Analysis and Response* integrated solutions: a) Anomaly detection and Data Analysis using Machine Learning; i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints b) Big Data Analysis; i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints c) Security Orchestration Automation and Response (SOAR); i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints d) Threat Hunting and Vulnerability Discovery using Artificial Intelligence; i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and	Points will be awarded based on the number of endpoints for the project. Points will only be awarded once for each of (a) to (e). Sum of points below, up to a **maximum of hundred and ten (110) points:** 10 points 20 points 30 points 40 points 5 points 10 points 15 points 20 points 5 points 10 points 15 points 20 points 5 points 10 points 15 points		For <u>each</u> of the sub-categories in the Rated Criteria R1 the Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has Successfully Implemented Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions within FVEY nations. One or more Projects can be used to meet the Rating Criteria R1 (a) to (e) but not more than one project may be used for any one of (a) to (e)

	iv) More than 8000 endpoints e) User and Entity Behavioural Analysis; i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints	20 points 4 points 6 points 8 points 10 points		
R2	The Respondent has Successfully Implemented one (1) Complex IM/IT Project which included the design, development, integration, implementation, and delivery of Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions within FVEY nations and provision of at least 12 months of Stabilization Support in the last seven (7) years for systems incorporating multi-level security environments and a Cross Domain Gateway between them: i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints	**Points will be awarded based on the number of endpoints for the project. Maximum: Twenty (20) points** 5 points 10 points 15 points 20 points		The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has Successfully Implemented Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions within FVEY nations for the Rated Criteria R2
R3	The Respondent has Successfully Implemented one (1) Complex IM/IT Project in the last seven (7) years, which included the design, development, integration, implementation, and delivery of Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions and re-synchronization within FVEY nations and provision of at least 12 months of Stabilization Support for all of the following in a given network: (a) within a globally distributed network components on two (2) or more continents with a minimum of ten (10) separate operating nodes, (b) interconnected at disadvantaged speed (less than 1.544 Mbps links) remoted in austere environments to a High speed (100Mbps or above) central network, and (c) for information related to Mandatory Evaluation Criteria #1 to #6 in a network of: i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and	**Points will be awarded based on the number of endpoints for the project.** **Maximum: Twenty (20) points** 5 points 10 points 15 points		The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has Successfully Implemented Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions within FVEY nations for the Rated Criteria R3

	iv) More than 8000 endpoints	20 points		
R4	The Respondent has Successfully Implemented one (1) Complex IM/IT Project in the last seven (7) years, which included the design, development, integration, implementation, and delivery of Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions within FVEY nations in a military environment and provision of at least 12 months of Stabilization Support for: i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints	**Points will be awarded based on the number of endpoints for the project.** **Maximum: Ten (10) points** 2 points 4 points 6 points 10 points		The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has Successfully Implemented Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions within FVEY nations for the Rated Criteria R4
Total Score (Maximum of 160 points, Mandatory Pass Score of 80 points)				

* Note: For all Rated Criteria R1 to R4, 2000 or less end points will earn zero (0) points

Table 3 - 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 that is often used to describe machines (or computers) that mimic "cognitive" functions that It is the ability of a functional unit to perform functions that are generally associated with human intelligence and self-improvement (i.e. mimic “cognitive” functions that humans associate with the human mind, such as “reasoning”, "learning" and "problem solving") without human intervention.
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 cyber attacks 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	Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.
Cloud Computing	Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using services provided outside of the organization under 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.

Term	Definition
Command and Control (C2) Networks	Generically, the term Command and Control (C2) means a process (not the systems, as often thought) that -cyber security decision makers, including organizations responsible for decision making, use to plan, direct, coordinate, and control their own team resources and cyber assets to ensure seamless organizational functioning, mission continuity and success.
Common Operating Picture (COP)	The COP is a command and control tool that provides situational awareness and response options enabling users to make accurate, informed decisions. Data is integrated from multiple sources to support all functions of a response using one spatial data platform. The COP will provide the acting incident management team with a comprehensive picture to make adjustments to any current activity and also plan ahead for the next operational period.
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	Cyber Security is defined as integrated technologies and processes at all conceptual layers of an enterprise including the perimeter, the internal network,

Term	Definition
	the various endpoints, the applications, and the data contained for analyzing the information, defending the enterprise network and responding to adversaries and the threats posed by them. In addition, it involves developing cyber security solution for next generation cyber concepts and processes to provide the optimal security at each layer, developing these in a way that can support each other, in where it is best in the architecture (and design) to employ these to provide a robust cyber analysis, defence, and response.
Decision Analysis and Response	Attaining an accurate characterization of cyber-assets individually or as a network for vulnerability, usage weakness, or threat based on months/years of aggregated data and implementing approved security and defensive cyber course of actions to maintain continued freedom of action.
Deployed	A capability supporting an expeditionary (geographically dispersed, most often operated in a threat environment) base that employs and sustains task 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
Intrusion Detection System	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner through a software and/or hardware appliance. The service is implemented on host or at network with a monitoring activity that is associated with intrusions or insider misuse, or both.
Intrusion Protection System	Software or hardware appliance that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents such as unwanted activity that disrupts operations.
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.

Term	Definition
Machine Learning	The capability composed of many technologies (such as deep learning, neural networks and natural language processing), used in unsupervised and supervised learning, that operate guided by relevant data from existing information.
Multi-level Security	Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization
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.
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.
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 and/or capability fully implemented (can be part of a multi-phase project) 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.
User Entity Behaviour Analysis (UEBA)	User and entity behavior analytics (UEBA) solutions use analytics to build the standard profiles and behaviors of users and entities (hosts, applications, network traffic and data repositories) across time and peer group horizons. Activity that is anomalous to these standard baselines is presented as suspicious, and packaged analytics applied on these anomalies can help discover threats and potential incidents. The most common use cases sought by enterprises are detecting

Term	Definition
	malicious insiders and external attackers infiltrating their organizations (compromised insiders).
Vulnerability Assessment	The vulnerability assessment (VA) is a capability to identify, categorize and manage vulnerabilities. These include unsecure system configurations, software or hardware issues that make it susceptible to insider or external cyber intrusion and attack, or missing patches, as well as other security-related updates in the systems connected to the enterprise network directly, remotely or in the cloud.

Annex B: 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.

1.2.1 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;
(b) Industrial Security Manual (Latest Edition).

1.2.2 SECURITY REQUIREMENT FOR FOREIGN SUPPLIER:

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

SECRET, NATO Unclassified, NATO Restricted, NATO SECRET, Foreign Classified

For the exchange of Canada Classified information, the contractor and/or any and all subcontractors must be from a country with which Canada has an international bilateral industrial security instrument or will have such an instrument with Canada by the end of the bidding period. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-eng.html For the exchange of NATO information the contractor/offeror/subcontractor must be a NATO member in good standing.

All **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets, furnished to the Foreign recipient **Contractor / Offeror / Subcontractor**, shall be safeguarded as follows:

1. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of the **Contract / Standing Offer / Subcontract**, hold a valid Facility Security Clearance (FSC), issued by the National Security Authority (NSA) or Designated Security Authority (DSA) **of the supplier's country**, at the equivalent level of **SECRET AND NATO SECRET** and hold an approved Document Safeguarding Capability Clearance at the level of **SECRET AND NATO SECRET** in accordance with the National legislation, regulations and policies of the supplier's country.
2. All **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets provided or generated under this **Contract / Standing Offer / Subcontract** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Contract / Standing Offer / Subcontract,** in accordance with the National legislation, regulations and policies of the supplier's country.
3. The Foreign recipient **Contractor / Offeror / Subcontractor** shall provide the **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Security legislation, regulations, policies and as prescribed by the National Security Authority (NSA) or Designated Security Authority (DSA) of the supplier's country.
4. All **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets provided to the Foreign recipient **Contractor / Offeror / Subcontractor** pursuant to this **Contract / Standing Offer / Subcontract** by the Government of Canada, shall be marked by the Foreign recipient **Contractor / Offeror / Subcontractor** with the equivalent security classification utilized by the supplier's country and in accordance with the National legislation, regulations and policies of the supplier's country.
5. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of this **Contract / Standing Offer / Subcontract**, ensure the transfer of **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets be facilitated in accordance with the

National legislation, regulations and policies of the supplier's country, and in compliance with the provisions of the Bilateral Industrial Security Instrument between the supplier's country and Canada.

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

7. Canadian persons that examine, posses, or transfer controlled goods (*refer to Note) that are domestically controlled by Public Services and Procurement Canada (PSPC) for Contracts and Subcontracts are required to register with PSPC's Controlled Goods Program (CGP) before accessing controlled goods, unless excluded from CGP registration as defined by the Controlled Goods Regulations.

   Throughout the duration of this Contract and Subcontract, the Foreign recipient Contractor and Subcontractor must adhere to its respective national policies pertaining to the examination, possession, or transfer of controlled goods and must immediately report to its responsible National Security Authority (NSA) all cases in which it is known or there is reason to suspect that controlled goods, furnished or generated pursuant to this Contract and Subcontract have been lost or disclosed to unauthorized persons (entities not registered with the CGP or entities not excluded from CGP registration), including but not limited to a third party government, person, firm, or representative thereof. Controlled goods which are lost or compromised while handled outside of Canada, should be immediately reported, as per the requirements of the Treasury Board of Canada Secretariat's Controlled Goods Directive and Directive on Material Management and to the Canadian Government Authority owner of the controlled goods, for example the Canadian Department that issued the controlled goods to the Foreign recipient Contractor and Subcontractor, as part of this Contract and Subcontract. Additionally, controlled goods that are lost or disclosed to unauthorized persons which are subject to the United States of America's (U.S.) the export controls of International Traffic in Arms Regulations of the United States of America International Traffic in Arms Regulations, will require the NSA or the Canadian Government Authority owner to report the situation to the U.S. exporter or the U.S. Department of State's Directorate of Defense Trade Controls (DDTC).

   *Note: Controlled goods are goods, including components and their associated technologies (e.g., blueprints, technical specifications, etc.), that primarily have a military or national security significance, including "defense articles" that are controlled by the United States' International Traffic in Arms Regulations. The list of controlled goods Controlled Goods List contained in the Schedule to the Defence Production Act (section 35) details the specific controlled goods that are domestically controlled by PSPC.

8. Such **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets releasable to

Australia, Canada, the United States of America, the United Kingdom, and New Zealand must be released only to foreign recipient **Contractor / Offeror / Subcontractor** personnel who have a need to know for the performance of the **Contract / Standing Offer / Subcontract,** must be a citizen of Australia, Canada, the United States of America, the United Kingdom, and/or New Zealand and must each hold a valid personnel security screening at the level of **SECRET OR NATO SECRET** as required, granted or approved by their respective country National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the National legislation, regulations and policies of the supplier's country.

9. **CANADA PROTECTED / CLASSIFIED** information/assets shall be released only to Foreign recipient **Contractor / Offeror / Subcontractor** personnel, who have a need-to-know for the performance of the **Contract / Standing Offer / Subcontract** and who have a Personnel Security Clearance at the level of **SECRET or NATO SECRET** as required, granted by their respective National Security Authority (NSA) or Designated Security Authority (DSA) of the supplier's country, in accordance with the National legislation, regulations and policies of the supplier's country.

10. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not access **NATO RESTRICTED** information/assets without prior consultation with their respective NSA/DSA for appropriate safeguarding measures in accordance with the National legislation, regulations and policies of the supplier's country.

11. The Foreign recipient **Contractor / Offeror / Subcontractor** personnel requiring access to **NATO UNCLASSIFIED** information/assets are not required to hold a personnel security clearance issued by their National Security Authority/Designated Security Authority. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, nevertheless, ensure that the **NATO UNCLASSIFIED** information/assets are not releasable to third parties and that the "need to know" principle is applied to personnel accessing this information/asset. For the purpose of this clause, the "need to know" principle means that the National Security Authority/Designated Security Authority has positively determined that a prospective recipient of **NATO UNCLASSIFIED** information/assets, has a requirement for access to, knowledge of, or possession of the **NATO UNCLASSIFIED** information/assets, in order to perform the services and tasks required pursuant to the **Contract / Standing Offer / Subcontract. Contracts / Standing Offers / Subcontracts**, which contain **NATO UNCLASSIFIED** requirements are NOT to be awarded without the prior written approval of the Canadian DSA.

12. The Foreign recipient **Contractor / Offeror / Subcontractor** personnel requiring access to **NATO CONFIDENTIAL** or above information/assets and/or sensitive sites shall hold a valid personnel security screening at the level of **NATO SECRET**, have been properly cleared, briefed and approved by the respective delegated **NATO** responsible security authority.

13. **FOREIGN, NATO AND CANADA PROTECTED** and **CLASSIFIED** information/assets provided or generated pursuant to this **Contract / Standing Offer / Subcontract** shall not be further provided to a third party Foreign recipient Subcontractor unless:

a. written assurance is obtained from the third-party Foreign recipient's National Security Authority (NSA) or Designated Security Authority (DSA) to the effect that the third-party Foreign recipient Subcontractor has been approved for access to **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets by the third-party Foreign recipient's NSA/DSA; and

b. written consent is obtained from the NSA/DSA of the supplier's country, if the third-party Foreign recipient Subcontractor is located in a third country.

14. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of their respective National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the National legislation, regulations and policies of the supplier's country.

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

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

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

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

19. The Foreign recipient **Contractor / Offeror / Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets pursuant to this Contract / Standing Offer /

Subcontract has been compromised.

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

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

22. The Foreign recipient **Contractor / Offeror / Subcontractor** shall comply with the provisions of the International bilateral industrial security instrument between the supplier’s country and Canada, in relation to equivalencies.

23. The Foreign recipient **Contractor / Offeror / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex B.

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

Non-NATO Subcontractor Information

25. In addition to these contract security clauses, the following clauses apply to all industry from a NON-NATO member country – accessing NATO classified information and assets. No NATO information will be released to non-NATO countries unless approved by the Canadian DSA.

26. When the foreign recipient supplier is registered with the industrial security program of a non-NATO member nation and requires access to NATO classified information, it is the responsibility of the NSA or DSA of that nation, in which the hiring entity is located and incorporated, to determine whether that NON-NATO National could be granted access to NATO classified information and assets by seeking the approval of either the Canadian DSA or NATO Headquarters (HQ). The decision whether to grant access is mutually determined between the relevant Designated Security Authority(ies) and the originator of the NATO Classified information.

27. When the Foreign recipient supplier from a Non-NATO member country is anticipated to require access to NATO classified information, the foreign recipient subcontractor must first seek approval from the Canadian DSA through the foreign recipient NSA or DSA.

28. The Canadian DSA must investigate the circumstances warranting access of NATO classified information and assets to citizens from a Non-NATO member country, working in Canada, and provide a determination as to whether NATO classified information and assets can be accessed by citizens from a non-NATO member country.

29. In cases where the Canadian DSA determines suppliers from Non-NATO member countries can be granted access to NATO classified information, a signed letter from the Canadian DSA must be used as the approving vehicle.

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.

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

1.3.2 SECURITY REQUIREMENT FOR FOREIGN SUPPLIER:

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

For the exchange of Canada Classified information, the contractor and/or any and all subcontractors must be from a country with which Canada has an international bilateral industrial security instrument or will have such an instrument with Canada by the end of the bidding period. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-eng.html For the exchange of NATO information the contractor/offeror/subcontractor must be a NATO member in good standing

All **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets, furnished to the Foreign recipient **Contractor / Offeror / Subcontractor**, shall be safeguarded as follows:

1. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of the **Contract / Standing Offer / Subcontract**, hold a valid Facility Security Clearance (FSC), issued by the National Security Authority (NSA) or Designated Security Authority (DSA) **of the supplier's country,** at the equivalent level of **SECRET, TOP SECRET, TOP SECRET SIGINT AND NATO SECRET** and hold an approved Document Safeguarding Capability Clearance at the level of **SECRET, TOP SECRET, TOP SECRET SIGINT AND NATO SECRET** in accordance with the National legislation, regulations and policies of **the supplier's country**.

2. All **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets provided or generated under this **Contract / Standing Offer / Subcontract** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Contract / Standing Offer / Subcontract**, in accordance with the National legislation, regulations and policies of **the supplier's country**.

3. The Foreign recipient **Contractor / Offeror / Subcontractor** shall provide the **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Security legislation, regulations, policies and as prescribed by the National Security Authority (NSA) or Designated Security Authority (DSA) **of the supplier's country**.

4. All **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets provided to the Foreign recipient **Contractor / Offeror / Subcontractor** pursuant to this **Contract / Standing Offer / Subcontract** by the Government of Canada, shall be marked by the Foreign recipient **Contractor / Offeror / Subcontractor** with the equivalent security classification utilized by **the supplier's country**

and in accordance with the National legislation, regulations and policies of **the supplier's country**.

5. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of this **Contract / Standing Offer / Subcontract**, ensure the transfer of **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets be facilitated in accordance with the National legislation, regulations and policies **of the supplier's country**, and in compliance with the provisions of the Bilateral Industrial Security Instrument between **the supplier's country** and Canada.

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

7. Canadian persons that examine, posses, or transfer controlled goods (*refer to Note) that are domestically controlled by Public Services and Procurement Canada (PSPC) for Contracts and Subcontracts are required to register with PSPC's Controlled Goods Program (CGP) before accessing controlled goods, unless excluded from CGP registration as defined by the Controlled Goods Regulations.

   Throughout the duration of this Contract and Subcontract, the Foreign recipient Contractor and Subcontractor must adhere to its respective national policies pertaining to the examination, possession, or transfer of controlled goods and must immediately report to its responsible National Security Authority (NSA) all cases in which it is known or there is reason to suspect that controlled goods, furnished or generated pursuant to this Contract and Subcontract have been lost or disclosed to unauthorized persons (entities not registered with the CGP or entities not excluded from CGP registration), including but not limited to a third party government, person, firm, or representative thereof. Controlled goods which are lost or compromised while handled outside of Canada, should be immediately reported, as per the requirements of the Treasury Board of Canada Secretariat's Controlled Goods Directive and Directive on Material Management and to the Canadian Government Authority owner of the controlled goods, for example the Canadian Department that issued the controlled goods to the Foreign recipient Contractor and Subcontractor, as part of this Contract and Subcontract. Additionally, controlled goods that are lost or disclosed to unauthorized persons which are subject to the United States of America's (U.S.) the export controls of International Traffic in Arms Regulations of the United States of America International Traffic in Arms Regulations, will require the NSA or the Canadian Government Authority owner to report the situation to the U.S. exporter or the U.S. Department of State's Directorate of Defense Trade Controls (DDTC).

   *Note: Controlled goods are goods, including components and their associated technologies (e.g., blueprints, technical specifications, etc.), that primarily have a military or national security significance, including "defense articles" that are controlled by the United States' International

Traffic in Arms Regulations. The list of controlled goods Controlled Goods List contained in the Schedule to the Defence Production Act (section 35) details the specific controlled goods that are domestically controlled by PSPC.

8. Such **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets releasable to Australia, Canada, the United States of America, the United Kingdom, and New Zealand must be released only to foreign recipient **Contractor / Offeror / Subcontractor** personnel who have a need to know for the performance of the **Contract / Standing Offer / Subcontract**, must be a citizen of Australia, Canada, the United States of America, the United Kingdom, and/or New Zealand and must each hold a valid personnel security screening at the level of **SECRET OR NATO SECRET** as required, granted or approved by their respective country National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the National legislation, regulations and policies of **the supplier's country**.

9. **CANADA PROTECTED / CLASSIFIED** information/assets shall be released only to Foreign recipient **Contractor / Offeror / Subcontractor** personnel, who have a need-to-know for the performance of the **Contract / Standing Offer / Subcontract** and who have a Personnel Security Clearance at the level of **SECRET or NATO SECRET as required**, granted by their respective National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country**, in accordance with the National legislation, regulations and policies of **the supplier's country**.

10. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not access **NATO RESTRICTED** information/assets without prior consultation with their respective NSA/DSA for appropriate safeguarding measures in accordance with the National legislation, regulations and policies of **the supplier's country**.

11. The Foreign recipient **Contractor / Offeror / Subcontractor** personnel requiring access to **NATO UNCLASSIFIED** information/assets are not required to hold a personnel security clearance issued by their National Security Authority/Designated Security Authority. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, nevertheless, ensure that the **NATO UNCLASSIFIED** information/assets are not releasable to third parties and that the "need to know" principle is applied to personnel accessing this information/asset. For the purpose of this clause, the "need to know" principle means that the National Security Authority/Designated Security Authority has positively determined that a prospective recipient of **NATO UNCLASSIFIED** information/assets, has a requirement for access to, knowledge of, or possession of the **NATO UNCLASSIFIED** information/assets, in order to perform the services and tasks required pursuant to the **Contract / Standing Offer / Subcontract**. **Contracts / Standing Offers / Subcontracts**, which contain **NATO UNCLASSIFIED** requirements are NOT to be awarded without the prior written approval of the Canadian DSA.

12. The Foreign recipient **Contractor / Offeror / Subcontractor** personnel requiring access to **NATO CONFIDENTIAL** or above information/assets and/or sensitive sites shall hold a valid personnel security screening at the level of **NATO SECRET**, have been properly cleared, briefed and approved

by the respective delegated NATO responsible security authority.

13. **FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED** information/assets provided or generated pursuant to this **Contract / Standing Offer / Subcontract** shall not be further provided to a third party Foreign recipient Subcontractor unless:

    a. written assurance is obtained from the third-party Foreign recipient's National Security Authority (NSA) or Designated Security Authority (DSA) to the effect that the third-party Foreign recipient Subcontractor has been approved for access to FOREIGN, NATO AND CANADA PROTECTED and CLASSIFIED information/assets by the third-party Foreign recipient's NSA/DSA; and

    b. written consent is obtained from the NSA/DSA of **the supplier's country**, if the third-party Foreign recipient Subcontractor is located in a third country.

14. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of their respective National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the National legislation, regulations and policies of the supplier's country.

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

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

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

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

Designated Security Authority (DSA).

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

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

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

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

23. The Foreign recipient **Contractor / Offeror / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex B.

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

25. A Communications-Electronic Security (COMSEC) account at the {insert appropriate level} level must be issued and confirmed by the National Communication Security Authority (NCSA) of {name of country}. The Foreign recipient {**Contractor / Offeror / Subcontractor**} requiring access to accountable COMSEC material (ACM) and/or COMSEC information/assets must be citizens of {name of country}, hold a valid Personnel security clearance commensurate with the information/assets that will be accessed, have a need to know, have undergone a COMSEC briefing and signed a COMSEC Briefing Certificate. Access by Foreign Nationals or {Contracting officers should enter the terminology "Resident Aliens" in cases when the country of the Foreign recipient Contractor is the USA} must be approved by the NCSA of {name of country}, on a case by case basis. Such approvals must be communicated in writing to the Canadian Designated Security Authority (DSA).

1.4 Security Requirements Check Lists (SRCLs)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contra:
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

Canada	NATO / OTAN	Foreign / Étranger
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?

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED? — ✓ No / Non — Yes / Oui
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

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? — ✓ No / Non — Yes / Oui
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

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 Organization / 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 : FVEYS members only as applicable	Specify country(ies): / Préciser le(s) pays : CAN/UK/US members only as applicable	Specify country(ies): / Préciser le(s) pays : FVEYS members only as applicable

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

Canada	NATO / OTAN	Foreign / Étranger
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 C: Response Submission Form

Invitation to Qualify No. W6369-20CY06/A Response Submission Form				
Prime Respondent 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			
Prime 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 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.
Prime 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 the section 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:
If submitting a response to the ITQ as a Respondent Core Team each Core Team Member must complete the section below [Respondent to add more rows if more than two (2) Core Team members]
Core Team Member Full Legal Name:
Core Team Member address:
Core Team Member Representative Name:
Email:
Signature of authorized representative of Core Team Member:
Telephone:
Date:

Annex D: 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 was posted on Buy and Sell allowing for Industry to provide feedback prior to issuing the final ITQ. Suppliers were invited to provide written comments and questions on the draft ITQ.

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 Suppliers 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 intends to post (within the constraints of national security) 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 intends to post (within the constraints of national security)-unclassified components of the RFP on Buy and Sell, however only Pre-qualified Suppliers will be invited to bid on the solicitation.

Annex E: Query on In-Service Support

In order to assist Canada in determining in-service support (ISS) options early in the procurement process Canada requests bidders provide answers to the following question with their response. Do note responses to these questions are NOT mandatory and will NOT play a part in the respondents bid evaluation.

1. What initial support is included with the potential solution?
2. What type of support is required with the solution after initial support (e.g. how many years, any option years etc.)?
3. What type of Service Level Agreement would be required (e.g. support parameters)?
4. What type of payment (e.g. fixed monthly, services rendered, etc.) structure would be required?
5. Would your proposed solution contain IP rights that would be restricting future In-service contract?
6. Would a third party be allowed access or use of the IP rights you own to perform in-service support functions? If not please advise why this is not possible?

Attachment 1: Draft Statement of Requirements (DSOR)

Attachment 2: Draft Concept of Operations (CONOPS)

National Defence | Défense nationale

Statement of Requirements

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

C.000707

PROJECT APPROVAL DOCUMENTATION

VERSION [1.0]

RECORDS MANAGEMENT LOCATION: [INSERT WHERE UP TO DATE DOCUMENT IS FILED (GCDOCS/RDIMS/ETC.)]

Draft

Draft

TABLE OF CONTENTS

1 INTRODUCTION 7
1.1 Background 7
1.2 Business Need Statement and Outcomes 7
1.2.1 Business Need Statement 7
1.2.2 Drivers for Change 8
1.2.3 Capability Gap 9
1.2.4 Business Outcomes 9
2 HIGH LEVEL MANDATORY REQUIREMENTS (HLMRs) 11
2.1 Key Assumptions 12
2.2 Initial Operational Capability (IOC) (high level) 13
2.3 Final Operational Capability (FOC) (high level) 13
2.4 Capability Deficiency 13
2.5 Project Constraints 17
2.6 Current Situation 18
2.7 Project Interdependencies 18
2.7.1 Dependencies 19
2.7.2 Contributions 19
3 SYSTEM OPERATION 21
3.1 Mission and Scenarios 21
3.2 Environment 22
3.3 Threats 23
3.4 Concepts of Operations 25
3.5 Concept of Support 26
3.6 Key Roles 26
3.7 Key Tasks 27
3.7.1 Preparing for Defensive Cyber Operations (DCO) 27
3.7.2 DCO Preparation Operations 30
3.7.3 DCO Execution 31
3.7.4 DCO Support Functions 33

Draft

3.7.5 Knowledge and Action Management Systems 36
3.8 User Characteristics 36
3.8.1 Cyber Operators 36
4 DESIGN AND CONCEPT GUIDANCE 39
4.1 Included Work and Services 39
4.1.1 Cyber Domain Data Sources 40
4.1.2 Deployed Capabilities 40
4.2 Excluded Work and Services 41
4.3 Use of Technology 41
4.4 Design Concept 43
4.5 Security Assessment and Authorization 47
5 SYSTEM EFFECTIVENESS REQUIREMENTS 48
5.1 General Requirements 48
5.2 Operability 48
5.3 Survivability 49
5.4 Maintainability 49
5.5 Availability 50
5.6 Reliability 50
5.7 Environmental Sustainability 51
5.8 Gender-Based Analysis Plus (GBA+) 51
5.9 Safety and Health 52
5.10 Delivery Requirements 52
5.11 Sub-System Effectiveness Requirements 52
6 PERFORMANCE MEASURES 53
6.1 System Level Measures 53
6.2 Sub-System Level Measures 57
7 PERSONNEL AND TRAINING REQUIREMENTS 58
7.1 Personnel – Staffing 58
7.1.1 Operational Staff 58
7.1.2 Maintenance Staff 58

Draft

7.2 Training 58
7.2.1 Training Needs Assessment 59
7.2.2 Training Environment 59
7.2.3 Training Deliverables 59
8 MILESTONES 61
9 GLOSSARY 62
10 ACRONYMS & ABBREVIATIONS 70
11 CYBER ENTITIES KEY ATTRIBUTES 76
11.1 Key Attributes of Human Cyber Entities 76
11.2 Key Attributes of Non-Human Cyber Entities 77

TABLE OF FIGURES

Figure 1 – DCO Action and Decision Template 22

LIST OF TABLES

Table 1 – High Level Mandatory Requirements 11
Table 2 – Assumptions 12
Table 3 – Constraints 17
Table 4 – CD-DAR Interdependencies 19

Draft

Recommended by the Project Team:
Signature _____ Date _____ Project Director (PD)
Signature _____ Date _____ Senior Project Manager (PM)
Endorsed by Senior Review Board:
Signature _____ Date _____ Chief of Force Development
Approved by Project Sponsor:
Signature _____ Date _____ MGen A.R. Jayne Project Sponsor

Draft

1 INTRODUCTION

1.1 Background

There have been significant changes in the cyber threat landscape over the last 20 years. Today's attackers are far more sophisticated and organized and have specific goals and/or agendas. They have more resources available to them, nation states, organized crime syndicates, and terrorist groups may direct and fund them. Cyber-attackers and their sponsors are interested in illegitimately acquiring information, accounts, and data, all of which they can use for criminal, political, or military advantage against Canada and its allies.

In response, 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 assessed 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 government 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 Cyber Defence – Decision Analysis and Response (CD-DAR) Project, C.000707, will acquire defensive cyber capabilities to monitor and defend DND/CAF networks, to include the ability to detect, analyze and respond to threats. The CD-DAR capability will also provide reliable contextual analysis to support DND/CAF decisions and actions in the conduct of Defensive Cyber Operations (DCO) within designated Command Network[1] (Comd-Net) Extensions and Interfaces, and deployable Defence Wide Area Network (DWAN) systems. Consolidated Secret Network Infrastructure (CSNI) is a part of the Comd-Net within DND`CAF and a significant portion of the scope of this project will be applied to CSNI.

1.2 Business Need Statement and Outcomes

1.2.1 Business Need Statement

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 therein; and complete situation awareness, detection,

[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.

Draft

analysis, and formulation of a response to cyber threats in a timely manner across strategic, operational, tactical domains.

1.2.2 Drivers for Change

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. 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 the CD-DAR capability 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 capability, 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 solutions will combine the functionality of existing and new

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

Draft

tools, providing an integrated COP reducing the need to train every security analyst on each individual tool.

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 available to investigate these events to protect the IT network's integrity. As a result, DND is increasingly challenged to remain up-to-date on this ever-changing front. Coupled with the current out-of-date and inefficient cyber defence capabilities, DND/CAF security and defence remain vulnerable to an ever increasing cyber threat significantly elevating the risk to missions and operations.

1.2.3 Capability Gap

As further detailed in section 2.4, the capability gaps are deficiencies in or a lack of:

a. Network Discovery;
b. Integrated software cyber defence tools;
c. A trusted database repository;
d. Common Operating Picture;
e. Human Factors; and
f. Forensics.

1.2.4 Business Outcomes

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

Draft

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 (GC) and the Defence Team through the provision of innovative, scientifically advanced technologies and personnel solutions into the future.

Draft

2 HIGH LEVEL MANDATORY REQUIREMENTS (HLMRs)

Key operational Drivers of the required capability are addressed by the High Level Mandatory Requirements (HLMR). HLMRs 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 Requirements (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 (C2). 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 Statement of Operational Requirements "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 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 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 analysis 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.

Draft

#	Capability	HLMR
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.

2.1 Key Assumptions

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 (Director Information Management Engineering and Integration (DIMEI), Shared Services Canada (SSC)) to formulate a resolution.

Draft

2.2 Initial Operational Capability (IOC) (high level)

The Initial Operational Capability (IOC) will attain the HLMR capabilities in Table 1 within limited Comd-Net and deployed DWAN infrastructure. This will include the installation and configuration of supporting infrastructure at applicable sites where select personnel will also be trained on CD-DAR systems. The refinement of performance indicators, reporting systems and operational processes will also be attained by IOC.

2.3 Final Operational Capability (FOC) (high level)

The Full Operational Capability (FOC) will see the attainment of capabilities of all HLMR, outlined in Table 1, on the remainder of Comd-Net and deployed DWAN infrastructure. The networks will be identified in the SOR generated within the Definition Phase of the Project. FOC will also achieve the outcome stated in the Business Case Analysis (BCA): a Cyber Force that is equipped, trained, and prepared to effectively conduct DCO and a cyber capability that will support future development.

2.4 Capability Deficiency

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 CFNOC.

Together with stakeholders (those with vested interests in operating the networks described below primarily within DND and OGDs or agencies such as Communications Security Establishment (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 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 the Assistant Deputy Minister (Information Management (ADM(IM)), will direct the routine operation and defence of DND/CAF networks.

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

Draft

a. Cyber Defence Operation – coordinates DND/CAF DCO and incident response with organizations internal and external to the department;

b. Cyber Threats Intelligence Cell – currently operates 8/5 (with a surge capability) to provide proactive and reactive intelligence to enhance cyber defence operations;

c. Surveillance Team – conducts network traffic analysis of DND/CAF cyber domain in order to identify potentially compromised devices for further investigation;

d. 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 ITI;

e. Incident Handling Team – performs the national incident handling leadership role as part of the established framework for a coordinated enterprise approach;

f. Enterprise Intrusion Detection System Support – responsible for providing 24/7 support of the following: (i) Configuration, testing, deployment of various Intrusion Detection System (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);

g. Enterprise Vulnerability Assessment Support Team – performs vulnerability and risk management on selected networks; and

h. 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.

As briefly outlined in Section 1.2.3, the capability gaps are deficiencies in or a lack of:

a. 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

[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)

[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).

Draft

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;

b. 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:

   i. 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

   ii. 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;

c. 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 Joint Staff (SJS) 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

[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.

Draft

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;

d. 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 commander's 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;

e. 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 (GC 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:

    i. Integrated threat intelligence that looks for known bad actors by leveraging global threat intelligence,

    ii. Behavioural analytics that applies known patterns to discover malicious behaviour, and

iii. Anomaly detection using statistical profiling to build a historical baseline to provide alerts on deviations from established baselines that conform to potential attack vectors; and

f. 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.

2.5 Project Constraints

Table 3 – Constraints

#	Category	Description
1	Security Clearance	Due to the nature of the domain, this project must require personnel and industry with security clearances up to TOP SECRET Signals Intelligence (SIGINT) and with citizenship restrictions from Australia / New Zealand / United Kingdom / United States (AUS/NZ/UK/US) to CANADIAN citizens only.
2	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 SA information. To be successful, the CD-DAR capability most not require excessive training

[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.

Draft

		that fundamentally changes the skills and the available trades or occupations fulfilling those roles.

2.6 Current Situation

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 (Cyber Security Awareness (CSA) / Defensive Cyber Operations – Decision Support (DCO-DS) projects) Business Case Analysis. The DCB also agreed that the project should proceed to Programme Management Board (PMB) for the Definition Phase endorsement, following a review of project scope, scalability and timelines.

A Request for Information (RFI) was issued in December 2017 with the purpose of consulting the industry in regards to the solution feasibility, costing, and timelines. The industry submissions in response to the RFI highlighted significant advancements in technology in the last few years, and an estimated costing was provided for CSA and DCO-DS integrated capability, for the given timeframe. The last Senior Review Boarding (SRB) progress review was held in Feb 2020 with the next planned for February 2021. In June 2020, Treasury Board of Canada (TB) approved the project to enter the Definition Phase. Additionally, an RFI amendment and draft Invitation to Qualify (ITQ) were prepared and posted in July 2020. The ITQ, updated as per Industry recommendations, will be posted to BuyandSell in April 2021.

The CD-DAR project team has completed significant activities in preparation to meet the critical milestones such as detailed costing for the Definition and Implementation Phases, Technical Architecture Document (TAD), Business Transformation Plan, in addition to project documents such as Project Charter (Options Analysis (OA) Phase signoff October 2020), Project Management Plan, and Risk Management Plan etc. The project has engaged key stakeholders across DND (DIMEI, Director General Information Management Operations (DGIMO), CFNOC, Defence Services Operations Centre (DEFSOC), Defence Research and Development Centre (DRDC), etc.), GC (SSC and CSE), and allied partners to ensure that the interoperability and dependencies are well understood given the project size and complexity. Together with Director Electronic System Procurement (DES Proc) and Public Services and Procurement Canada (PSPC), the project team is also developing an overall procurement strategy and timelines, and where feasible, preparatory procurement activities in advance to meet the expected timelines of Definition and Implementation Phases.

2.7 Project Interdependencies

The interdependencies affecting the successful implementation of CD-DAR are listed in Table 4 below.

Draft

Table 4 – CD-DAR Interdependencies

Project Title	Project Number	Interdependency Description	Impact if not delivered	Risk Response	Required Date
Information Technology Infrastructure in Support of Command and Control (ITI in Sp of C2)	C.000698	The ITI in Sp of C2 will transform and enhance DND/CAF ITI in order to address identified deficiencies and to position the enterprise to address future challenges. It will enable more effective execution of C2 at all levels. ITI in Sp of C2 depends on CD-DAR to enhance the security of the integrated Secret network.	None	CD-DAR will most likely deliver in advance of ITI in Sp of C2, consequently CD-DAR will need to easily adapt to service the new environment.	TBD
Network Command and Control Integrated Situational Awareness Capability (Net C2 ISAC)	C.000375	Net C2 ISAC will provide a prioritized view of Information Technology (IT) services upon which operations depend.	CD-DAR may be required to increase scope to include Situational Awareness of the IT Services.	Early engagement with senior management and CFD to increase funding and adjust schedule through Investment Plan Change Proposal – Impact Assessment (IPCP–IA).	TBD

2.7.1 Dependencies

The CD-DAR project is forward looking and will be delivering future capabilities. Its design and deliverables will likely need some flexibility to align with current and planned functionality and capabilities delivered by other projects. Furthermore, changes mandated by various operational and technical authorities, over the lifetime of the project, as well as directives and policies unknown at the present time, may set additional dependencies for the solution.

2.7.2 Contributions

The project hopes to leverage existing and planned capabilities outside of the project's scope and being delivered by other parties, either within DND/CAF (e.g. CFINTCOM), OGDs or external security partners, with the intent of maximizing the integrated nature of the CD-DAR solution. These things include but are not limited to:

a. Threat intelligence from OGDs and trusted security partners; and

Draft

b. Additional sources of authentication, authorization, audit and related infrastructure elements.

Draft

3 SYSTEM OPERATION

3.1 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 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. These shall be integrated into a solution to provide reliable contextual analysis in order to support the decisions and Response Actions (RA) of the people of the Command Network in the conduct of DCO.

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-NET and its extensions, operations utilising these extensions will be provided the same cyber defence capability in support of their mission.

A cyber operation is the application of coordinated cyber capabilities to achieve an objective in or through cyberspace. 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. As with all military operations, operational effects are done through formalized C2 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 C2 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.

Draft

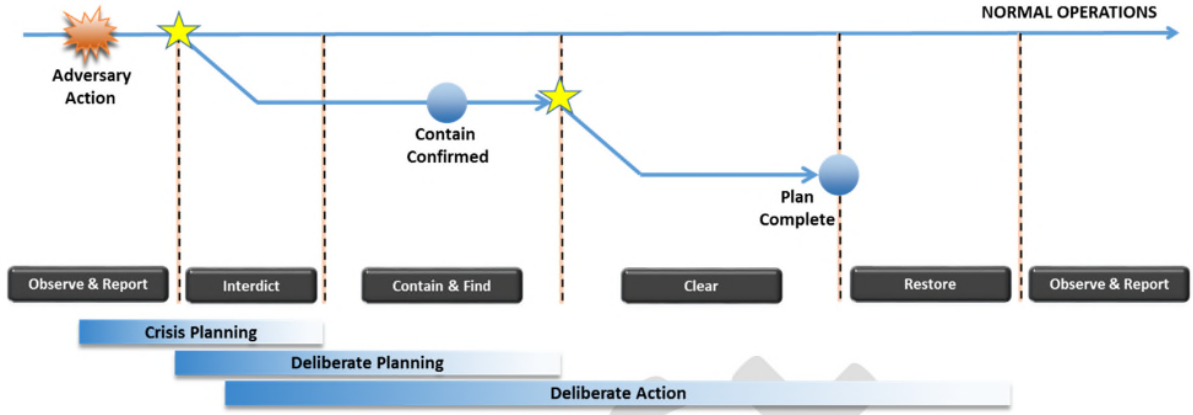


Figure 1 – DCO Action and Decision Template

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.

3.2 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.

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

Draft

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 Strong, Secure, Engaged: Canada's Defence Policy (SSE).

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 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 shall also address the need to handle information across various security domains and caveats; and

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.

3.3 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.

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

Draft

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*, 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.

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-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.

---

[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.

Draft

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.

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.

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.

3.4 Concepts of Operations

The Concept of Operations (CONOPS) defines the CAF Cyber Force's roles and responsibilities, complete with the processes and tools that will form the CD-DAR capability for the DND/CAF. It provides a description of the new capability and the conditions under which it will operate, the processes that will be used to secure and defend the DND/CAF Cyber environment and how Commanders, Executives, Staff and Cyber Operators will interact with CD-DAR.

The CONOPS focuses on the Force Employment (FE)[10] of the CD-DAR defensive cyber capabilities to monitor and defend DND/CAF networks, to include the ability to detect, analyze, and respond to threats. The CD-DAR capability will also provide reliable contextual analysis to support DND/CAF decisions and actions in the conduct of DCO within designated Comd-Net Extensions and Interfaces, and deployable DWAN (Designated network – Protected B and below) systems. The CSNI (Classified network – Secret), part of Comd-Net within DND/CAF, is a significant portion of the scope of CD-DAR will be applied to CSNI.

[10] At the operational level, Force Employment refers to the command, control and sustainment of allocated forces, Defence Terminology Bank (DTB), Record #32173.

Draft

Refer to the CD-DAR CONOPS for further detail.

3.5 Concept of Support

The Concept of Support (CONSUP) defines a proposed framework to manage CD-DAR as a capability. It delineates the management framework to provide an integrated approach to CD-DAR capability definition, development, institutionalization, maintenance, and evolution. Such a Capability Management Framework (CMF) will provide clarity in responsibility, accountability and process for the capability acquisition and support life-cycle from concept development to capability procurement and implementation, release, in-service support and disposal.

Refer to the CD-DAR CONSUP for further detail.

3.6 Key Roles

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 Joint Task Force (JTF) or Command 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 CDS [3]. Assuming no significant organizational and IT governance changes in the foreseeable future, Director of Staff Strategic Joint Staff (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 their area of responsibility.[11] Assuming no significant 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

[11] 2700-1 (SJS J6), 10 November 2017

Draft

changes in the foreseeable future, ADM(IM)/Director Information Management Security (D IM Secur) 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; and

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.

3.7 Key Tasks[12]

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, SA, RAs, 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 Royal Canadian Navy (RCN), Royal Canadian Air Force (RCAF), Canadian Army (CA), Canadian Joint Operations Command (CJOC), Canadian Special Operations Forces Command (CANSOFCOM), and SJS. Cyber SA may be pushed through the Joint Battlespace Management Capability (JBMC) and integrated with SA from other operational domains, i.e., air, maritime, land, space, and special operations forces.

CD-DAR supports a number of the cyber operations tasks and functions that were defined in the cyber operations Joint Doctrine Note 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.

3.7.1 Preparing for Defensive Cyber Operations (DCO)

Four key questions need to be answered in setting up a cyber-defence operation:

[12] Extracted from Defensive Cyber Operations Concept Version 1.0 October 14 2018

Draft

a. What is it that we are trying to protect?

b. What are the possible threats against what we are trying to protect?

c. How do we try and detect those threats?

d. How do we respond when we detect a threat manifestation?

Defensive Cyber Operations start with what you are planning to defend. Clearly a Secret level network infrastructure contains secret data, so that's a starting point. Not being able to get at accurate and truthful data that you need, in a timely fashion, carries the same potential impact of not having that data in the first place.

There are many tools that will help creating and managing the existing hardware and software assets an organization has, so the right collection of technology, people and process can be assembled from available Commercial off the Shelf (COTS) and Government off the Shelf (GOTS). However, very few vendors have an understanding of your business and the data you use to conduct operations, so there are very few tools which you can procure to help with this activity. Nevertheless, consider creating and maintain a data asset inventory at the time you are preparing your Security Information and Event Management (SIEM) and related tools to manage your software and hardware assets. Identifying the information you are trying to protect and the infrastructure you use to access it, is the foundation of any DCO. It should tell you what you are trying to protect.

Understanding what you are trying to protect helps to circle the wagons, understanding what's outside of that circle is crucial for your defence, so it is just as important to build and maintain an inventory of your threats and Tactics, Techniques and Procedures (TTPs) used by your adversaries in order to prepare your defence.

Understanding and knowledge come from one primary thing – relationships. Maintaining an inventory of "everything" is helpful but it becomes really useful for SA when you can create, persist and evolve linkages between entities (people, places, things, and events) over long periods of time to build knowledge and understanding, leading to awareness. Without awareness you lack the ability to detect normal and abnormal behaviours and the incursion of an adversary. You must ensure any solution is capable of building knowledge through relationship, and link creation and exploitation.

Direct detection of malicious elements, through known signatures, sources, profiles and behaviours, through Anti-Virus (AV), Anti-Spam (AS), Intrusion Prevention System (IPS) / IDS and other malware detection products is an intrinsic capability of all DCOs, but it is necessary to expand these detection capabilities to match the sophistication of current adversaries and attacks. Detection of the abnormal and sophisticated only comes from the breadth and depth of the accumulated knowledge mentioned above. Detection of threats will be based on the

Draft

traditional direct mechanism but more importantly on your development of rules and analytics that contribute to the heuristic behaviours of your detection tools.

3.7.1.1 Establish External Terrain Advantage (ETA)

If you consider the cyber domain as a landscape, external terrain advantage comes with an understanding of your adversaries and their behaviours for which you must mount a defence. While the adversaries are many and trying to maintain an effective and current knowledge of them, in order to gain the advantage, it's important to remember that there are many opposing forces to them in the form of the many organizations whose job it is to mount cyber-defences.

It's clear that the only way to gain the advantage is through interoperability and information sharing, with trusted security partners and integration of trusted security information sources in order to establish the required defensive knowledge necessary to conduct DCO.

3.7.1.2 Establish Internal Terrain Advantage (ITA)

Similarly to the above, establishing an advantage over your adversary, for your internal cyber domain/landscape, would mean you have a comprehensive understanding of all of your internal assets (hardware, software, network, etc.) and what is going on in your IT infrastructure such that your adversary cannot establish a foothold on your internal infrastructure. As the ultimate aim of DCO this, of course, is a very challenging goal, often determined with a series of metrics such as:

a. Mean-Time-To-Detect (MTTD);
b. Mean-Time-To-Identify (MTTI);
c. Mean-Time-To-Contain (MTTC);
d. Mean-Time-To-Respond/Resolve (MTTR);
e. Number of systems with known vulnerabilities;
f. Number of Secure Sockets Layer (SSL) certificates configured incorrectly;
g. Volume of data transferred on the network; and
h. Number of user's with "super user" access.

The above provides a small sample of many metrics used to capture how well an organization understands their internal cyber domain.

3.7.1.3 Adversary-focused Monitoring Strategy

The defence of a network requires a deliberate Adversary-focused Monitoring Strategy (AMS) to ensure that the network defender can predict, prepare for, and see adversary activities.

A completed AMS should allow direct connections to be made between threats, engineering efforts, and the actions of the DCO operator, therefore ensuring operations are effective and

Draft

efficient. A deliberate monitoring strategy allows the defender to understand how the adversary is likely to attack (based on a Return-on-investment (ROI) analysis), how to monitor for attacks, and how attacks can be deterred. An AMS provides answers to these questions:

a. Who are the threat actors that we are likely to face and what do they wish to achieve in terms of outcomes/effects and why?

b. What are the tactics that, given the architecture of the network (how will they be used, and where are they located), are most likely to be used to achieve adversary outcomes?

c. What are the technical capabilities that are available, or that can be made available within the specific network to support monitoring?

d. How can the technical capabilities be combined to meet the needs of the defensive and security community – maximizing defensive utility and minimizing adversary freedom of action and ROI.

3.7.1.4 Validation and Testing

The validation and testing function is a continuous effort designed to ensure the efficacy and efficiency of the technical plans, safeguards, and coordination mechanisms for DCO, and is made up of two activities:

a. Testing the design of all operational capabilities; and

b. Validating the effectiveness of implementations over time.

Validation and testing should be executed by the engineering community as a part of their responsibilities to engineer, integrate, and maintain supporting DCO ecosystems. This promotes closer working relationships between the engineering community and the operational community.

3.7.2 DCO Preparation Operations

DCO preparation operations are technically a component of Preparation for DCO as they set conditions for success for DCO execution. They act as the mechanism for ensuring the effective application and integration of preparation activities with DCO Execution activities. DCO preparation operations are also needed to ensure that information generated from DCO Execution informs and re-orients *Preparation to DCO* and Support to DCO. Specific activities include:

a. Setting specific conditions to ensure success of a DCO mission and that it can be responsive to any mission or operational requirements;

b. Conducting resource intensive activities to make changes required to understand new threats and ‘make it normal’. (see text box); and

Draft

c. Set the conditions to ensure a DCO mission can support an operational, security, or intelligence task.

3.7.3 DCO Execution

The subsections below briefly outline activities designated as being part of DCO execution.

3.7.3.1 Monitoring

The monitoring function is the act of watching for events of concern and flagging these events for either Respond – Understand or Respond – Neutralize. Events can be generated by signatures, behaviour pattern analysis, third party notification, or alerting from defined triggers from AMS. MITRE, SysAdmin, Audit, Network and Security (SANS), and the National Institute of Standards and Technology (NIST) institutions are some examples of monitoring strategies used by the DCO.

3.7.3.2 Response Activities

At the point where an event has occurred, the options available to the attacker have already been assessed as a part of the ITA and ETA functions, and the monitoring plan has been developed within the AMS function, ensuring that the system is instrumented to monitor activities that the adversary would want to take.

There are three basic types of response options: *Respond – Understand, Respond – Neutralized*, and *Respond – Deceive*. All events will eventually be neutralized, the key question is how much understanding and deception activities are required before that occurs, while it is occurring, or afterwards. Knowledge gained is recorded and used for future DCO.

3.7.3.2.1 Cyber Event Triage

A cyber event triage process is to determine if an event requires a DCO response. It examines whether the event could support adversary outcomes or be an identifiable part of adversary activities. Events that show potential association with adversary outcomes should be designated as a DCO event. Knowledge gained is recorded and used for future DCO.

3.7.3.2.2 Respond – Understand

Once a DCO event is detected, analysis of the event is performed to determine what action is required. Decisions are made based off of a technical analysis to understand the mechanics of the attack, intelligence analysis, and situation analysis.

The two most important DCO tasks are:

a. To understand what the adversary has technically done on the system; and

b. What the adversary is trying to achieve.

In some cases, the activities required to understand a DCO event could include intelligence operations for collection or counter-intelligence.

Draft

3.7.3.2.3 Respond – Neutralize

The goal of *Respond – Neutralize* is to disable or render inoperable the technical cyber tools of the adversary and can be performed at any stage in the response process. The neutralize threat activities should be implemented by in-service support (ISS) and engineering with guidance from DCO with authority from the responsible commander. Any immediate threat defence that is scripted and pre-approved can be neutralized by the DCO operator directly.

3.7.3.2.4 Response Doctrine

DCO's technical response activities is similar to the industry "detect, understand, respond, and restore" methodology with a few additional components (see DCO concept for detail). Adopting industry doctrine and best practices allow for effective and efficient operations by enabling the use of third party advisors, commercial support, commercial core training, and improving overall sustainability of the capability.

3.7.3.3 Deception Activities

A deception operation within the cyber environment is not inherently different from a real-world deception operation. Efforts are made to misinform, confuse, distract, and delay an adversary. It is also possible to gain intelligence about an adversary based on how they interact with a deliberate deception, which can be immensely useful in the case where a capable adversary is lured into disclosing tools or tactics that have not been previously observed. Actions can also be analyzed to discern the real-world intent and target of that adversary.

Deception activities include proactive deliberate activities and *Respond-Deceive* actions that occur in response to a particular event.

Types of deception operations can include:

a. The implementation of honeypots, including modern machine learning assisted environments that aim to capture and maintain the attention of an attacker;

b. The monitoring of deliberately unused sets of IP space to catch internal network reconnaissance and lateral movement attempts;

c. The introduction of endpoint processes, agents, or user accounts that act as tripwires; and

d. The publishing of external information that includes information that can be used as a tripwire or as an indicator reconnaissance.

Deception activities often result in the exposure of sensitive adversary tools, tactics, and tradecraft as they are forced to interact with devices and software that specifically attempts to understand their activities.

Draft

3.7.3.4 Defensive External Interdiction

Defensive External Interdiction (DEI) is a category of action that can be requested by the DND/CAF of a commercial or foreign state third party where that third party takes an action that has defensive value for the DND/CAF. Actions taken by a third-party leverage that third-party's position within the global telecommunications environment or their national authorities that have the legal ability to block, alter, slow, or redirect elements of malicious communications destined for the DND/CAF.

3.7.4 DCO Support Functions

The long-term viability and effectiveness of the DCO function requires that specific support functions be designed and implemented alongside the core DCO functions. Core DCO support functions include:

a. Innovation and Advantage;

b. DCO Engineering; and

c. Network Operations (NetOps) / Maintenance.

The subsections below briefly outline activities designated as being part of DCO support functions.

3.7.4.1 Innovation and Advantage

The DCO function must be maintained in a state where it possesses advantages over adversaries.

The delivery of an advantage has the following stages[13]:

a. Identify potential advantages;

b. Understand the technology;

c. Validate the context and value of the advantage; and

d. Deliver the advantage where and when it is needed.

Having these advantages generates a deterrence effect on potential adversaries and supports a range of departmental activities beyond DCO including mission assurance, security operations, and IT security.

Innovation and advantage is much more than a traditional Research and Development (R&D) project, principally because of the range of information it considers, and because the activity ends in the delivery of a concrete tool. In order to achieve this, the innovation and advantage function is responsible for the following outputs:

[13] Details of each stage can be found in the Defensive Cyber Operations Concept Version 1.0 October 14 2018

Draft

a. Setting the direction of R&D initiatives;

b. Setting direction and requirements for horizon 0, 1, and 2 minor and major capital projects supporting DCO;

c. Directing process improvements and promoting culture change within DCO and its supporting functions; and

d. Set requirements for CAF cyber exercises or any that CAF DCO resources participate in.

This leads to keeping close to current generation technologies and providing an advantage to adversaries.

3.7.4.2 DCO Engineering

DCO capabilities require dedicated and continuous engineering efforts. Those efforts traditionally begin once the future technology or new requirement is identified and progresses through stages including prototyping, requirements development, design work, procurement, and fielding.

The adoption of the new DCO concept requires a significant increased role for the security engineering community as the DND/CAF looks to create technical advantages, form external and internal terrain, defeat highly capable adversaries, execute DCO business functions leveraging knowledge and action management systems, and develop effective solutions to defend deployed networks and missions systems for the warfighter. The systems that the DCO operator will use to defend all DND/CAF systems have to be built, configured, and adapted to meet new requirements.

When done well, engineering is the central enabler to the efficient and effective employment of DCO in domestic, deployed, and mission systems. Its importance cannot be overstated.

The engineering function for this concept includes these specific roles:

a. The development of integrated solutions: An integrated solution in this context refers to platform integration, architectural integration, and the integration across varying technical environments;

b. Engineering DCO technical measures and DCO response measures: Set of capabilities, referred to as DCO technical measures that require design, engineering, and testing. Temporary capabilities to defend, mitigate, remediate, or deter an attack, referred to as DCO response measures, must be designed and tested;

c. Integration (or labelling) of DCO capabilities within the Cyber Security Reference Architecture (CSRA): As DCO capabilities are identified they need to be either

Draft

labelled as being a DCO capability or entered and accounted for as a new component of the architecture;

d. Pre-positioned procurement: The engineering function will implement a system of pre-positioned procurement that will enable projects and missions to adopt current best of breed technologies rapidly. To achieve this, the engineering function will proactively obtain and maintain contracting vehicles and inventories to support rapid deployments, as required by SSE. This strategy provides operational flexibility and the opportunity to ensure that mission systems are not sent into contested cyber environments without required capabilities. This activity is a direct mission enabler, the absence of which would cause direct an incontrovertible mission risk; and

e. Providing technical support for all phases of DCO: Expert advice on capabilities and what they can provide is required. This advice is critical for managing incidents, understanding the true technical context of a threat, and developing nuanced approaches to threats and risks.

3.7.4.3 Network Operations / Maintenance

The execution of DCO requires that resources have the ability to focus on what is most important to the DCO function. The focus on adversary outcomes allows a delineation between countering an outcome and conducting NetOps. Although delineated, they should not be considered to be separate or unrelated as they are, in very realistic terms, highly interdependent and complementary.

The following lists some interdependencies between NetOps activities and DCO:

a. DCO and NetOps require access to mostly the same toolsets;

b. Data gathered by NetOps needs to account for requirements from the DCO function, and vice versa;

c. Processes used by NetOps needs to account for requirements from the DCO function and vice versa; and

d. Taking action to identify, understand, or respond to an incident or threat are a subset of actions that are taken to manage a network. The operational mechanisms, processes, auditing mechanisms, and tracking capabilities of NetOps are direct enablers for DCO.

Although interdependent, the execution of both sets of activities should be kept distinct where possible.

Draft

3.7.5 Knowledge and Action Management Systems

The development of a competent and maintainable DCO capability requires that the entirety of the function become data, information, and knowledge driven. While not in a mature state, the drive to create a system to fulfill these requirements is still in process. As a result, the complete definition of what is needed for knowledge and action management systems for DCO will take effort to define, but some high-level characteristics include, but not limited to:

a. An intelligence analysis suite and intelligence knowledge repository;

b. An integrated monitoring suite (SIEM, Endpoint Detection and Response (EDR), etc.);

c. Automated and event driven operational risk management tools;

d. Automation of Security Risk management, compliance, and vulnerability management;

e. A cyber capability inventory that includes planning features for planning and executing DCO;

f. An enterprise incident management capability that provides an incorporated knowledge base to assist the resolution or neutralization of events; and

g. A link to or implementation of NetOps management tools.

3.8 User Characteristics

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, RAs, 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. As required Cyber domain SA is pushed to the DND/CAF JBMC for integration to SA of other operational aspects of CAF missions and operations.

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

3.8.1 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

Draft

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 RAs; and

e. TTPs 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

Draft

viii. Cyber Operations Centre functions.

Draft

4 DESIGN AND CONCEPT GUIDANCE

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

4.1 Included Work and Services

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

a. The ability to maintain SA, through a COP, of alerts, threats, and remediation across the DND/CAF Command Network, and to feed SA 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.

   As described in Section 2.4, the COP is malleable and attuned to each commanders needs whether Strategic, Operational or Tactical. It provides leeway in the operational views to consolidate information for commanders. It also operates on networks that are unavailable, unreliable, providing local cyber environment SA, or that have limited capacity (episodic) environments;

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 or on demand discovery of cyber entities and events 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 to rapidly identify the presence of non-compliant cyber entities or behaviours, events, alerts, vulnerabilities, or other changes to the status of the entities within the DND/CAF cyberspace;

e. An ability to perform 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;

Draft

f. An ability 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;

g. An ability to perform automated task management to adaptively and dynamically identify, contain and eradicate a threat; and

h. An ability to utilize an integrated operational training system 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:

   i. Operational Threat, Penetration and Attack simulation capability to exercise the Cyber Operator team and evaluate its operational readiness and effectiveness,

   ii. An individual operator training component focussed on individual operators (task, roles and advancement in role),

   iii. Skills training and validation for Cyber Operators and non-Cyber Operators, and civilians, in their assigned roles, individually and collectively, and

   iv. A collective training component for the defensive cyber security operations capability. It is a replication of the set of operation systems with offline datasets allowing complete range of functionalities and running realistic scenarios for training purposes.

4.1.1 Cyber Domain Data Sources

At present, Threat Intelligence is being shared with approximately 15 internal (e.g., CFINTCOM, CJOC, ECS') and external organizations and organizational units (e.g., CSE, CCCS, FVEYs, NATO partners) presumably in a range of formats and levels of automation. It is a critical form of information to internal and shared cyber security and defence that warrants further attention.

4.1.2 Deployed Capabilities

A key driver of the CD-DAR Project is to defend freedom of action[14] for operational commanders. CD-DAR will provide theatre commanders the capability to access the Cyber Domain for operations through cyberspace; will have trustworthiness on information transmitted/shared within DND/CAF cyberspace; will have the capability to access intermittent and low bandwidth situations, and will be able to take advantage of deployable detection and response capabilities as they become available. This is especially crucial for deployment and local capability to leverage automated security and defensive measures as they become available.

[14] **Freedom of Action** is the ability to employ forces with little to no constraints, so being able to operate within the cyber environment with confidence that the environment will be available and can be trusted when needed.

Draft

4.1.2.1 Canadian Surface Combatant

The Canadian Surface Combatant if the RCN platform scheduled to replace the Halifax Class frigates. As the Canadian Surface Combatant may be tasked to act as a Joint Task Force Headquarters at sea, the Canadian Surface Combatant will need the ability to conduct DCO of their respective network environments. Therefore, CD-DAR Project is mandated to fit Canadian Surface Combatant with a similar capabilities as any other land-based JTF Headquarters (HQ).

4.2 Excluded Work and Services

The CD-DAR project will not evaluate and/or recommend point products, including security products, except insofar as they contribute to improving the overall security posture of the mandated domains it targets. For example, product features that don't contribute to cybersecurity are of little interest, unless they contribute to integration and/or interoperability and improving the cybersecurity posture. Features, that of course degrade the cybersecurity posture of the target domains, are of great interest during evaluation and testing, but again, the context will always be in consideration of the overall security posture. For example, the capability of an antivirus package to integrate into a SIEM and/or Cyber COP is of greater interest than whether its Graphical User Interface (GUI) is end-user friendly. (It's expected that some other group is evaluating and selecting individual products based on features and capabilities other than those related to CD-DAR's capability vision.)

4.3 Use of Technology

It is expected that the CD-DAR solution will be an amalgam of technologies that when integrated into a final solution will meet the project's aspiration for flexibility, adaptability, longevity and effectiveness in delivering DCO. Some of the key technologies include:

a. Security Information and Event Management (SIEM) software tools – The cornerstone of DCO is knowing your cyber landscape. What is it made of? How is it used? What constitutes "normal" behaviour? When something changes? And did we expect the change? When do we expect things to happen? What are the risks, threats and adversaries we may encounter? How do we expect them to behave?

   As human beings, we are asking and answering ourselves these questions constantly every day, to be aware of the things around us. SIEM tools do that for our ITI; and there are a plethora of these tools available. We will need some. We will have to integrate, understand and control/direct them, for us to provide effective DCO. We need to be able to paint our [cyber] landscape down to the finest brush stroke, so we are able to see what's wrong with the picture as soon as it happens.

b. Big Data / Data Lake platforms – There's no question that SIEM tools (above) generate a flood of data that quickly overwhelm, and yield useless, traditional approaches to data storage. On top of that, the analysis, augmentation and convolution we'll do turning that data into useful information will double, triple or

possibly blow that quantity up even higher, not to mention how much of that data we need to retain and for how long. Big data and data lake technologies will have to be incorporated just to survive an initial implementation.

Data lakes or more properly referred to as ***data reservoirs***, (since everything about them needs to be controlled to prevent being overwhelmed, either flooding us out or turning them into data "swamps",) need to designed/architected and supported to ensure every piece of data is accessible, useable and governed to deliver value the solution and the organization as a whole.

c. Artificial Intelligence / Machine Learning (AI/ML) – Artificial Intelligence (AI) and Machine Learning (ML), two distinct concepts although often taken together, offer a number of advantages to DCO. AI is about observing and understanding the environment in a humanistic fashion, and being able to respond in a similar context. ML is about taking that understanding to build and retain knowledge, which can subsequently be employed to take action. Taken together in the cybersecurity context they can be used to detect and automate, semi-automate or trigger a response to a [cyber] threat or incident, with a similarly automated, semi-automated or manual [workflow] response that will mitigate or vanquish the malicious action. Use of this technology is a significant part of the CD-DAR Project's innovation and future looking capability.

d. Behavioural Pattern Analysis – Behavioural pattern analysis is something that is generally an output or function of AI/ML. Determining and remembering what is "normal" (or being told what is normal,) behaviour is how the abnormal behaviour of adversaries is detected. It assists monitoring activities through automating some observation of events in the cyber domain to find possible threats and/or activities that should be investigated and confirmed as "normal" or "abnormal" and if the latter, it provides the mechanism to raise an alert. It can be very effective if it is appropriately taught what to look for.

e. Cloud Computing [Platforms] – Cloud computing platforms have demonstrated their effectiveness, for some workloads, in delivering simpler, more responsive and scalable infrastructure resources as a component of ITI. The CD-DAR project will seek to engage this technology in two ways.

First, as the Department seeks to utilize cloud computing technology as an element of its ITI, the solution must ascertain the implications of using this technology from a cybersecurity perspective, and ensure the solution remains vigilant with regard to could technology use, its risks, vulnerabilities and integrity in the cybersecurity context.

Draft

Second, the CD-DAR solution may take advantage of cloud computing technologies in delivering its solution to benefit from its approach to resource allocation, self-healing aspects and its ability to scale as needed, without significant effort required by IT service technicians and administrators.

4.4 Design Concept

The CD-DAR Project, 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 Comd-Net Extensions and Interfaces, and deployable DWAN systems in the conduct of DCO.

The solution will include DCO capabilities that include, but are not limited to:

a. **Unauthorized Hardware Detection**: Prevent and correct unauthorized operation of hardware on DND/CAF's ITI largely by implementing Centre for Internet Security (CIS) critical security control (CSC) – 1. CD-DAR will deliver an automated means of identifying all IT devices connected to the network, their location (logical and physical), and their configuration;

b. **Unauthorized Software Detection**: Prevent and correct unauthorized operation of software on DND/CAF's ITI largely by implementing CIS CSC – 2. CD-DAR will deliver an automated means of identifying all software installed on the network, their location (logical and physical), and their configuration.

   Regarding entities (i.e., hardware and software) installed on the network, the capability will specifically:

   i. Standardize entity names,

   ii. Automatically identify all entities and their configurations (authorized and non-authorized),

   iii. Topologically provide a visual network map of all entities,

   iv. Automatically track all entities connected to the network (authorized and non-authorized),

   v. Maintain a secure database of authorized entities,

   vi. Automatically validate authorized entity identity, and

   vii. Automatically respond to the discovery of unauthorized entities;

c. **Unauthorized Administrative Privileges**: Prevent and correct unauthorized, usually excessive, hardware and software administrative privileges on DND/CAF's ITI largely

Draft

by implementing CIS CSC – 5. CD-DAR will deliver a capability to assure proper use of administrative accounts.

This capability will specifically:

i. Standardize entity names,

ii. Automatically identify all entities and their configurations (authorized and non-authorized),

iii. Track administrative accounts,

iv. Maintain a secure database of authorized entities,

v. Evaluate administrative accounts to ensure compliance and cyber defence, and

vi. Automatically respond to the discovery of unauthorized entities;

d. **Misconfigurations**: Prevent and correct unauthorized configurations on DND/CAF's ITI largely by implementing CIS CSC – 3. CD-DAR will deliver an automated means of analyzing compliance with authorized configurations.

Specifically, configuration compliance will:

i. Standardize entity names,

ii. Automatically identify all entities and their configurations (authorized and non-authorized),

iii. Automatically track all entities connected to the network (authorized and non-authorized),

iv. Automatically trigger, log, alert and report configuration compliance information, and

v. Automatically assess compliance with baseline configurations taking into account likelihood of compromise, and identification of critical entities to support prioritization;

e. **Known Vulnerabilities**: Prevent and correct known vulnerabilities on DND/CAF's ITI largely by implementing CIS CSC – 4. CD-DAR will deliver an automated means of analysing the vulnerabilities in existing configurations.

Specifically vulnerability compliance will:

i. Standardize entity names,

Draft

ii. Automatically identify all entities and their configurations (authorized and non-authorized),

iii. Automatically track all entities connected to the network (authorized and non-authorized),

iv. Automatically trigger, log, alert and report known vulnerabilities,

v. Automatically assess the impact of known vulnerabilities taking into account DND cyberspace entity type from a system or service perspective, the entire kill chain, likelihood of compromise, and identification of critical entities to support prioritization, and

vi. Automatically identify, acquire, install and verify patches for all products and systems including operating systems, applications, switches, routers and devices;

f. **File Security**: Prevent and correct incorrect file labels for selected types of data files, assure enforcement of chain of custody in data files and enforce specific information policies on DND/CAF's ITI. CD-DAR will automatically produce and enforce data labelling to support document control policies related to cross-domain file transfers.

Specifically, cross domain file transferring functionality will:

i. Monitor and Detect associated network traffic events,

ii. Monitor and Detect associated user events,

iii. Automate data labelling of files, and

iv. Enforce data labelling of files; and

g. **Anomalous Activities:** Monitor and correct adversarial activities to infiltrate DND/CAF's ITI, subvert its appropriate use and exfiltrate data from it. CD-DAR will provide an EDR capability.

Specifically endpoint defence will:

i. Gather and relate:

1) New datasets and metadata as required,

2) 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 Central Processing Unit (CPU) and memory usage, and user account in use),

Draft

3) Forensics data (historical) about endpoint devices (such as processes ran, files accessed and created, applications/commands/scripts used, user accounts used, and applications installed),

4) Remotely gather memory images or files for forensics investigation,

5) Hard drive images (server, workstation or mobile) for forensics investigation,

6) Full Packet data,

7) Raw network traffic data for out-of-band collection,

8) Data to support forensic analysis,

9) Entity inventory data,

10) Configuration Management Data,

11) Accredited User Data,

12) Accredited Administrator Identity Data,

13) Vulnerability Data,

14) Threat Intelligence Data, and

15) Open Source Intelligence (OSINT) for multi-source and multi-caveat analysis (OS16),

ii. Automatically monitor, trigger, log, alert and report events:

1) Ingest and Correlate IDS and SIEM data,

2) Cyber entity events,

3) Network traffic events across domains / caveats, and

4) User events,

iii. Support investigations and analysis:

1) Perform retrospective analysis with correlation of historic events, trends and behaviours to real-time events; reconstruct activities based on context/metadata; and support hunting for Advanced Persistent Threats (APTs), insider threats, and indicators via tailored analysis of short-term historical data,

2) Meet GC requirements for digital chain of custody, and

3) Ingest and correlate Security Assessment and Authorization data, and

Draft

iv. Enable responses:

    1) For pre-authorized situations, automatically execute with the ability to manually override, log and report technical responses, and

    2) Identify, define, automate, log and report workflows responding to incidents.

4.5 Security Assessment and Authorization

A complete Security Assessment and Authorization, in accordance with the Security Assessment and Authorization Guideline (SAAG), will be conducted, resulting in the promulgation of appropriate direction regarding the implementation of the hardware, software, personnel, and procedures necessary to meet the capability security requirements.

Draft

5 SYSTEM EFFECTIVENESS REQUIREMENTS

This section defines the system effectiveness requirements for the CD-DAR project. These requirements describe and detail the capability needed for the CAF and should be used in parallel to the CD-DAR CONOPS.

The system effectiveness requirements have been captured in the Requirements table in Section 9 of this document, and complemented by the Performance Requirements presented in Section 6.

The sole basis of measurement of success of the resultant project deliverables will be based on meeting the requirements of IOC and FOC, outlined in Section 2.2 and Section 2.3 respectively, in conjunction with the Requirements Table presented in Section 9.

5.1 General Requirements

Common requirements for the CD-DAR project have been identified in Section 9.1 of the Requirements Table.

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

5.1.1 Essential

An essential 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 essential criteria and all desirable criteria, but fails to meet one essential criterion, that solution will be rejected. Within this document, the word "must" or "shall" are to be considered synonymous with essential.

5.1.2 Desirable

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

5.1.3 Caveat on Levels of Measurement

The stipulation of an essential criterion presumes that it is achievable at reasonable cost. However, should any essential 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 PD in consultation with the PM.

5.2 Operability

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

Draft

are accessible. These include Enduring Environment, Episodic Environments, Collaborative Environments, and Cyber Environments that have been outlined in Section 3.2.

Operability requirements have been identified through the Requirements Table in Section 9. These requirements highlight the needs for the project across the Discover, Analyze, Respond and Evolve phases of cyber defence (refer to the CD-DAR Analysis Framework at Figure 2).

5.3 Survivability

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 shall be supported and maintained in accordance with the project CONSUP.

The System architecture shall 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.

The capability shall be effective in all operating environments, as identified in Section 3.2 of this SOR, as the CD-DAR solution will be integrated into the host network as an internal capability. The System shall, to the greatest extent possible, be designed to survive the threats identified in Section 3.3 of this SOR, through the use of adaptive technology and analytics incorporated into the CD-DAR solution.

Survivability requirements have been identified through the Requirements Table in Section 9. These requirements highlight the needs for the project across the Discover, Analyze, Respond and Evolve phases of cyber defence.

5.4 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 shall be supported and maintained in accordance with the project CONSUP.

The system shall be repaired and operating as determined through the Security Categorization (formerly Statement of Sensitivity) and the Security Assessment and Authorization (SA&A) process.

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

The System architecture shall 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, as required for planned system maintenance and upgrades, must be relatively infrequent, of short duration and with no impact to the DND/CAF ITI. In order to maintain operational tempo, the system must be able to be restored to its minimal operational

Draft

configuration (to be defined at a later time) rapidly. Therefore, every reasonable 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 shall meet the maintainability requirements for this hardware. In addition, any developmental software shall 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 shall apply industry best practices and guidelines to ensure that the capability's software and system are scalable, extensible and modifiable, while remaining interoperable with OGDs and allied partners.

Maintainability requirements have been identified through the Requirements Table in Section 9. These requirements highlight the needs for the project across the Discover, Analyze, Respond and Evolve phases of cyber defence.

5.5 Availability

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 shall be supported and maintained in accordance with the project CONSUP.

In order to maintain operational tempo, the system must be able to be restored to its minimal operational configuration 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 short duration and relatively infrequent.

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

Availability requirements have been identified through the Requirements Table in Section 9. These requirements highlight the needs for the project across the Discover, Analyze, Respond and Evolve phases of cyber defence.

5.6 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.

Draft

Reliability requirements have been identified through the Requirements Table in Section 9. These requirements highlight the needs for the project across the Discover, Analyze, Respond and Evolve phases of cyber defence.

5.7 Environmental Sustainability

The CD-DAR solution shall meet the DND standards for environmental stewardship. The DND/CAF adopted the following code of environmental stewardship. The DND/CAF shall:

a. Integrate environmental concerns with other relevant concerns including those from operations, finance, safety, health and economic development in decision-making;

b. Meet or exceed the letter and spirit of all federal laws;

c. Improve the level of environmental awareness throughout the DND/CAF through environmental awareness training, and encourage and recognize the actions of personnel leading to positive impacts on the environment;

d. 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 Defence Administrative Orders and Directives (DAOD) 4003-1, *Hazardous Materials Management*);

e. Ensure that environmental considerations are integrated into procurement policies and practices;

f. 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

g. Acquire, manage and dispose of lands in a manner that is environmentally sound, including the protection of ecologically significant areas.

Environmental sustainability requirements have been identified through the Requirements Table in Section 9. These requirements highlight the needs for the project across the Discover, Analyze, Respond and Evolve phases of cyber defence.

5.8 Gender-Based Analysis Plus (GBA+)

To be written once the GBA+ analysis has been completed for the project.

Draft

5.9 Safety and Health

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

Safety and Health requirements have been identified through the Requirements Table in Section 9. These requirements highlight the needs for the project across the Discover, Analyze, Respond and Evolve phases of cyber defence.

5.10 Delivery Requirements

The quantity of devices required to fulfill the CD-DAR project requirements is a component of the Prime System Integrator's (PSI) architecture design and deliverables and is not able to be specified at this time.

PSIs are encouraged to utilize indigenous businesses as part of the GC commitment to foster economic development within Canada's indigenous communities.

5.11 Sub-System Effectiveness Requirements

N/A. Any sub-system components for the CD-DAR project are required to meet the main project requirements for the above sections.

Draft

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; and

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

6.1 System Level Measures

Performance Objective ID	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 IPS	TBD
PO.3	SIEM Audit Entry and Console Display	Generate an audit entry and send it to a 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 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

Draft

Performance Objective ID	Performance Indicator	Description	Qty
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
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 RAs	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 system administrator, 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 of Sensors	Develop, download, test and deploy IDS signatures to a fleet of sensors	TBD

Draft

Performance Objective ID	Performance Indicator	Description	Qty
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
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 of the 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

Draft

Performance Objective ID	Performance Indicator	Description	Qty
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 Life-cycle 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 TTPs	TBD
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

Draft

Performance Objective ID	Performance Indicator	Description	Qty
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 Cyber security and DCO capabilities, even when portions of the cyberspace are compromised or contested.	True
PO.40	Document Disclosure Protection	Protect from disclosure of sensitive documents and records maintained by the defensive cyber security operations capability.	True

6.2 Sub-System Level Measures

Refer to Section 9 requirements table.

Draft

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 3.6 above.

The solution shall 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

It is expected 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 shall provide Incremental project-related content training, based on a train the trainer approach, integrated to the existing DND/CAF DCO training program.

The solution shall 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.

Draft

7.2.1 Training Needs Assessment

A complete Professional Development Needs Assessment (PDNA) will be conducted, defining directions on occupational specialty, preferred qualifications Military Occupation (MOC), training duration, preferred ranks, and career profiles.

7.2.2 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 shall provide an integrated operational training system 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 include:

a. Operational Threat, Penetration and Attack simulation capability to exercise the Cyber Operator team and evaluate its operational readiness and effectiveness;

b. An 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 shall provide a training simulation capability to support collective operational training in a customizable operational context. The simulation capability training scenarios shall be created, maintained, edited and executed by Cyber Operators using existing workstations and systems within an exercise/training environment. The solution shall capture best practices and implement knowledge-based learning from previous operations and actions.

7.2.3 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

Draft

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

b. An Operation Mentor and Capability Development (OMCD) capability is planned in order to mentor Cyber Operators to improve skills and enhance CAF cyber operations in order to maintain proficiency. Refer to the CD-DAR CONOPS for further detail.

Draft

8 MILESTONES

Management Milestone	Baseline Date	Expected Date	Actual Date	Approval Authority	Variance (Months) [Baseline - Actual]
SS (ID) – Approved (highest level)			Jan 2016	DCB	
Options Analysis – SOR – Approved			Apr 2019	CFD	
Options Analysis – Project Charter – Sign-Off			Oct 2020	C Cyber	
PA / EA (Def) – Approved (highest level)			Jun 2020	Treasury Board	
RFI Amendment and Draft ITQ posting	N/A		July 2020	PSPC	
ITQ posting	Oct 2020	April 2021		PSPC	+6 months
Draft Request for Proposals (RFP) posting	Mar 2021	Mar 2022		PSPC	+13 months
Implementation - Invitation for Bids – Approved	Feb 2022	Nov 2022		DGGC	+9 months
RFP posting	May 2022	Dec 2022		PSPC	+7 months
Implementation – Contract Documents – Finalized	Dec 2022	Aug 2023		DGGC	+8 months
Initial Planning Meeting (IPM)	Nov 2022	Oct 2023		ADM(Fin)	+11 months
PMB	Feb 2023	Nov 2023		PMB	+9 months
PA / EA (Imp) – Approved (highest level)	Jun 2023	May 2024		Treasury Board	+11 months
Implementation – Contract - Awarded	Sep 2023	Jul 2024		DGGC	+10 months
Implementation – IOC	Sept 2026	Aug 2027		C Cyber	+12 months
Implementation – FOC	Sept 2027	Aug 2028		C Cyber	+12 months
Implementation – Project Closed-Out	Dec 2027	Nov 2028		ADM(IM)	+12 months
Last SRB Meeting (progress review)			Feb 2020		
Next SRB Meeting (progress review)	Feb 2021	Feb 2021			

Draft

9 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.
Authorization	The right or a permission that is granted to a system entity to access a system resource. [Source: NIST SP 800-82 Rev. 2 – Glossary]
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. 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" is 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]
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 cyber-attacks 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]
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]
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	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 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]
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]
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 “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 Minister of National Defence (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]
Passively Monitor	Passive wiretapping (monitoring) is the monitoring or recording of data that attempts only to observe a communication flow and gain knowledge of the data it contains, but not alter or otherwise affect that flow. [Source: NIST Glossary: CNSSI 4009-2015 IETF RFC 4949 Ver2 – Adapted]
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.
Response Action	In DCO, 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]
Security Categorization	The process of determining the security category of business activities, information systems, and IT assets. [Source: Terminum]
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).
Task	A set of actions performed to accomplish a specific purpose whose accomplishment is one of the duties of an employee holding a particular position. [Source: Termium]
Trust Relationship	Policies that govern how entities in differing domains honor each other's authorizations. [Source: NIST SP800-95]
Virtual Device	A device that mimics a hardware device / appliance but exists only in a software form.

10 ACRONYMS & ABBREVIATIONS

Acronym / Abbreviation	Description
ACISS	Army Communications and Information System Specialist
ADM(Fin)	Assistant Deputy Minister (Finance)
ADM(IM)	Assistant Deputy Minister (Information Management)
AI	Artificial Intelligence
AMS	Advisory-focus Monitoring System
AOR	Area of Responsibility
API	Application Programming Interface
APT	Advanced Persistent Threats
AS	Anti-Spam
ATIS	Aerospace Telecommunications and Information System Technician
AUS	Australia
AV	Anti-Virus
BCA	Business Case Analysis
C Cyber	Chief of Cyberspace Staff
C2	Command and Control
C4ISR	Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance
CA	Canadian Army
CAF	Canadian Armed Forces
CANSOFCOM	Canadian Special Operations Forces Command
CCE	Communications Configuration Enumeration
CCSS	Communications Configuration Score System
CD-DAR	Cyber Defence - Decision Analysis and Response
CDR	Cyber Data Repository
CDS	Chief of the Defence Staff
CFD	Chief of Force Development
CFIOG	Canadian Forces Information Operations Group
CFNOC	Canadian Forces Network Operations Centre
CFSCE	Canadian Forces School of Communication and Electronics
CIICS	Cyber Information and Incident Sharing System
CIS	Centre for Internet Security
CITE	Cyber Integrated Test Environment
CJOC	Canadian Joint Operations Command
CMF	Capability Management Framework
COA	Course of Action

COD	Cyber Operational Dashboard
Comd-NET	Command Network
CONOPS	Concept of Operations
CONSUP	Concept of Support
COP	Common Operational Picture
CORA	Centre for Operational Research Analysis
COTS	Commercial off the Shelf
CPE	Common Platform Enumeration
CPU	Central Processing Unit
CSA	Cyber Security Awareness
CSC	Critical Security Controls
CSE	Communication Security Establishment
CSNI	Consolidated Secret Network Infrastructure
CSP	Cloud Service Provider
CSRA	Cyber Security Reference Architecture
CVE	Common Vulnerabilities and Exposures
DAR	Decision Analysis Response
DAOD	Defence Administrative Orders and Directives
DCB	Defence Capability Board
DCO	Defensive Cyber Operations
DCO-DS	Defensive Cyber Operations – Decision Support
DEFSOC	Defence Service Operations Centre
DEI	Defensive External Interdiction
DES Proc	Director Electronic Systems Procurement
DG Cyber	Director General Cyberspace
DGGC	Director General level Governance Committee
DGIMO	Director General Information Management Operations
DIMEI	Director Information Management Engineering and Integration
DIM Secur	Director Information Management Security
DND	Department of National Defence
DoD	Department of Defence (US)
DOS SJS	Director of Staff Strategic Joint Staff
DRA	Dynamic Risk Assessment
DRDC	Defence Research and Development Canada
DRM	Dynamic Risk Management
DWAN	Defence Wide Area Network
EDR	Endpoint Detection and Response
ETA	External Terrain Advantage

FE	Force Employment
FOC	Full Operational Capability
FVEY	Five Eyes
GBA+	Gender-Based Analysis Plus
GC	Government of Canada
GC CSEMP	Government of Canada Cyber Security Event Management Plan
GOTS	Government off the Shelf
GUI	Graphic User Interface
HA	High Availability
HLMR	High-Level Mandatory Requirements
HQ	Headquarters
HW	Hardware
IDM	Internal Defensive Measures
IDS	Intrusion Detection System
IEG	Information Exchange Gateway
IOC	Initial Operational Capability
IoCs	Indicators of Compromise
IP	Internet Protocol
IPCP-IA	Investment Plan Change Proposal – Impact Assessment
IPM	Initial Planning Meeting
IPS	Intrusion Prevention System
ISS	In-Service Support
IT	Information Technology
ITA	Internal Terrain Advantage
ITI	Information Technology Infrastructure
ITI in Sp of C2	Information Technology Infrastructure in Support of Command and Control
ITQ	Invitation to Qualify
ITS	Information Technology System
ITSM	Information Technology Service Management
JBMC	Joint Battlespace Management Capability
JTF	Joint Task Force
KML	Keyhole Markup Language
LCMM	Life-Cycle Material Manager
MISP	Malware Information Sharing Platform
ML	Machine-Learning
MND	Minister of National Defence
MOC	Military Occupation
MTBF	Mean Time between Failures

MTTC	Mean Time to Contain
MTTD	Mean Time to Detect
MTTI	Mean Time to Identify
MTTR	Mean Time to Respond/Resolve
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NAVCOMM	Naval Communicators
NCIOP	Naval Combat Information Operators
Net C2 ISAC	Network Command and Control Integrated Situational Awareness Capability
NetOps	Network Operations
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
NVG	NATO Vector Graphics
NZ	New Zealand
OA	Operational Authority
OA Phase	Options Analysis Phase
OGD	Other Government Department
OMCD	Operational Mentor and Capability Development
OSINT	Open Source Intelligence
PA(Def)	Project Approval (Definition)
PACS	Physical Access Control Systems
PAD	Project Approval Directive
PAT	Port Address Translation
PB(ID)	Project Brief (Identification)
PCAP	Packet Capture
PD	Project Director
PDNA	Professional Development Needs Assessment
PM	Project Manager
PMB	Programme Management Board
PO	Performance Objective
PSPC	Public Services and Procurement Canada
PSI	Prime System Integrator
Qty	Quantity
R&D	Research and Development
RA	Response Actions
RBAC	Role-Based Access Control
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy

RFI	Request for Information
RFP	Request for Proposals
ROI	Return on Investment
SA	Situational Awareness
SA&A	Security Assessment and Authorization
SAAG	Security Assessment and Authorization Guidelines
SANS	SysAdmin, Audit, Network and Security
SCAP	Security Content Automation Protocol
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
SS(ID)	Synopsis Sheet (Identification)
SSC	Shared Services Canada
SSE	Strong, Secure, Engaged
SSL	Secure Sockets Layer
SW	Software
SWID	Software Identification
TA	Technical Authority
TAD	Technical Architecture Document
TB	Treasury Board of Canada
TBD	To Be Determined
TTPs	Tactics, Techniques and Procedures
UDL	Unified Data Landscape
UEBA	User and Entity Behaviour Analytics
UK	United Kingdom
US	United States
XCCDF	Extensible Configuration Checklist Description Format
ZIP	Zone Interfcace Point

Draft

11 CYBER ENTITIES KEY ATTRIBUTES

11.1 Key Attributes of Human Cyber Entities

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

Draft

11.2 Key Attributes of Non-Human Cyber Entities

Serial	Description
1	Host Type - physical or virtual
2	Host Name (in accordance with naming convention in use)
3	Hardware manufacturer/serial number/asset tag number (with asset tag to correlate with account holder)
4	Processor (manufacturer, serial number, model, etc.)
5	Memory (manufacturer, serial number, model, etc.)
6	Inventory and Identification of all Line Replaceable Units (LRUs) on board the device (CD-ROM/DVDRW/USB ports, physical/ keyboard/ mouse/ monitors/ NICs, processors, mother boards, power supplies, containers/frames etc.)
7	Type or Primary Purpose of Device (workstation, virtual desktop router, switch, firewall, gateway, web filter, intrusion detection system, intrusion prevention system, domain controller, wireless access points, application servers, mail server, databases, intranet applications, etc.)
8	Device Model, sub-model, version
9	MAC address (or addresses if more than one interface) for all natures of external interfaces
10	IP address and subnet (fixed or DHCP assigned)
11	Host URL name Host URL name
12	How IP address assigned, DHCP, DHCP reserved, or fixed host assigned
13	Host Time
14	Host Network Time Server (if set remotely)
15	Host Gateway(s)
16	Host DNS main, alternate, second alternate
17	Host DHCP server
18	Host WINS server
19	Host Web Proxy server (if applicable)
20	Host Routing Tables
21	Host Port Forwarding Tables

Draft

Serial	Description
22	Host Network Address Translation Tables (NAT)
23	Host Domain
24	Assigned Primary Domain Controller
25	Assigned Secondary Domain Controller
26	Active Directory (AD), Lightweight Directory Access Protocol (LDAP), X.500 registration status
27	IPv4 or IPv6
28	Host Permission Rights (owner, administrators, users, guests, etc.) and how assigned/controlled (local or active directory)
29	SNMP data used and version number
30	ICMP status
31	Host based anti-virus software and version
32	Host based intrusion prevention software and version
33	Host based intrusion detection software and version
34	Host based firewall service status
35	Host Certificate Authority
36	Host Ports (open, closed, listening, stealth mode)
37	OS and version
38	Baseline image version (if applicable)
39	Installed software inventory - High level
40	Installed software inventory - Detailed level - all DLLs, and supporting executables, configuration files, and related software modules or components.
41	Baseline configuration hashcode (for ease in baseline configuration change detection)
42	Services running on device and ports in use
43	Host services certificates
44	Username(s) logged-in and currently authenticated

Draft

Serial	Description
45	Location – Physical place name (as in CFB Petawawa, building P114, Room 101, desk 5) and its Geodetic equivalent (latitude, longitude and altitude), or simply if mobile, its latitude, longitude and altitude.
46	Owner – Hardware account holder
47	Source of power (mains, internal battery, external battery)
48	Source of backup power system
49	Physical properties - temperature, humidity
50	Existing vulnerability reports, known threats, history of reports associated with events/incidents
51	Named network, enclave, subnet etc. to which the device is connected directly
52	Date of last audit/inspect/review
53	Access/location of device internal logs (if any) (SIEM, SNMP, SCOM, etc.)

Draft

Assistant Deputy Minister (Information Management)

Concept of Operations (CONOPS)

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

Draft

DSP NO.:	C.000707
TITLE:	Cyber Defence – Decision Analysis and Response (CD-DAR)
PROJECT PHASE:	Definition
PROJECT SPONSOR:	Assistant Deputy Minister (Information Management) (ADM(IM))
EFFECTIVE DATE:	2 February 2021
VERSION	1.0

Draft

This page intentionally left blank.

SIGNATURE PAGE

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

Endorsed by:

DPDCC	Signature	Title	Telephone	Date
		Project Manager (PM), CD-DAR		

D Cyber Ops FD	Signature	Title	Telephone	Date
		Project Director (PD), CD-DAR		

DGICFD	Signature	Title	Telephone	Date
		DGICFD		

Approved by:

C Cyber	Signature	Title	Telephone	Date
		C Cyber	TBD	

Draft

Draft

This page intentionally left blank

RECORD OF AMENDMENTS

Draft documents being distributed should follow the version convention as identified in the 'Project Documents and Records Management Plan', until the document is formally approved through the Cyber Defence – Decision Analysis and Response (CD-DAR) Documents and Records Management process.

The first official release of this document shall be version 1.0

Each new version (V1.0, V2.0, etc.) of this document shall be identified in the following table by the Version identifier assigned to the revised document. The table shall also include the Change Request (CR) number assigned to each approved change that was incorporated in the revised document.

All elements of this released document including, but not limited to, Front Matter, Body Matter (text, tables, and figures/illustrations), and Back Matter shall be subject to formal document and records management, and integrated change management processes.

Note: When a document includes one or more excerpts from one or more other documents, those excerpts will only be revised when the source documents are revised.

Version	Date	Modified by	CR	Comments
V1.0	2021-02-xx	Maj N. Mallory		Original version

Draft

This Page left intentionally blank

Draft

EXECUTIVE SUMMARY

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-sponsored cyber espionage and disruptive cyber operations. This threat can be expected to grow in the coming years. Addressing the cyber threats is complicated by the difficulties involved in identifying the source of cyber-attacks with certainty and the jurisdictional challenges caused by the possible remoteness of cyber-attacks.

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 (DCO).

Ultimately, DND/CAF's cyber force will be equipped, trained and prepared to effectively conduct DCO built on a strong foundational cyber security and defence capability; and an ISS capability framework able to maintain and optimize DCO operational processes, CD-DAR hardware and software tools, and recurring training of personnel to ensure the CD-DAR capability remains available, reliable and operationally relevant, and allows future growth development throughout its in-service life.

Draft

[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.

This Page left intentionally blank

Draft

TABLE OF CONTENTS

1 Introduction 1

1.1 OBJECTIVE 1

1.2 CAPABILITY NEED 1

1.3 SCOPE 1

1.4 MISSIONS 2

1.5 ASSUMPTIONS 2

1.6 CONSTRAINTS 3

1.7 INTERNAL STAKEHOLDERS 3

1.8 EXTERNAL STAKEHOLDERS 6

2 CURRENT SYSTEM DESCRIPTION 8

2.1 CYBER FORCE EMPLOYMENT 8

2.2 CYBER DEFENCE ORGANIZATIONS 8

2.2.1 Canadian Forces Network Operations Centre (CFNOC) 8

2.2.2 Defence Service Operations Centre (DEFSOC) 10

2.2.3 JFCCC Cyber Component Coordination Element (JFCCC CCCE) 11

2.2.4 Relationship between CFNOC, DEFSOC and JFCCC CCCE 13

2.3 CFNOC CURRENT OPERATING CONCEPT 13

2.3.1 Defensive Cyber Operations Framework 14

2.4 ORGANIZATIONAL INTERACTIONS AND INTELLIGENCE/INFORMATION EXCHANGE 16

2.4.1 Cyber Defence Operations (CD Ops) Team 16

2.4.2 Cyber Threat Intelligence Cell (CTIC) 17

2.4.3 Incident Handling (IH) Team 18

2.4.4 Surveillance Team 19

2.4.5 Reconnaissance Team 20

2.4.6 Forensics Team 21

2.4.7 Enterprise Intrusion Detection System Support Team 24

2.4.8 Enterprise Vulnerability Assessment Support Team 25

2.5 TRAINING DEVELOPMENT – SKILLSETS, ROLES AND CYBER EXERCISE OPPORTUNITY 25

2.5.1 Cyber Operator Skill Sets 26

2.5.2 Roles of the Cyber Operator (Tiers 1, 2 and 3) 26

2.5.3 Collective Training Exercises 27

3 JUSTIFICATION AND NATURE OF CHANGE 29

3.1 DRIVERS FOR CHANGE 29

Draft

3.2 DESCRIPTION OF DESIRED CHANGES 30
3.2.1 Network Discovery 30
3.2.2 Trusted Database Repository 31
3.2.3 Common Operating Picture (COP) 31
3.2.4 Human Factors 32
3.2.5 Capability to Conduct Forensics 33
3.3 PRIORITIES AMONG CHANGES 33
4 CD DAR System Overview 35
4.1 OPERATIONAL OBJECTIVES (BUSINESS OUTCOMES) 35
4.2 HIGH LEVEL MANDATORY REQUIREMENTS 35
4.3 OPERATIONAL VIEW (OV-1) 37
4.3.1 Operational Environment, Interoperability, Flexibility and Resilience 39
4.3.2 Cyber Security and Defence Staff 40
4.4 CD DAR OPERATING MODEL 40
4.4.1 Cyber Common Operating Picture (COP) 41
4.4.2 Security Orchestration Automation Response (SOAR) 42
4.4.3 Operational Training 45
4.4.4 Cyber Security Monitoring 46
4.4.5 Cyber Defence Analysis and Decision Support 49
4.4.6 CD-DAR Integration 52
4.4.7 Cyber Data Repository (CDR) 53
4.4.8 Cyber Entity and Event Discovery 54
4.5 INNOVATION 55
4.5.1 Operation Mentor and Capability Development (OMCD) 55
4.5.2 Big Data Analytics 56
4.5.3 Artificial Intelligence 57
4.6 IN SERVICE SUPPORT (ISS) ENVIRONMENT 58
4.6.1 1st Level Support 59
4.6.2 2nd Level Support 59
4.6.3 3rd Level Support 62
4.6.4 4th Level Maintenance 62
5 Conclusion 63
5.1 OPERATIONAL IMPACTS 63
5.2 ORGANIZATIONAL IMPACTS 63

Draft

5.3 IMPACTS DURING DEVELOPMENT AND DELIVERY 64

Annex A – CFNOC Organizational Interaction Diagrams A-1

Annex B – Acronyms and Abbreviations B-1

TABLE OF FIGURES

Figure 1 – CFNOC – Level 4 organization within CFIOG 9

Figure 2 – DEFSOC – Level 4 organization within 7 Comm Gp 11

Figure 3 – JFCCC CCCE – Level 4 organization under CFIOG 12

Figure 4 – CFNOC Operating Concept 14

Figure 5 – DCO Framework 15

Figure 6 – High Level Operational View (OV-1) 38

Figure 7 – Cyber Response Development Lifecycle 47

Figure 8 – CITE Lab Environments 61

Figure 9 – CD Ops interaction and Int / Info exchange with stakeholders A-1

Figure 10 – CTIC interaction and Int / Info exchange with stakeholders A-2

Figure 11 – Incident handling Team interaction and Int / Info exchange with stakeholders A-3

Figure 12 – Surveillance Team interaction and Int / Info exchange with stakeholders A-4

Figure 13 – Reconnaissance Team interaction and Int / Info exchange with stakeholders A-5

Figure 14 – Forensics Team interaction and Int / Info exchange with stakeholders A-6

Figure 15 – CD Ops Cyber Event Coordination Workflow A-6

Figure 16 – Cyber Event Management including with FVEY on Pegasus A-7

Figure 17 – Cyber Information and Management Workflow A-7

Figure 18 – Incident Handling Workflow A-8

Figure 19 – Assessment of Known Threats Workflow A-8

Figure 20 – Assessment of Unknown Threats Workflow A-8

Figure 21 – Asset Discovery Workflow A-9

Figure 22 – Target Scanning Workflow A-9

Figure 23 – Vulnerability Assessment Workflow A-9

Figure 24 – System/Network Penetration Test Workflow A-9

Figure 25 – Test Emulation Workflow A-10

Figure 26 – Enterprise Intrusion Detection System (IDS) Workflow A-10

Draft

Figure 27 – IDS Capability Development Workflow A-10

Figure 28 – Enterprise Vulnerability Assessment Workflow A-10

LIST OF TABLES

Table 1 – CD-DAR Internal Stakeholders 3

Table 2 – CD-DAR External Stakeholders 6

Table 3 – Forensics Activities 21

Table 4 – CD-DAR HLMRs 36

Draft

1 INTRODUCTION

1.1 Objective

This Concept of Operations (CONOPS) defines the cyber force's roles and responsibilities, complete with the processes and tools that will form the Cyber Defence – Decision Analysis and Response (CD-DAR) capability for Department of National Defence / Canadian Armed Forces (DND/CAF). It provides a description of the new capability and the conditions under which it will operate, the processes that will be used to secure and defend the DND/CAF Cyber environment, as specified in the project scope below, and how Commanders, Executives, Staff and Cyber Operators will interact with CD-DAR.

1.2 Capability Need

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

1.3 Scope

This CONOPS focuses on the Force Employment (FE)[2] of the CD-DAR defensive cyber capabilities to monitor and defend DND/CAF networks, to include the ability to detect, analyze, and respond to threats. The CD-DAR capability will also provide reliable contextual analysis to support DND/CAF decisions and actions in the conduct of Defensive Cyber Operations (DCO) within designated Command Network[3] (Comd-Net) Extensions and Interfaces, and deployable Defence Wide Area Network (DWAN) (Designated network – Protected B and below) systems. Consolidated Secret Network Infrastructure (CSNI) (Classified network – Secret) is part of Comd-Net within DND/CAF and a significant portion of the scope of CD-DAR will be applied to CSNI. The structure of Comd-Net is ever changing as more services, systems and network infrastructures are consolidated into CSNI to serve CAF requirements and operations more effectively. CD-DAR capabilities on deployed DWAN will consist of all infrastructure from the endpoint up to and including the input interface to the Shared Services Canada (SSC) controlled DWAN infrastructure at the Network Access Gateway (after decryption) located within Canada.

All networks and infrastructure outside of DND/CAF Command Network are out of scope for CD-DAR, however it is understood that such systems may provide input to the inclusive

[2] At the operational level, Force Employment refers to the command, control and sustainment of allocated forces, Defence Terminology Bank (DTB), Record #32173.

[3] 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.

Draft

networks. These input will be monitored by CD-DAR at the point of entry for any anomalies that may trigger an event.

Ultimately, the CD-DAR capability will enable the CAF cyber force to defend CAF's freedom of action and interests in cyberspace, and deliver military effects in and through a contested cyber environment in support of CAF missions and operations.

1.4 Missions

Strong, Secure, Engaged: Canada's Defence Policy (SSE), gives significant attention to operating in and defending cyberspace, assuming a more assertive posture in the cyber domain and expanding DND/CAF cyber capabilities. CD-DAR aligns with SSE and the DND/CAF Cyber Mission Assurance (CMA) Program by delivering cyber capabilities to support military operations by protecting critical military networks and equipment from cyber-incidents and better allow cyber capabilities to support the "CAF core missions:

a. Detect, deter and defend against threats to or attacks on Canada;

b. Detect, deter and defend against threats to or attacks on North America in partnership with the United States, including Through the North American Aerospace Defense Command (NORAD);

c. Lead and/or contribute forces to the North Atlantic Treaty Organization (NATO) and coalition efforts to deter and defeat adversaries, including terrorists, to support global stability;

d. Lead and/or contribute to international peace operations and stabilization missions with the United Nations (UN), NATO and other multilateral partners;

e. Engage in capacity building to support the security of other nations and their ability to contribute to security abroad;

f. Provide assistance to civil authorities and law enforcement, including counter-terrorism, in support of national security and the security of Canadians abroad;

g. Provide assistance to civil authorities and non-governmental partners in responding to international and domestic disasters or major emergencies; and

h. Conduct search and rescue operation."[4]

1.5 Assumptions

The assumptions for the CD-DAR capability include:

a. Funding for any required updates to the operational infrastructure will be allocated;

b. The bandwidth within the current Information Technology Infrastructure (ITI) will be able to accommodate the CD-DAR capability Situational Awareness (SA) data update requirements, especially at deployed locations;

[4] Strong, Secure, Engaged: Canada's Defence Policy (SSE), Minister of National Defence, 2017.

Draft

c. Government and DND/CAF policy, organizations and practices will continue improving their response to cyber threats;

d. Supporting Government departments, including the Communications Security Establishment (CSE), SSC and Canadian Security Intelligence Service (CSIS) will continue contributions to national cyber security; and

e. Current Director General Information Management Operations (DGIMO) processes will be adapted to the fielded technologies, respond to external drivers of social change and changes in the nature of the Cyber conflict.

1.6 Constraints

The constraints to the CD-DAR capability include:

a. Security Clearance – the nature of the cyber security domain requires personnel and Industry with security clearances up to TOP SECRET Signals Intelligence (SIGINT) and with citizenship restrictions from Australia / New Zealand / United Kingdom / United States (AUS/NZ/UK/US) to CANADIAN citizens only; and

b. Design Requirement – The systems 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. To be successful, the CD-DAR capability most not require excessive training that fundamentally changes the skills and the available trades or occupations fulfilling those roles.

1.7 Internal Stakeholders

Internal stakeholders consist of organizations within the DND/CAF that are either directly or indirectly affected by the CD-DAR capability. The CD-DAR internal stakeholders are identified in Table 1 below.

Table 1 – CD-DAR Internal Stakeholders

Organization	Responsibility
Strategic Joint Staff (SJS)	Provides military analysis and decision support to the Chief of Defence Staff (CDS), the principal military advisor to the Government of Canada (GC). The Joint Battlespace Management Capability (JBMC) supports CAF operational information and decision-making processes to determine the correct mix of people, process and technology for the provision of a fused CAF COP for use by Commanders to achieve SA. CD-DAR will feed JBMC with cyber SA relevant to ongoing operations.
Canadian Joint Operations Command (CJOC)	Responsible for integrating CAF capabilities, including Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR), along with space and

Draft

Organization	Responsibility
	cyber capabilities into mission specific task forces. Executes and sustains operations in Canada, across North America and overseas in response to direction issued by the GC.
Director General Information Operations Group (DGIMO)	Provides the operational foundation for the Information Management Group (IM Gp). The division spans all levels of command – tactical, operational, and strategic – in order to coordinate, support, and provide the Command and Control (C2) and intelligence capabilities the CAF and the Department need to do their job.
7 Communication Group (7 Comm Gp)	7 Comm Gp is a direct report of DGIMO. 7 Comm Gp provides, coordinates and manages DND/CAF information technologies and network services that enable the C2 and information sharing in support of DND business objectives and CAF command. Its mission is to sustain communications and information systems (CIS) in order to enable the CAF to exercise C2 while force generating line capabilities in support of CAF operations.
Defence Service Operations Centre (DEFSOC)	DEFSOC reports to 7 Comm Gp. DEFSOC delivers Information Technology (IT) network In-Service Support (ISS) to DND/CAF operations and activities, including Enterprise IT support and information network support to the environments and Commanders.
Canadian Forces Information Operations Group Headquarters (CFIOG)	CFIOG reports to DGIMO. CFIOG generates and employs SIGINT, Electronic Warfare (EW), and cyber operations capabilities to enable CAF operations and the DND. CFIOG provides force capability development for cyber defence, intelligence, and information support services in support of Canadian, American, British, New Zealand, Australian, and coalition forces and supports classified networks for communications and the Technical Security Inspection Team (TSIT).
Canadian Forces Network Operations Centre (CFNOC)	CFNOC reports to CFIOG. CFNOC provides 24/7 status monitoring and incident handling in support of network operations and defence of DND/CAF networks against cyber exploits.
Joint Force Cyber Component Commander Cyber Component	The JFCCC CCCE reports to JFCCC through CFIOG. JFCCC CCCE provides subject matter experts within the cyber environment and sustains cyber situational awareness globally as

Draft

Organization	Responsibility
Coordination Element (JFCCC CCCE)	it impacts CJOC and its missions. The element is collocated with CJOC.
Director General Enterprise Application Services (DGEAS)	Provides IT application and Information Management (IM) services to support CAF operations and DND corporate objectives.
Director General Information Management Project Delivery (DGIMPD)	Collaboratively partners with clients, stakeholders, and IM Group colleagues to strategically plan, design, develop, and deploy technology enabled solutions, capabilities, and changes to the Information Management / Information Technology (IM/IT) capability of DND/CAF.
Director General Information Management Technology and Strategic Planning (DGIMTSP)	Establishes strategic and tactical direction on IM/IT Program transformation for DND/CAF. DGIMTSP supports CAF operations, departmental priorities, and government objectives by ensuring seamless and timely access to trusted information, intelligence, and technology in a secure environment.
Directorate Information Management Capability Development (DIMCD)	DIMCD reports to DGIMTSP. DIMCD is responsible for the management, oversight and coordination of activities within DND/CAF to support the GC IT transformation program. It is also responsible for managing the departmental Enterprise License Portfolio. DIMCD is currently the PD for the Information Technology Service Management (ITSM). In addition, DIMCD is the centre of expertise through the National Service Management Office (NSMO).
Directorate Information Management Engineering and Integration (DIMEI)	DIMEI reports to DGIMTSP. DIMEI leads DND/CAF in the engineering, testing, and integration of IM/IT infrastructure capabilities. DIMEI supports the Defence Chief Information Officer (DCIO) as Chief Engineer and Chief Architect, and is also involved with C4ISR and cyber security. DIMEI identifies opportunities within the current technical architecture to improve efficiency, reduce complexity and costs, and to increase interoperability with partner organizations, particularly NATO and the Combined Communications and Electronics Board (CCEB) nations.
Director Information Management Security (DIM Secur)	DIM Secur reports to DGIMTSP. DIM Secur oversees IT and Information Security in the DND/CAF. It supports and advises the DCIO, the Chief Security Officer (CSO) and various Operational Authorities (OAs) on the effectiveness of IT security risk-mitigation measures through the Security Assessment and Authorization (SA&A), Oversight and

Draft

Organization	Responsibility
	Compliance (O&C), and Industrial Information Security programs. It also performs the functions of departmental authorizer for all IT systems, Departmental Communication Security (COMSEC) Authority (DCA), and Departmental Emission Security (EMSEC) Authority.

1.8 External Stakeholders

External stakeholders consist of organizations outside the DND/CAF that interface or exchange cyber information / intelligence with the DND/CAF and/or the CD-DAR capability. The CD-DAR external stakeholders are listed in Table 2 below.

Table 2 – CD-DAR External Stakeholders

Organization	Responsibility
Public Safety Canada (PSC)	Spearheads the GC's first priority, to protect the safety and security of Canadians both at home and abroad, by coordinating the activities of federal departments and agencies tasked with protecting Canadians and their communities, businesses and interests. PSC functions as a centralized hub for coordinating efforts in counter-terrorism, critical infrastructure, and cyber and transportation security. The CAF continues to work closely with PSC in support of the National Cyber Security Strategy.
Communications Security Establishment (CSE)	CSE is the national SIGINT agency for foreign intelligence and the Technical Authority (TA) for cyber security and information assurance. CSE's Canadian Centre for Cyber Security (CCCS) helps protect the systems and information that Canadians rely on every day, and is the lead cyber TA for GC. Operational authority remains with all individual departments.
Shared Services Canada (SSC)	SSC provides modern secure and reliable IT services to GC organizations. Part of its mandate is to design and operate an effective, efficient and secure IT infrastructure that protects GC data and technology assets. SSC develops security policies, standards, plans and designs, and provides security-related services for the delivery of Government services. SSC is responsible for applying controls such as firewall, anti-virus and anti-malware, secure remote access, and vulnerability management to GC systems and services.
Canadian Security Intelligence Service (CSIS)	CSIS collects and analyzes threat-related information concerning the security of Canada in areas including terrorism, espionage,

Draft

Organization	Responsibility
	the proliferation of weapons of mass destruction, foreign interference and cyber-tampering affecting critical infrastructure.
Royal Canadian Mounted Police (RCMP)	The RCMP has a broad mandate when it comes to investigating and apprehending criminals in the online world, or otherwise disrupting cybercrime activity. The RCMP Cybercrime Strategy is therefore broad in scope and reflects the role of cyber in several law enforcement areas. Its vision is to reduce the threat, impact and victimization of cybercrime in Canada through law enforcement action.
Five Eyes (FVEY)	The FVEY partnership is an intelligence alliance comprising Australian, Canada, New Zealand, the United Kingdom and United States and are party to the multilateral UKUSA Agreement. DND/CAF will continue to work closely with the FVEY partners on cyber security. Their expertise and support is indispensable to the success of our cyber defence operations.
North Atlantic Treaty Organization (NATO)	NATO is an intergovernmental military coalition that relies on strong and resilient cyber defence to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security. NATO's main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience across the Alliance. NATO stood up a new Cyberspace Operations Centre as part of its strengthened Command Structure. NATO can draw on national cyber capabilities for its missions and operations.

Draft

2 CURRENT SYSTEM DESCRIPTION

2.1 Cyber Force Employment

As mentioned in section 1.3, this CONOPS covers the FE of the CAF cyber force in support of CAF operations and missions. Joint operations are conducted using the FE process, which includes all activities required to plan, execute, and review (lessons learned (LLs)) joint operations. Conversely, the Concept of Support (CONSUP) addresses the Force Generation (FG) and Force Development (FD) of the cyber force and operational cyber capabilities.[5]

CAF operations fall within three broad categories, i.e. Routine, Contingency, or Rapid-response operations. Routine operations are normally recurring in nature, can usually be planned for, and are programmed on an annual basis. Most defensive cyber operations are routine operations.

Contingency operations are planned in advance of known events or events that could reasonably be expected, thereby permitting a formal operational planning process. CJOC has developed the Contingency Plan (CONPLAN) CETO for operations which the primary focus is Cyber Operations. A Standing Operation (OP) Order has also been developed to facilitate the instantiation of CONPLAN CETO, referred to as OP LADON.

Finally, Rapid-response operations are those FE activities that require an immediate CAF action to save lives, reduce human suffering, or mitigate property damage. In the interest of achieving timely effects, planning will be reduced to its essential components; thus higher risk is accepted in planning, preparing and coordinating the operation. Rapid-response operations will further be discussed in section 2.4.[6]

2.2 Cyber Defence Organizations

As illustrated at Figure 1, the CAF cyber force is employed under the Command authority of the CDS and lead by the Cyber Force Commander (CFC). Routine operations are under the leadership the CAF Cyberspace Division Commander, while JFCCC is accountable to Commander CJOC for the C2 of Contingency and Rapid-response operations.

Each DND/CAF Cyber Defence unit involved in the conduct of DCO, their respective cyber security and defence roles and responsibilities and current Cyber Defence processes is described in the following sub-sections.

2.2.1 Canadian Forces Network Operations Centre (CFNOC)

CFNOC's mandate is derived from SSE, the National Cyber Security Strategy and specifically articulated in Canadian Forces Cyber Division (CFCD) Operation Plans and CFIOG Commander's Directives.

CFNOC is the national operational cyber defence unit permanently assigned mission critical tasks to represent DND/CAF and applicable network OAs. CFNOC has evolved from an organization executing Network Operations (Net Ops) and Mission Assurance (MA) tasks into

[5] Canadian Forces Joint Publication (CFJP) 3.0 – Operations, Chapter 2, p.2-1.

[6] CFJP 3.0 – Operations, Chapter 6, p.6-3.

Draft

an organization focused on Defensive Cyber Operations – Internal Defence Measures (DCO-IDM).[7]

More specifically, CFNOC is mandated to:[8]

a. Plan and execute DCO-IDM in support of DND/CAF;

b. Prepare Force Elements for DCO-IDM and TSIT activities in accordance with CFIOG's Force Posture and Readiness (FP&R);

c. Provide tactical defensive cyber intelligence in support of CAF tactical DCO in accordance with intelligence priorities; and

d. Maintain a 24/7 cyber defence response capability.

2.2.1.1 Organizational Structure

CFNOC is a level 4 organization within ADM (IM), and one of four units under CFIOG.

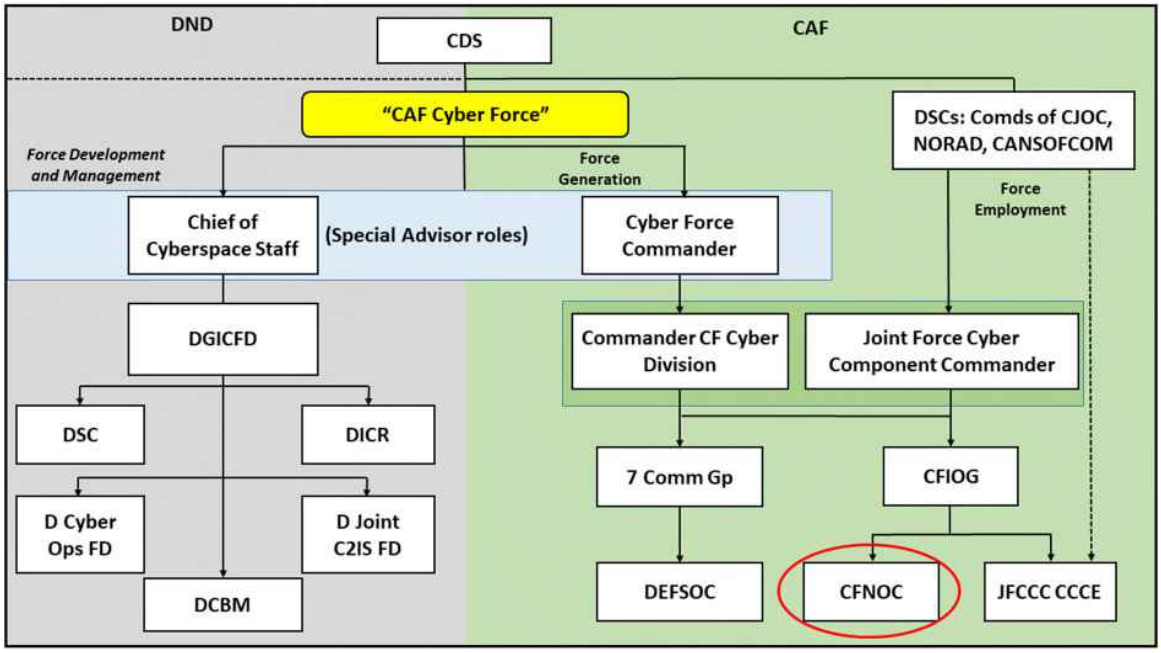


Figure 1 – CFNOC – Level 4 organization within CFIOG

2.2.1.2 Roles and Responsibilities

CFNOC's mission, in concert with DND/CAF Whole of Government (WoG) partners and allies, is to gain and maintain cyber superiority within DND/CAF cyber Areas of Responsibility (AOR)

[7] DCO-IDM: In defensive cyber operations, measures and activities conducted within one's own cyberspace to ensure freedom of action, DTB Record #694340

[8] CFNOC CONOPS, 12 April 2019.

in order to assure friendly-force freedom of action, and enable operational commanders to make informed defence and security decisions related to the cyber environment.

On behalf of the CAF CFC, CFNOC directs the routine operation and defence of DND/CAF networks. CFNOC is a dynamic organization that has been undergoing significant changes. CFNOC's functions are led by the Ops Section, with the Cyber Defence Operations (CD Ops) Section providing guidance and coordination throughout the lifecycle of a cyber-event.

2.2.2 Defence Service Operations Centre (DEFSOC)

The Defence Service Operations Centre (DEFSOC) coordinates the delivery of IT services across the department, provides functional direction to Service Management Centres (SMC), and coordinates enterprise support at the 3rd level in concert with the National Service Desk (NSD). At the national level, DEFSOC performs service requests and incident management, and is responsible for coordinating service operations, including the primary interface with SSC and other external service providers, including Telus, Bell, etc. In addition, it will monitor and facilitate shared SA of the performance of DND/CAF networks.

2.2.2.1 Organizational Structure

As depicted at Figure 2, DEFSOC is a level 4 organization within ADM (IM) under 7 Comm Gp. While DEFSOC doesn't directly interact with users, it does act as the operational level entity for escalation of incidents from SMCs via the NSD or the Net Ops Coordination Team.

DEFSOC has two units responsible for providing in-service support to DND/CAF enterprise IT:

a. The NSD in which Agents respond to all inquiries to DEFSOC, as well as initiating the necessary processes for event; and

b. The Net Ops Desk, which manages Service Request Management, Incident Management, and Problem Management.

DEFSOC-NSD can function as a 1st Level Service Provider, however this is typically during off peak hours, as well as deployed operations. DEFSOC submits service requests into the Enterprise ITSM (EITSM) system on a client's behalf and direct the request to the relevant SMC's Service Department for further action when the SMC returns to duty.

DEFSOC Net Ops co-ordinates fulfillment of requests requiring multiple service providers, which may include SSC. DEFSOC resolves escalation issues and de-conflicts network operations to support consistent network availability.

Draft

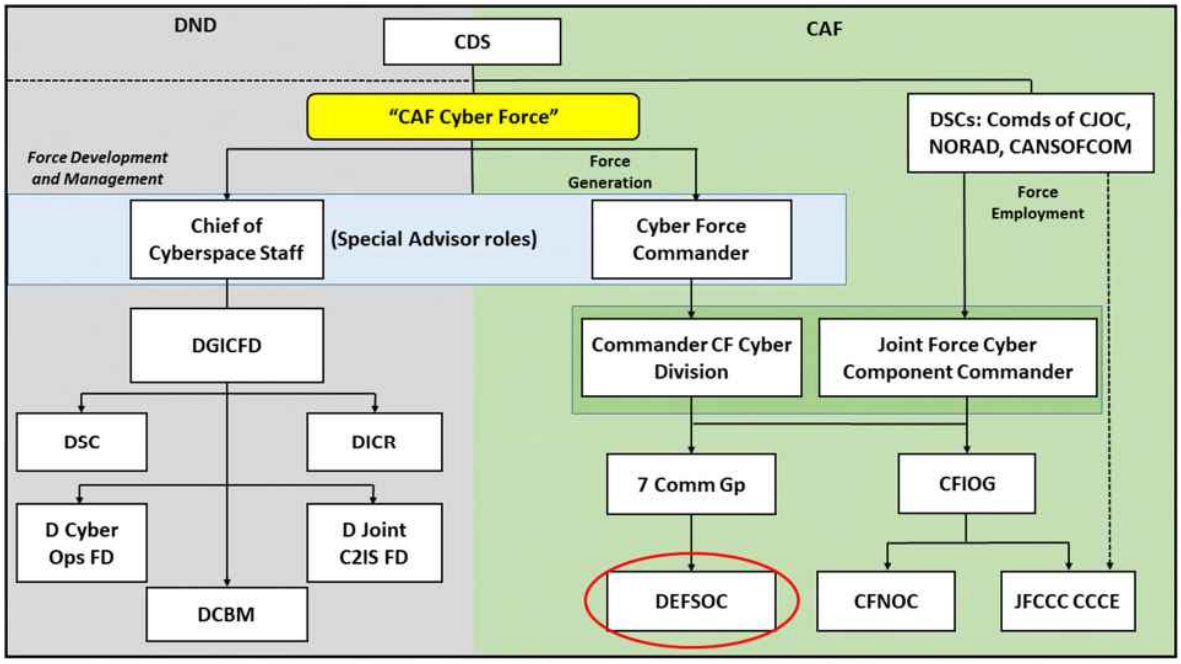


Figure 2 – DEFSOC – Level 4 organization within 7 Comm Gp

2.2.2.2 DEFSOC's Roles and Responsibilities

DEFSOC provides national ITSM operations coordination across the DND/CAF. It sustains and governs DND IT and CAF CIS operations management and coordinates the provisioning of IT services to meet DND business and CAF operational objectives. Key DEFSOC responsibilities include:

a. DND/CAF IT service operations coordination;

b. Service issues resolution;

c. Enterprise network monitoring and reporting;

d. National Service Desk;

e. Canadian Forces Service Release; and

f. Change Management Prioritization.

2.2.3 JFCCC Cyber Component Coordination Element (JFCCC CCCE)

Given the increasingly cyber-enabled operational environment, a new section comprised of cyber domain Subject Matter Experts (SME) was created under JFCCC. The JFCCC Cyber Component Coordination Element (CCCE) delivers expertise and advice on the full range of Cyber Operations to Commander CJOC and staff across all functional areas in support of CAF missions both at home and abroad. The unit is under the operational command (OPCOM) of CFIOG, but under the operational control (OPCON) and planning authority of CJOC, reporting to the CJOC Chief of Staff (COS) Ops.

Draft

2.2.3.1 Task Force Cyber Component Coordination Element (TF CCCE)

The Task Force Cyber Component Coordination Element (TF CCCE) is an extension of the JFCCC in theatre on expeditionary or domestic operations. The TF CCCE Team Lead is responsive to the Task Force Commander (TFC) and is accountable to JFCCC through the JFCCC CCCE. The TF CCCE Team Lead is normally delegated authority to provide advice regarding cyber operations to the TFC and act as a forward planning element for cyber activities and operations. The JFCCC provides the TF CCCE Team Lead with specific guidance, clear expectations, and limit of responsibility.

2.2.3.2 Organizational Structure

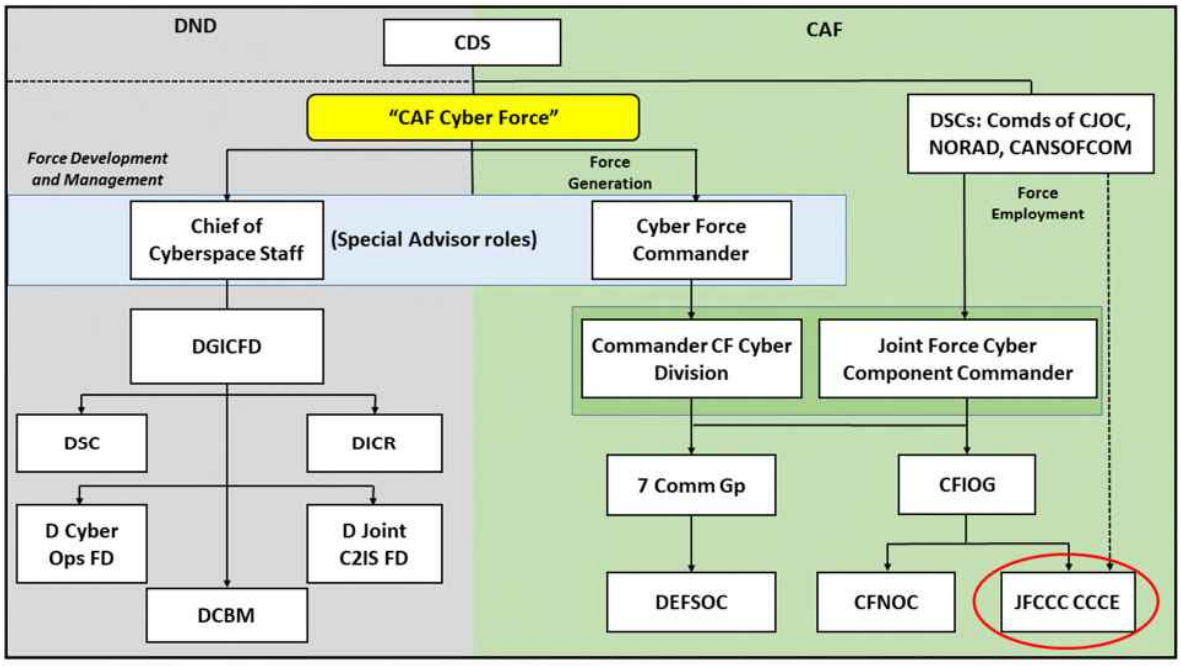


Figure 3 – JFCCC CCCE – Level 4 organization under CFIOG

2.2.3.3 JFCCC CCCE's Roles and Responsibilities

JFCCC CCCE's mandate is to advise the CJOC Commander and planning staff on cyber domain matters, and to prepare the cyber annexes to all CJOC Operations orders. Its primary roles are as follows:

a. Provide advice on the employment of cyber capabilities for missions and training events;

b. Develop and maintain comprehensive cyber SA for Comd CJOC;

c. Coordinate activities with Other Government Departments (OGD) and allied military forces to scope and react to threats to Canada originating from cyberspace;

d. Provide a single CFIOG point of presence supporting Commander CJOC; and

e. Capture cyber lessons learned and identify requirements in order to develop modern capabilities.

Beside its cyber advisory and planning role for deployed and domestic operations, JFCCC CCCE is not directly involved in cyber defence.

2.2.4 Relationship between CFNOC, DEFSOC and JFCCC CCCE

2.2.4.1 CFNOC Relationship with JFCCC CCCE and DEFSOC

CFNOC, JFCCC CCCE and DEFSOC do not have interlinking responsibilities but collaborate whenever possible in each other's domain.

2.2.4.2 DEFSOC Relation to CFNOC

There is no command relationship between DEFSOC and CFNOC. DEFSOC provides support to CFNOC but does not play an active role in cyber defence. CFNOC relies on DEFSOC's support for incident reporting and service management, such as software update, hardware upgrade, etc. Since the split of DEFSOC from CFNOC there hasn't been a true relationship between the two units. Their roles are fairly distinct, and their activities are coordinated (prioritized, deconflicted, etc.) at the operational level by the DGIMO J3 team.

The following is one easy way to differentiate the mandate of CFNOC from that the DEFSOC:

CFNOC is concerned with "*What is happening **on** the network*"; while

DEFSOC deals with "*What is happening **with** the network*".

2.2.4.3 DEFSOC Relation to JFCCC CCCE

As with CFNOC, DEFSOC does not have a command relationship with JFCCC CCCE, but there is strong collaboration in providing SME support for cyber defence planning purposes.

2.2.4.4 JFCCC CCCE Relation to CFNOC

Even though there is strong technical collaboration with CFNOC, JFCCC CCCE does not have a command relationship with CFNOC. CFNOC supports JFCCC CCCE with SME advice for planning cyber defence for deployed and domestic operations.

2.3 CFNOC Current Operating Concept[9]

CFNOC's essential task is the conduct of DCO-IDM in support of DND/CAF. While the nature of these activities will vary, it is important to note that CFNOC executes its functions under the auspices of Cyber Defence vs. Cyber Security. While the two are tightly linked, there are distinct difference that must be understood by all members of CFNOC and those that interface with the Unit. The implementation, enforcement and management of Cyber Security policy and standards are critical enablers for the effective conduct of DCO. DCO is focused on the continuity of military operations (Mission Assurance) where cyber security is focused on maintaining the confidentiality, integrity and availability of DND/CAF networks through industry best practices.

All of CFNOC's activities and functions can be broken down into one of four phases:

[9] Operating Concept, CFNOC CONOPS, page 3.

Draft

a. Strategic / Operational Guidance and Direction;

b. Prioritization & Planning;

c. Execution; and

d. Reconstitution.

Figure 4 depicts CFNOC's Operating Concept.

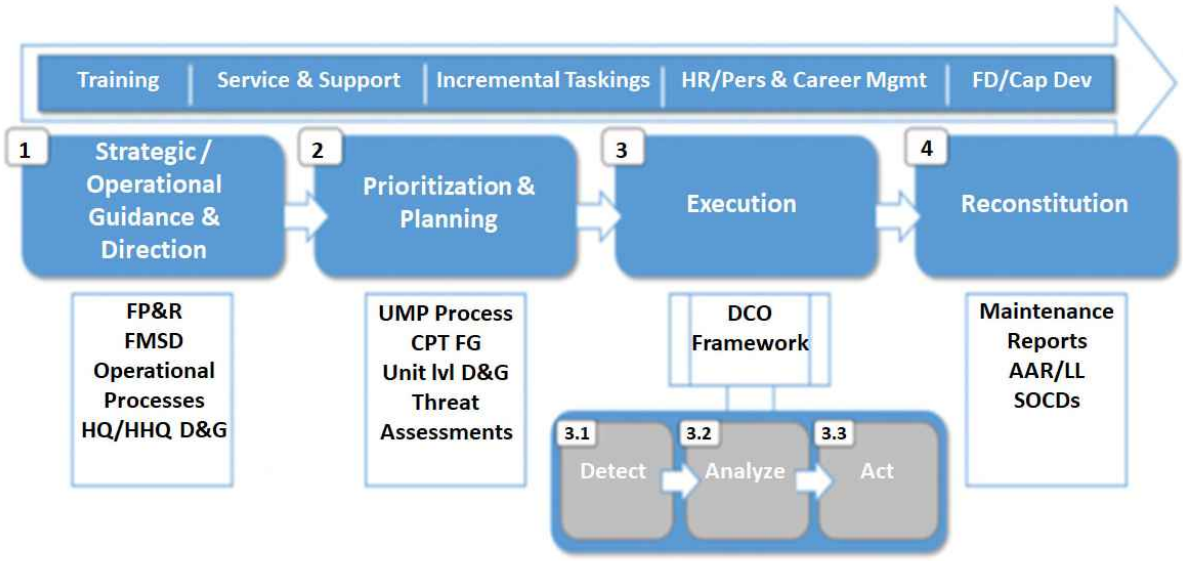


Figure 4 – CFNOC Operating Concept

The execution phase is CFNOC's Center of Gravity (CoG) in the conduct of Cyber Operations and is realized through the application of a DCO Framework. The DCO Framework (illustrated at Figure 5) defines the Concept of Employment for CFNOC Force Elements.

The main input to this stage are tactical level intelligence and desired objectives & effects to enable the execution of DCO by CFNOC Force Elements.

2.3.1 Defensive Cyber Operations Framework

All DCO activities fall into one of the three main phases of the DCO Framework: Detect, Analyze and Act. (See Figure 5).

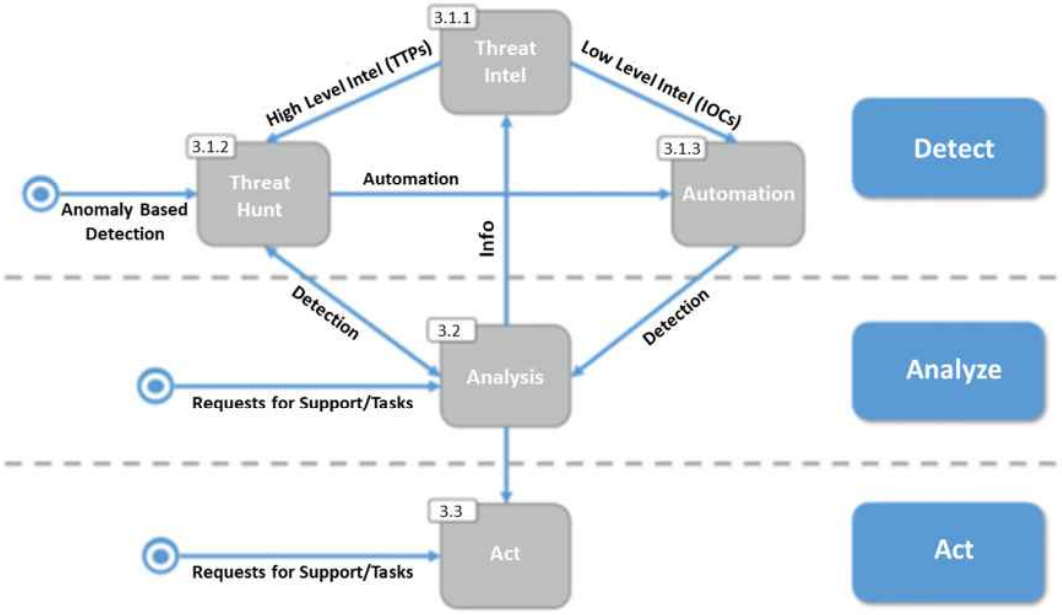


Figure 5 – DCO Framework

2.3.1.1 Detect

The Detect phase incorporates the activities required to collect and disseminate actionable intelligence products to support the discovery of a cybersecurity event leading to the detection of cybersecurity incidents.

2.3.1.2 Analyze

Once Threats have been detected, further analysis is required to provide context to the nature of the threat and equip CFNOC Force Elements with sufficient knowledge to be able to transition into the Act phase. The main activities conducted during this phase are detailed network and host based analysis of detected threats to determine the breadth and depth of the compromise, including detailed malware analysis and forensic investigation of impacted end-points.

2.3.1.3 Act

Once Force Elements have sufficient knowledge about the nature of detected threats, they are then postured to act upon them. The nature of this response is primarily derived through the sequence of Operations Orders and the inherent objectives and effects that are to be achieved. Typical DCO-IDM activities that encompass this phase are:

a. Incident Response;

b. Deception Operations;

c. Fixing Operations; and

d. Reporting.

Draft

2.4 Organizational Interactions and Intelligence/Information Exchange

Exchange and sharing of intelligence/information by CFNOC's various teams with stakeholders is crucial to the success of defensive cyber operations.

2.4.1 Cyber Defence Operations (CD Ops) Team

Cyber Defence Operations (CD Ops) coordinates DND/CAF DCO and incident response with organizations internal and external to the department. CD Ops provides SA through reporting and coordinates the efforts of CFNOC's various teams in the event of a cyber event or incident.

2.4.1.1 CD Ops Team Key Activities

Key activities performed by CD Ops include:

a. Coordination with External (to CFNOC) Organizations on Cyber Events;

b. Coordination within CFNOC on DND/CAF Cyber Events; and

c. Weekly Briefing to CDS and CJOC.

2.4.1.2 Interaction and Int / Info Exchange with Stakeholders

CD Ops interaction and Intelligence (Int) / information (Info) exchange with stakeholders:

a. Providing SA and requests higher authorization from CFIOG;

b. Exchanging reports to FVEYs daily/weekly;

c. Collaborating with CSIS as required per tasking;

d. Receiving advance intelligence reports from CCCS;

e. Receiving alerts, notifications of action is taken (e.g. patches applied) from SSC – Government of Canada – Computer Incident Response Team (GC-CIRT);

f. Receiving alerts from Public Safety – Canadian Cyber Incident Response Centre (CCIRC) on activities of interest to DND/CAF (e.g. unusual DND Internet Protocol (IP) address accessing external networks); and

g. Also exchanging incident information with NATO Computer Incident Response Capability (NCIRC).

See Figure 9 in Annex A for a graphical representation of the CD Ops Team's interactions and Int / Info exchange with stakeholders.

2.4.1.3 CD Ops Team Workflows

The three workflows used by CD Ops are also presented in Annex A, and consist of:

Figure 15 – CD Ops Cyber Event Coordination Workflow;

Figure 16 – Cyber Event Management including with FVEY on Pegasus through Defence Computer Incident Response Team (DCIRT); and

Figure 17 – Cyber Information and Management Workflow.

Draft

2.4.2 Cyber Threat Intelligence Cell (CTIC)

The Cyber Threat Intelligence Cell (CTIC) currently operates 8/5 (with a surge capability) to provide proactive and reactive intelligence to enhance cyber defence operations. The main focus is regarding CAF systems that are vulnerable, valuable to an adversary and critical to deployed Ops and the daily conduct of operations. The CTIC's main objectives are as follows:

a. Understand DND /CAF 's critical ITI and their vulnerabilities;

b. Understand adversarial Tactics, Techniques and Procedures (TTPs) and intent as they pertain to these vulnerabilities;

c. Mitigate residual risk to DND/CAF systems in a proactive manner, by providing advice to system administrators and engineers; and

d. Reduce response time in case of compromise, by creating a response strategy based on understanding of DND/CAF's networks and their adversaries' actions.

2.4.2.1 CTIC Key Activities

The key activities performed by CTIC involve:

a. Intelligence Decision Support to cyber operations – CTIC applies conventional intelligence processes (e.g. Intelligence Preparation of the Operational Environment (IPOE)) to address cyber domain and provide intelligence and priorities to commander's decision support;

b. Emerging Threat Awareness – CTIC needs to stay current on open source cyber intelligence and develop awareness of threats, identify patterns, and require access to historical data for trends; and

c. Tactical Threat Assessments (with JFCCC CCCE) – CTIC prepares tactical threat assessments as required, usually only when equipment is being deployed into a theater of operations. This is done in conjunction with the work done by JFCCC CCCE (formerly known as the Joint Cyber Operations Team (JCOT)) at CJOC.

2.4.2.2 Interaction and Int / Info Exchange with Stakeholders

CTIC's interaction and Int / Info exchange with stakeholders include:

a. Providing intelligence that may influence future Ops to CFNOC Operations Officer (Ops O);

b. Providing intelligence reporting and intelligence priorities to CD Ops, also receiving tasking from CD Ops;

c. Refining Treat Risk Assessments (TRA) and provides to JFCCC CCCE; however, will receive JFCCC CCCE's mission assessment for analysis;

d. Exchanging intelligence with and reporting to the Canadian Forces Intelligence Command (CFINTCOM) – Cyber team;

e. Providing intelligence to SSC and receives threat information from SSC for SA;

f. Providing weekly briefings on incidents / threats on GC networks and receiving threat information for SA from Public Safety-CCIRC;

Draft

g. Requesting expertise from CCCS, at the same time receiving alerts, notification for vetting; and

h. Although not formalize, but also sharing information with Joint Signal Regiment (JSR) to prepare equipment and deployment.

A graphical representation of CTIC's interactions and Intelligence / Information exchange with stakeholders is available in Annex A at Figure 10.

2.4.3 Incident Handling (IH) Team

The CFNOC Incident Handling (IH) Team, in accordance with IMS 6003-1-1, performs the national incident handling leadership role as part of the established framework for a coordinated enterprise approach. IH team is the central point of contact for reporting and handling all information systems security incidents. For further information on the activities of CFNOC IH, refer to ref. N.

2.4.3.1 IH Team Key Activities

The key activities performed by the Incident Handling Team include:

a. Reporting and Handling of all information systems security incidents – Not all incidents handled by IH are cyber incidents. IH relies on the Information Systems Security Officers (ISSO) to perform their duties on site to identify incidents and alert IH. ISSOs are generally not full time positions, and more often than not, ISSO duties are not their first priority; and

b. ISSO Training, which is critical to ensure compliance and identify incidents.

2.4.3.2 Interaction and Int / Info Exchange with Stakeholders

IH Team interaction and Int / Info exchange with stakeholders include:

a. Providing incident reports to CD Ops and receiving tasking from CD Ops;

b. Receiving intelligence reports from SSC;

c. Receiving incident reports from units / bases / wings ISSOs;

d. Providing intelligence to the National ISSO and CAF Elements ISSOs for mitigation and training purpose;

e. Informing Chief of Defence Intelligence (CDI) national special centre of any IT security incident initiated by IH and affecting sensitive compartmented information;

f. Reporting immediately to Director General Defence Security (DGDS) for all security breaches, security violations or attempts to penetrate security measures of highly sensitive info or classified equipment;

g. Providing incidents to CCCS; and

h. Providing medium to high risk incidents to DIM Secur; also receiving tasking from DIM Secur.

A graphical representation of the IH Team interactions and Int / Info exchange with stakeholders is available in Annex A at Figure 11.

Draft

2.4.3.3 IH Team Workflows

The IH Team principal workflow is presented in Annex A and consist of:

> Figure 18 – Incident Handling Workflow – DND Information System Security Incident Management Process.

2.4.4 Surveillance Team

The Surveillance team conducts network traffic analysis of DND/CAF networks in order to identify potentially compromised devices for further investigation. The schemes of maneuver include signature-based detection of known threats (commercial and custom signatures), and anomaly-based identification of previously unknown threats. The Surveillance team participates in maintaining the networks' robustness, allowing CAF to maintain cyber superiority within the CAF Cyber AOR.

2.4.4.1 Surveillance Team Key Activities

Key activities performed by the Surveillance team include:

a. Security Monitoring of Previously Identified Threats, e.g. threats provided by subscription services, or by other know sources;

b. Network Anomaly Detection & Identification Research – Network traffic anomaly will trigger analysis that may involve other CFNOC teams, e.g. to access historical records to explain traffic patterns to determine if the anomaly can be explained; and

c. Technical Assistance Visit (TAV) participation – Together with Reconnaissance (RECCE) and Forensic, Surveillance provides support to TAVs.

2.4.4.2 Interaction and Int / Info Exchange with Stakeholders

Surveillance Team interaction and Int / Info exchange with stakeholders:

a. Providing to CD Ops returns and self-generated surveillance reports for triage and distributing to units as required; also receiving tasking from CD Ops;

b. Consulting and using CCCS tools in order to gather better intelligence data;

c. Receiving guidance from Military Police (MP) on the legal matters;

d. Continuously exchanging information with the National Counter-Intelligence Unit (NCIU), Canadian Forces National Investigation Service (CFNIS) and SSC-GC-CIRT;

e. Receiving tool support from DIMEI 3-5 to ensure all the systems are up-to-date;

f. Continuously collaborating and exchanging information with CTIC, RECCE and Forensics teams; and

g. Receiving in-house capabilities and data collection from the Enterprise Intrusion Detection System Support Team (EIDSST).

A representation of the Surveillance Team's interactions and Int / Info exchange with stakeholders is available in Annex A at Figure 12.

Draft

2.4.4.3 Surveillance Team Workflows

The two workflows used by the Surveillance Team are presented in Annex A and consist of:

Figure 19 – Assessment of Known Threats Workflow; and

Figure 20 – Assessment of Unknown Threats Workflow.

2.4.5 Reconnaissance Team

RECCE Troops provide 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. Security Posture Assessments (SPA) are tailored to client's requirements and information systems and are performed under strict supervision. RECCE Tp provides a final report and, if required, a briefing of specific recommendations on how to improve the client security posture based on the findings of the assessment.

2.4.5.1 RECCE Team Key Activities

Key activities performed by RECCE team include:

a. Asset Discovery (to provide SA and information on a given network (including Operating System (OS), ports and services running on each host, etc.);

b. Targeted Scanning (to confirm compliance for SA&A purposes, and on-going SA in support of missions);

c. Vulnerability Assessment (to validate implementation of DIMEI Security Engineering Validation (SEV) testing recommendations, and on-going continuous SA of DND/CAF networks to verify security recommendations have been implemented);

d. Penetration Testing – To determine the feasibility of a particular set of attack vectors; Identify risk levels from executing several low risk vulnerabilities executed in a particular sequence; identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software; assess the magnitude of potential business and operational impacts of successful attacks; test the ability of network defenders to successfully detect and respond to the attacks; and provide evidence to support increased vigilance in IT security posture of DND/CAF systems;

e. Opposing Forces (OPFOR) in exercises; and

f. (*Not a current capability*) Red Teaming.

2.4.5.2 Interaction and Int / Info Exchange with Stakeholders

RECCE Team interaction and Int / Info exchange with stakeholders:

a. Receiving tasking from CD Ops, at the same time providing back alerts;

b. Consulting with CTIC for input;

c. Exchanging suspicious activities, analyzing of TAV traffic and advising on specific tasks with Surveillance Team;

Draft

d. Providing tasking to RECCE detachment;

e. Providing TAV – After Action Analysis to Forensics Team;

f. Requesting specific vulnerability scans from the Enterprise Vulnerability Assessment Support Team (EVAST);

g. Providing an assessment and recommendations to "Clients", while also exchanging information related to network vulnerability requests; and

h. Receiving Penetration Testing (Pen Test) results on SEV Classified Test and Development Centre (CTDC) from DIMEI SEV.

A representation of the Reconnaissance Team's interactions and Int / Info exchange with stakeholders is available in Annex A at Figure 13.

2.4.5.3 RECCE Team Workflows

The RECCE Team utilises multiple workflows as presented in Annex A. These workflows consist of:

Figure 21 – Asset Discovery Workflow;

Figure 22 – Target Scanning Workflow;

Figure 23 – Vulnerability Assessment Workflow;

Figure 24 – System/Network Penetration Test Workflow; and

Figure 25 – Test Emulation Workflow.

2.4.6 Forensics Team

The Forensics Team provides specialized digital analytical services to DND/CAF. It also provides technical analysis of new cyber threats and malware techniques used by adversaries to penetrate DND/CAF networks. In addition to malware analysis, the Forensics section is responsible to maintain and collaborate with other agencies in regards to cyber security events.

2.4.6.1 Forensics Team Key Activities

Key activities performed by Forensics are identified in Table 3.

Table 3 – Forensics Activities

Image Data Capture (e.g. capture data from affected devices)	
Full Disk Image:	A physical (exact, sector by sector copy of a media device) or logical (all active data on a logical partition – no deleted files) image of the original storage media.
Removable Media Image	A physical (exact, sector by sector copy of a media device) or logical (all active data on each partition – no deleted files) image of the original media device.

Draft

Mobile Device Image	Recover/find documents, images, videos, contact information and possible email information, location information may be possible depending on the type of acquisition of the mobile device.
File / Folder Capture	Exact, unchanged copy (where applicable) of the files and/or folders from the original media.
System-Event Analysis	
Antivirus Scan with Latest Updated Antivirus Engines	Scans run on media using at least 5 of the engines listed: • Symantec endpoint protection • Avast • Avg • Kaspersky • McAfee • Avira
Operational Security (OPSEC) Investigation	• Improper use of admin accounts • Password complexity • Poor recycling practices (reusing a system without proper imaging, cleansing, etc.)
Perform Offline Vulnerability Investigation	• Check nodes for specific vulnerabilities • Verify best security practices
Malware Analysis	
Antivirus Scans	Determination if the file is malicious or not. Comparison against good/bad hash values (if applicable).
Dynamic Analysis	Listing of changes made to the system to include items such as changes to the file system, registry, network connections, etc., and create signatures for further detection.
Static Analysis	Reverse engineer to determine potential capabilities as well as identify obfuscation and encryption techniques to include to develop tools for encryption C2 channels as well as develop signatures for detection.
Review Firmware Logs	

Draft

Configuration File Analysis	• Determine details for general information and if the firmware itself is encrypted or not • Comparison of manufacturer supplied firmware and firmware supplied for analysis
Full Firmware Image Analysis	
To Include Malware Analysis on Multiple Files Found on a Single Source	A list of all files from the provided media with a true or false answer as to whether or not malicious, if malicious detailed output could be provided as per a normal malware analysis investigation per malicious file.
Transmission Security (TranSec) Analysis	
Caveat / Keyword Scan	Identification of files/folders with specific caveat or containing specific keywords. Caveat list to be provided by customer.
Removable Media Usage	List of files associated with device, including method and timeline of transfer (where applicable).
Network Share Access	Determination of access to specific network folders/files including date, time, user account, changes to those folders/files.
Incident Prevention Research	
Incident Mitigation Recommendations	

In addition to the services listed in the Forensic Service Catalog, the team provides mitigation recommendations and research capabilities for threat prevention.

2.4.6.2 Interaction and Int / Info Exchange with Stakeholders

Forensics Team interaction and Int / Info exchange with stakeholders:

a. Receiving tasking from CD Ops, but also providing back reports on incidents and tasking;

b. Providing information collections, which were sent by the Cyber Defence Immediate Response Team (CDIRT) to assess situation and acquire artifacts, to DND Units per tasking;

c. Providing technical assistance to RCMP (Technical Crime section) through NCIU on rare occasion;

d. Providing assistance to CCCS on Software (SW) and Hardware (HW) analysis on rare occasion;

e. Collaborating with SSC-Forensics, CFNIS and NCIU on all forensics cases; and

f. Participating in exercises with Allies 2-3 times per year.

A representation of the Forensics Team's interactions and Intelligence / information exchange with stakeholders is available in Annex A at Figure 14.

2.4.6.3 Cyber Protection Team (CPT)

During incident response and analysis, security engineers have a requirement to go onsite and capture large data sets from networks under investigation for offline analysis without producing indications that the network is under analysis. DND forensics and incident response teams are required to travel to remote locations to preform onsite data acquisition and local analysis of forensic information in order to provide DND chain of command information about the systems affected and assess the impact to the environment.

2.4.7 Enterprise Intrusion Detection System Support Team

The Enterprise Intrusion Detection System Support Team (EIDSST) is responsible for providing 24/7 support of the following:

a. Configuration, testing and deployment of various Intrusion Detection Systems (IDS) and analytical tools on CFNOC IDS sensors / servers for all CAF monitored networks;

b. Configuration, testing and deployment of various IDS sensors / servers on all networks;

c. Patching and upgrades of the IDS suites, as required; and

d. HW/SW support and maintenance of the IDS HW (securityOnion, Sourcefire, and CFNOC purpose-built).

2.4.7.1 EIDSS Team Key Activities

Key activities performed by EIDSST include:

a. Enterprise IDS tools deployment / maintenance – Includes configuration, testing and deployment of tools on sensors, deployment of sensors, and HW/SW maintenance); and

b. IDS capability development (Note: some Commercial off the Shelf (COTS) tools do not provide required data for deep-dive analysis, EDISST will develop in-house tools to support specific needs).

2.4.7.2 EIDSST Workflows

The EIDSS Team utilises two distinct workflows as presented in Annex A. These workflows consist of:

Figure 26 – Enterprise Intrusion Detection System (IDS) Workflow; and

Figure 27 – IDS Capability Development Workflow.

Draft

2.4.8 Enterprise Vulnerability Assessment Support Team

The Enterprise Vulnerability Assessment Support Team (EVAST) performs vulnerability and risk management on selected networks using IP360. EVAST scans the network with specific profiles at regular intervals (three times per year, plus one unscheduled scan) and on an as required basis. EVAST processes the scan reports to identify vulnerabilities and issues EITSM tickets for actions.

2.4.8.1 EVAS Team Key Activities

Key activities performed by EVAST include:

a. Performing routine scans on DND/CAF networks – On CSNI, routine scans are done three times a year, plus one unscheduled scan, looking for bad passwords, outdated patches, inactive / old applications that should have been removed, etc.;

b. Processing scan reports and identifying vulnerabilities – To eliminate false positives, then group similar cases together and issue an EITSM ticket for action;

c. Generating EITSM tickets to respective IT support teams for action; and

d. Updating historical databases for all scan reports.

2.4.8.2 EVAST Workflows

The workflow used by EVAST is presented in Annex A at Figure 28 – Enterprise Vulnerability Assessment Workflow.

2.5 Training Development – Skillsets, Roles and Cyber Exercise Opportunity

Cyber Operators are the backbone of the cyber force. They are the personnel, at all rank levels, with the primary role to "*conduct defensive cyber operations, and when required and where feasible, active cyber operations. They liaise and work collaboratively with other government departments and agencies, as well as with Canada's allies to enhance the Department of National Defence (DND) and the Canadian Armed Forces (CAF) ability to provide a secure cyber environment. They monitor CAF communication networks to detect and respond to unauthorized network access attempts and provide cyber support to meet the operational requirements of the Navy, Army, Air Force, and joint enablers.*"[10] Cyber Operators are not IT technicians and cyber forces are not the IT staff.

Cyber Operators conduct defensive cyber operations, and when required and where feasible, active cyber operations. They liaise and work collaboratively with other government departments and agencies, as well as with Canada's allies to enhance DND/CAF's ability to provide a secure cyber environment. They monitor CAF communication networks to detect, analyze and respond to unauthorized network intrusion attempts and provide cyber support to meet the operational needs of the Navy, Army, Air Force, and joint enablers.

Cyber Operators are not to be confused with Aerospace Telecommunications and Information Systems Technicians (ATIS), Army Communication and Information System Specialists

[10] Canadian Armed Forces Career website – Cyber Operator Overview, https://forces.ca/en/career/cyber-operator/

Draft

(ACISS), Naval Combat Information Operators (NCIO), and Naval Communicators (NC). These military occupations are primarily concerned with the setup, installation, operation and maintenance of communications networks and ITI while Cyber Operators are more concerned with protecting these networks from hostile threats and denying the use of cyberspace by hostile forces. That said, given their knowledge of cyber threats and methods of attack, Cyber Operators are often consulted by ATIS, ACISS, NCIO and NC personnel during the setup, installation, operation and maintenance stages of communications networks and ITI to support improved security measures and establish better defensive postures. In addition, it is imperative that routine and enterprise IT service activities be fully integrated with cyber force activities to ensure efficient cyber operations and reduce the potential for collateral cyber damage.

2.5.1 Cyber Operator Skill Sets

The Canadian Forces School of Communication and Electronics (CFSCE) in Kingston, Ontario is the designated school for the Cyber Operator trade training. Certified Cyber Operators affected to CFNOC are subjected to an On-the-Job Training (OJT) program complemented by industry provisioned specialized courses geared to the individual's role and progression.

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 offensive cyber operations, including cyber exploitation measures, cyber-attack and cyber fires;
e. Principles and techniques in defensive cyber operations, including internal defensive measure8.5s and response actions (RA); and
f. Tactics, techniques and procedures for:
    i. Cyber support coordination, command and control,
    ii. Cyber reconnaissance,
    iii. Cyber surveillance,
    iv. Cyber Forensics,
    v. Cyber threat analysis, and
    vi. Cyber security operations centre functions.

2.5.2 Roles of the Cyber Operator (Tiers 1, 2 and 3)

2.5.2.1 Junior Analyst

The Primary Role of a Tier 1 Cyber Operator is to work within a Cyber Defence Operations Centre to detect and track the activities of Cyber Entities within the tasked Area of Cyber Operations (AoCO) with a view to classifying entities as: Human or Non-Human, Friendly, Enemy, Other. When required, a Tier 1 Cyber Operator may be tasked to participate in Cyber

Draft

Reconnaissance, Surveillance, Forensics, Threat Intelligence, Cyber Exploitation or Attack Measures, Cyber Fires and Cyber Countermeasures tasks. When required, the Tier 1 Cyber Operator may be tasked to support the design, development and implementation of new or refined TTPs and cyber tools for Cyber Reconnaissance, Surveillance, Forensics, Threat Intelligence, Cyber Exploitation or Attack Measures, Cyber Fires and Cyber Countermeasures tasks.

2.5.2.2 Intermediate Analyst

The Primary Role of a Tier 2 Cyber Operator is to work within a Cyber Defence Operations Centre to attain an accurate characterization of detected Cyber Entities by any act or means so that high confidence, real-time decision, including weapons engagement, can be made. When required, a Tier 2 Cyber Operator may be tasked to participate in Cyber Reconnaissance, Surveillance, Forensics, Threat Intelligence, Cyber Exploitation or Attack Measures, Cyber Fires and Cyber Countermeasures tasks. When required, the Tier 2 Cyber Operator may be tasked to support the design, development and implementation of new or refined TTPs and cyber tools for Cyber Reconnaissance, Surveillance, Forensics, Threat Intelligence, Cyber Exploitation or Attack Measures, Cyber Fires and Cyber Countermeasures tasks.

2.5.2.3 Senior Analyst

The Primary Role of a Tier 3 Cyber Operator is to work within a Cyber Defence Operations Centre to guide and direct the actions of Tier 1 and Tier 2 operators to complete the analysis of the Cyber Operational Situation with a recommendation regarding appropriate Cyber Exploitation or Attack Measures, Cyber Fires and Cyber Countermeasures. When required, the Tier 3 Cyber Operator may be tasked to plan, lead and execute detailed Cyber Reconnaissance, Surveillance, Forensics, Threat Intelligence, Cyber Exploitation or Attack Measures, Cyber Fires and Cyber Countermeasures tasks. When required, the Tier 3 Cyber Operator may be tasked to design, develop and implement new or refined TTPs and cyber tools for Cyber Reconnaissance, Surveillance, Forensics, Threat Intelligence, Cyber Exploitation or Attack Measures, Cyber Fires and Cyber Countermeasures tasks.

2.5.3 Collective Training Exercises

Generally speaking, CFIOG and CFNOC specifically, have taken a mentoring role in cyber collective training activities. While not all training opportunities are listed herein, the argument is made that the formation is decisively involved in cyber exercise opportunity:

a. UNIFIED RESOLVE;
b. VILGILANT SHIELD;
c. ENTERPRISE CHALLENGE;
d. FABRIC SABRE;
e. STEADFAST COBALT;
f. COALITION WARRIOR;
g. CYBER COALITION; and
h. UNIFIED VISION.

Draft

Note that the main deficiency / roadblock to conducting individual and collective training is the lack of a virtual training environment at level II and level III.

Draft

3 JUSTIFICATION AND NATURE OF CHANGE

3.1 Drivers for change

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. CFNOC analysts are currently 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 (air gap) data from one tool to another, fill in forms and submit search queries or upload artifacts for analysis and storage. The CD-DAR capability can automate 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; cyber 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 currently being done manually and is prone to mistakes by analysts. DND/CAF are dealing with increasingly aggressive threats, such as ransomware[11], 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 capability will automatically provide context to alerts and add key information to enable automated or, at least, easier and faster manual triage.

CFNOC will leverage the CD-DAR capability to reduce the time required to train new cyber analysts. Automation removes the need for the analysts to know the details of which manual steps should be followed for each scenario. Knowledge is stored and managed within the CD-DAR capability and will help to reduce a 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 solutions will combine the functionality of existing and new tools, providing an integrated COP reducing the need to train every security analyst on each individual tool.

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 available to investigate these events to protect the IT network’s integrity. As a result, DND is increasingly challenged to remain up-to-date on this ever-changing front. Coupled with the current out-of-date and inefficient cyber defence capabilities, DND/CAF security and defence remain

[11] Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

vulnerable to an ever-increasing cyber threat significantly elevating the risk to missions and operations.

3.2 Description of Desired Changes

The DND/CAF lack a comprehensive cyber security system to meet the demands of DCO in contested cyberspace and to maintain corporate and operational effectiveness. DND/CAF relies on stand-alone unintegrated tools and dated, manual processes for cyber defence that are unable to fully respond to the ever growing and diversifying cyber threats. Without the CD-DAR capability, DND/CAF face increasing frequency of significant degradation to its ability to defend its C2 networks, which will negatively impact operational capabilities and potentially affect the safety and security of Canada and Canadians at home and abroad.

DND/CAF commanders and operators require an integrated cyber defence system that provides cyber situational awareness and the ability to respond to hostile and systematic threats from nation-states, organized crime syndicates and terrorist groups.

The functionality CD-DAR project will deliver is defined by the capability gaps, which are deficiencies in or a lack of, are listed and described below along complete with references to the High Level Mandatory Requirements (HLMR) (Section 4.2) that will address them.

3.2.1 Network Discovery

Software flaws and improper configuration of information system components are major vulnerabilities of information systems that allow for system exploitation. The SANS Institute, a respected and internationally renowned security research and training organization, with the participation of the National Security Agency (NSA), and other United States (US) national and international organizations maintains a report on the Top Critical Security Controls for Information Systems.

The top four controls consists of:

a. Inventory of authorized and unauthorized devices;

b. Inventory of authorized and unauthorized software;

c. Secure configurations for hardware and software on mobile devices, laptops, workstations and servers; and

d. Continuous vulnerability assessment and remediation.

In order to protect a network there must be a complete inventory, and their respective interconnections, 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 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. CFNOC is called upon to respond to incidents on non-enterprise systems they have no knowledge of, where 50% - 60% of the available information requires validation, for which Requests for Change (RFCs) are either outdated or unavailable. Software such as Nessus, Cyber Information and

Draft

Incident Sharing System (CIICS), and Malware Information Sharing Platform (MISP)[12] have been found to be capable of providing a solution but are not used in a cohesive fashion. The CD-DAR capability will find the best possible answers, ensure network discovery platforms are interoperable and cover the full range of product design capabilities. While some of this information is currently available, CD-DAR will provide a common, actionable repository. **Capability gaps identified under Network Discovery are addressed by HLMRs 1, 7 and 8 (Section 4.2).**

3.2.2 Trusted Database Repository

DND/CAF lacks a trusted Cyber Database Repository (CDR) that acts as the authoritative cyber entity and event data warehouse for the DND/CAF cyberspace. A CDR that holds all data relating to the collection/inventory 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, collection and analysis of logs and other data from organization networks, and other cyber security tasks. The database includes a large degree of automation, all industry standard report generation, query and graphical analysis tools.

The CTIC provides proactive and reactive intelligence to enhance DCO. To conduct analysis it must draw data and information from different systems and sources of information than span from unclassified to Top Secret security levels or caveats. Currently, the National Data Transfer Centre within the Strategic Joint Staff (SJS) 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 capability and limits how the information is stored and transferred for cyber intelligence purposes. Hence, there is a need for CDR to also gather, store and maintain 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.

The CDR consolidates information from existing tools and products that are not interoperable, and enables more global correlation for various Cyber Defence activities. It is the core component to build a modular, flexible, agile and interoperable DCO capability. A central repository that will enable Commanders to make informed decisions for required effective defensive actions. **Capability gaps identified under Trusted Database Repository are address by HLMRs 1, 2, 3, 4 and 6 (Section 4.2).**

3.2.3 Common Operating Picture (COP)

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 (Cyber-BMC), more frequently referred to as Cyber – COP. A COP is a shared, dynamic and interactive visual representation of operational

[12] 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.

information gathered from various sources that can be tailored to facilitate situational awareness, collaborative planning and decision-making. In addition, a Cyber-BMC needs to enable commanders to identify, monitor, characterize, track, locate, and take action in response to cyber domain activity in near real-time, as it occurs both globally and within AORs.

Current DND/CAF capabilities lack a central view to represent the state of the cyber environment or to assess the impacts of cyber activities. These capabilities are insufficiently integrated, lack responsiveness and are considered inadequate in providing operational information to support effective command decision-making processes. A COP should be malleable and attuned to each Commander and staff's needs whether Strategic, Operational or Tactical. CFNOC currently utilizes a home-grown software tool with no leeway in operational views to consolidate information for the commander. Moreover, this tool is ineffective for on networks that are disconnected, intermittent and unreliable, or that offer limited capacity (episodic) environments. Hence, CD-DAR will need to maintain situation awareness, through a COP, of alerts, threats, and remediation across the DND/CAF Command Network, and feed situational awareness to processes for decision on, and execution of, responses through standardized interfaces and supporting automated workflows for decision support to the command element, and the implementation of responses as directed. **Capability gaps identified under Common Operating Picture are addressed by HLMRs 1, 2, 4 and 6 (Section 4.2).**

3.2.4 Human Factors

The CD-DAR capability will address two distinct human factor aspects. The first being that, too much specialization is required from cyber analysts and the second, their cognitive overload. CD-DAR will provide integrated cyber defence solutions that will ease the burden of manually comparing information from one tool to the output of another. This will reduce the detailed knowledge and specialization required to become proficient with the various cyber defence tools. Moreover, automation of network security data / information collection, analysis, and correlation from multiple information sources (GC and Allies) will ease Cyber Operator's cognitive overload by plummeting the volume of manual threat detections and identifications. 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 Comd-Net, detect threats and predict the evolution of attacks that would be impossible to do using manual approaches. These security analytics will be stored in the CDR to enable sharing within the cyber security community, and include:

a. Integrated threat intelligence that looks for known bad actors by leveraging global threat intelligence;

b. Behavioural analytics that applies known patterns to discover malicious behaviour; and

c. 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 gaps identified under Human Factors are addressed by HLMRs 2, 3, 5, 6, 8 and 9 (Section 4.2).

Draft

3.2.5 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[13] environment where forensics can perform analysis and investigate while simultaneously allowing the physical hard drive to be wiped clean. Where equipment is geographically dispersed without on premise 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 procedures from taking place and potential evidence from being reviewed. By CD-DAR allowing forensics to be conducted immediately and remotely, without having to ship equipment across the country, DND/CAF will realize economies in time and money, with minimal impact to ongoing operations. **Capability gaps identified under Capability to Conduct Forensics are addressed by HLMRs 2, 3, 4, 5, 6 and 9 (Section 4.2).**

3.3 Priorities among Changes

Under Treasury Board's *Policy on Government Security*, the GC is consolidating its efforts to combat cyber threats. Cooperation and coordination between various government departments are on-going and DND/CAF will continue to be an active participant, including through the CD-DAR project.

Explicitly, CD-DAR project aligns with Initiative #65 in SSE to *"…assume a more assertive posture in the cyber domain by hardening our defences, and by conducting active cyber operations against potential adversaries in the context of government-authorized military missions*." The CD-DAR project will deliver on this SSE commitment by delivering cyber capabilities to support military operations by protecting critical military networks and equipment from cyber-incidents. More specifically, the new capability will replace current manual processes and multiple non-integrated systems with an integrated, modular and scalable solution that ensures interoperability with OGDs and allies. The new capability will consist of hardware, software, and associated operational processes.

Moreover, the CD-DAR project is aligning with the comprehensive and well-defined National Institute of Standards and Technology (NIST) Cyber Security Framework, which provides guidance and a set of standards for recommended security controls for information systems at federal agencies. NIST standards are based on best practices from several security documents,

[13] 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.

organizations, and publications, and are designed as a framework for federal agencies and programs requiring stringent security measures.

In addition to SSE initiative #65, CD-DAR strategically aligns and is supported by the following:

a. Delivers on IM Gp Cyber Programs Departmental Results Framework (DRF) 4.6.1 with the outcome of having fully capable and interoperable DCO capabilities in support of the CAF operations at the strategic and operational levels;

b. Aligns with the C4ISR Strategic Vision, Goals and Objectives as this project will contribute to secure and defend cyberspace for the CAF; and

c. Follows the Defence IM/IT functional planning guidance, specifically the objective where the department is investing in technology that can quickly identify and address IT security vulnerabilities and threats.

Draft

4 CD DAR SYSTEM OVERVIEW

4.1 Operational Objectives (business outcomes)

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

a. Communicate to stakeholders involved in cyber operations the process to be followed for Cyber threat capture, analysis and mitigation;

b. Determine the overall effectiveness of cyber operations through the rapid integration of situational awareness, understanding and action across network operations and cyber operations activities;

c. Implement a robust collection architecture that captures pertinent network flows and security events across the in-scope network infrastructure;

d. Develop a Cyber-BMC, commonly referred to as COP, integrated with the DND/CAF JBMC which combines SA of all CAF missions and operations Force Elements;

e. Rapidly detect changing attack vectors ranging from application through physical attacks;

f. Prioritize threat disposition through a centralized cyber security engine that provides advanced correlation functionality, near real time threat identification, and advanced analytic capabilities;

g. Correlate asynchronous sensor alerts into behaviour patterns;

h. Recognize anomalous behaviours in real time;

i. Skillfully apply advanced autonomous decision support tools, with Artificial Intelligence (AI), designed to provide faster and richer threat mitigation tactical direction;

j. Rapidly respond to the threat, events and incidents with automation and orchestration technology at its core;

k. To have the right processes and people in place to address the threats;

l. Research these attacks and share them with colleagues, both nationally and internationally;

m. Gauge performance through meaningful metric information and Key Performance Indicator (KPI)-driven measurement tools driving continuous improvement; and

n. To ensure lessons learned are captured and/or applied.

4.2 High Level Mandatory Requirements

The CD-DAR solution will provide defensive cyber capabilities to monitor and defend the in scope DND/CAF networks, and will provide capabilities, in the form of hardware, software,

Draft

training etc. in line with the High Level Mandatory Requirements (HLMRs), which address existing capability deficiencies. The established HLMRs are identified in Table 4 below.

Table 4 – CD-DAR HLMRs

HLMR	Short Title	Description
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 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 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 analysis 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.

HLMR	Short Title	Description
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.

4.3 Operational View (OV-1)

DND/CAF aims to achieve a security architecture with a cohesive design that ensures the confidentiality, integrity, and availability throughout the enterprise and aligns mission objectives and risks. Security is a process which includes People, Technology and Operations (processes). Integrating People, Operations and Technology requires a holistic approach that will allow DND/CAF to measure their security goals with a security maturity model – the NIST Cyber Security Framework (CSF) of Identify, Protect, Detect, Respond, and Recover for describing and building out the security architecture, its governance and for aligning Information Assurance (IA) security controls.

The DND/CAF security architecture will provide a means of automating cyber hygiene, including the Center for Internet Security's Critical Security Controls. The CSF is used to cover the breadth of cybersecurity objectives, while not being overly detailed. It is critical for a security architecture to maximize network visibility in order to support DCO in an efficient and effective manner. This includes having visibility of the network, data and endpoint layers and the choices of tools will make sure those are sufficiently represented.

DND/CAF, like most large enterprise organizations, are transforming legacy infrastructures with the addition of new initiatives like cloud computing, big data analytics, mobility and Internet of Things (IoT) applications. All of these changes present a number of network security challenges. DND/CAF need an interoperable and integrated network security architecture that is more threat-centric, offers scalability, automates manual processes, and replaces state-of-the-art tools with interoperable network security services. The DND/CAF security architecture includes centralized C2 via CFNOC, asset management, distributed detection and enforcement, information sharing, actionable intelligence and restorative services. It needs to address many factors that include, but are not limited to, efficiency, availability, elasticity, flexibility, resiliency, scalability, and capacity. The security architecture should also allow for the replacement of solutions to adopt new emergent technologies like a resilient security defined platform, Quantum computing based AI and analytics, smart security data, cognitive / sentient security analytics and offensive cybersecurity as they become available.

The Operational View – 1 (OV–1) presented at Figure 8, developed in accordance with the DND and Canadian Forces Architecture Framework (DNDAF), is a high level operational concept graphic which highlights the main aspects of the CD-DAR architecture and provides a description of both internal and external influences.

Draft

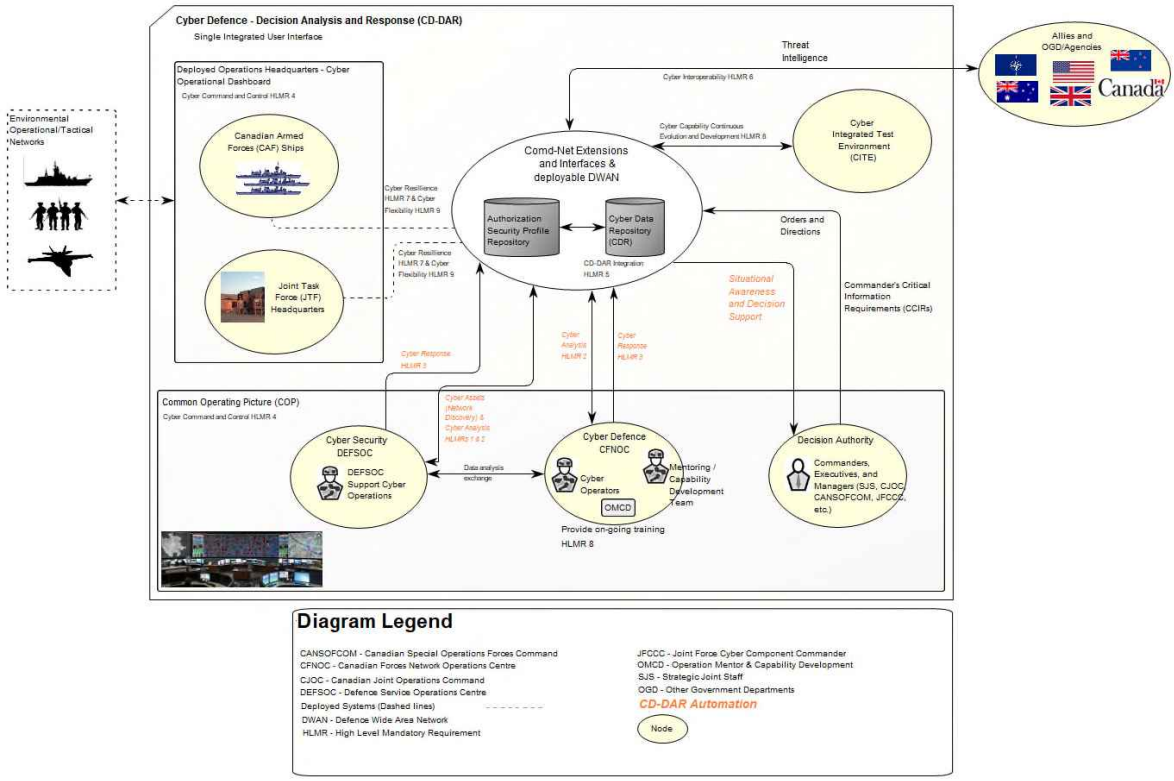


Figure 6 – High Level Operational View (OV-1)

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

The current concept of operations sees all Cyber Operators and other users (managers, executives, commanders and their staffs) perform their tasks through a single integrated environment. These tasks include, but are not limited to: workflow, monitoring, analysis, alerting, reporting, SA, response actions and training (individual and collective). Each Cyber Operator is presented with a common dashboard visualization tool, tailorable to their specific roles and responsibilities. Personnel such as departmental executives, commanders, managers and other elements of the DND/CAF network operations community (such as the Royal Canadian Navy (RCN), the Royal Canadian Air Force (RCAF), the Canadian Army (CA), CJOC, Canadian Special Operations Force Command (CANSOFCOM) and the SJS) would be similarly enabled with rights and privileges to information and actions based on their designated and assigned roles within DND/CAF DCO; most likely accessing cyber defence related information with JBMC, which integrates all aspects of an operation. The Canadian Surface Combatant, the ship currently being acquired by the RCN to replace the Halifax Class frigates which can be tasked to operate Joint Task Force Headquarters (JTF HQ), will be equipped with a CD-DAR capability to monitor and defend its own networks and that of deployed forces reporting to the maritime JTF HQ. Details will be further defined in the CD-DAR Project Definition Phase.

Other key aspects of this high level operational view (OV-1) include:

a. **Shared Threat Intelligence:** Threat intelligence is a significant form of information that influences both DND/CAF's security and defence posture and that of its partners;

b. **Authorized Data:** The ability to identify acceptable information in DND/CAF's cyberspace is a prerequisite to detection and response to unacceptable situations. For example, defining Authorized devices must be defined before unauthorized devices can be detected and dealt with; and

c. **Automation:** A key objective of CD-DAR is to maximize automation of DND/CAF's security and defence posture. Significant operational effort will be required to digitize shared threat intelligence from multiple partners with information received in various machine-readable and manual formats.

4.3.1 Operational Environment, Interoperability, Flexibility and Resilience

The CD-DAR capability will provide Cyber security and defence capabilities wherever Comd-Net Extensions and Interfaces, and deployed DWAN systems are accessible. This impacts the following environments:

a. **Enduring Environment**: This includes domestic and international locations where a full suite of support infrastructure is available as well as full connectivity to support 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**: Since most DND/CAF engagements will 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 capability will also address the need to handle information across various security domains and caveats; and

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 target 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.

Draft

4.3.2 Cyber Security and Defence Staff

DND/CAF cyber security and defence staff, most being at CFNOC, should be organized using security analysts, data scientists, tool developers and threat hunters. Security Analysts work inter-departmentally to identify and correct flaws in the DND/CAF's security systems, solutions, and programs while recommending specific measures that can improve the overall security posture. Data Scientists make use of data analytics, statistical testing, data mining and AI – Machine Learning / Deep Learning (ML/DL) to derive insight from big data. Tool developers create custom dashboards to improve cyber SA, adapters to ingest and convert unstructured to structured data and scripts to automate routine tasks and operations to increase efficiency. Threat Hunters use Analysis of Competing Hypotheses (ACH) methods for proactively and iteratively search through networks and datasets to detect threats that evade the existing security infrastructure.

Deep Learning

"an AI function that mimics the workings of the human brain in processing data for use in detecting objects, recognizing speech, translating languages, and making decisions. Deep learning AI is able to learn without human supervision, drawing from data that is both unstructured and unlabeled."

Investopedia, Nov 24, 2020

4.4 CD DAR Operating Model

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, while it is expected that several integrated Cyber security tools will be necessary to fulfill the CD-DAR requirements, the key functional elements sought may be functionally represented as follows:

a. An ability to maintain Cyber SA, through a Cyber Common Operating Picture (COP), of alerts, threats, and remediation across the DND/CAF Command Network, and to feed SA to processes for decision on, and execution of, responses through standardized interfaces and supporting automated workflows for decision support to the command elements, and the implementation of responses as directed.

   The COP is malleable and attuned to each commander's needs whether strategic, operational or tactical. It provides leeway in the operational views to consolidate information for commanders. It also operates on networks that are unavailable, unreliable, providing local cyber environment SA, or that have limited capacity (episodic) environments;

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"

Defence Terminology Bank, Record #21880

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

Draft

interoperated with applications and a trusted repository) into the assigned Command Network as one cohesive system. The CDR will also comprise data collections from multiple sources, enabling analysis across a diverse set of datasets, including access to network logs which can be enriched with data sources, including data from the ITSM / DEFSOC, Configuration Management Database (CMDB), SSC, Public Safety, Security Technical Implementation Guides (STIG), Baseline Configuration, and other network operations sources;

c. An ability to perform automated or on demand discovery of cyber entities and events to rapidly identify and track all assets (authorized and non-authorized) connected to Command Network and assess their attributes for vulnerability, configuration, risk and patch compliance;

d. An ability to perform automated cyber security monitoring to rapidly identify the presence of non-compliant cyber entities or behaviours, events, alerts, vulnerabilities, or other changes to the status of the entities within the DND/CAF cyberspace;

e. An ability to perform 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;

f. An ability 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;

g. An ability to perform automated task management to adaptively and dynamically identify, contain and eradicate a threat; and

h. An ability to utilize an integrated operational training system 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:

   i. Operational Threat, Penetration and Attack simulation capability to exercise the Cyber Operator team and evaluate its operational readiness and effectiveness,

   ii. Training focussed on individual operators (task, roles and advancement in role),

   iii. Skills training and validation for Cyber Operators and non-Cyber Operators, and civilians, in their assigned roles, individually and collectively, and

   iv. Collective training for the cyber security and defence operations capability. It is a replication of the set of operation systems with offline datasets allowing complete range of functionalities and running realistic scenarios for training purposes.

4.4.1 Cyber Common Operating Picture (COP)

The COP is the main interface that Cyber Operators, Managers, Executives and Commanders will use to operate the CD-DAR capability. The prerequisite to gaining access to CD-DAR is to obtain verified credentials. Once credentials are verified, users will have a shared, dynamic and

Draft

interactive visual representation of cyber operational information gathered from various sources that can be tailored to their respective roles and needs to facilitate situational awareness, collaborative planning and decision-making. The COP will allow users to detect, analyze, and monitor cyber threats, produce reports, send and receive notifications from OGDs, allies and 3rd party partners, manage threats, events and incidents, and execute responses. The COP also provides situational awareness of the assets, their security and connectivity status. Their status includes the ability to discover authorized and unauthorized cyber entities.

Cyber environments security status can be overlaid or included with missions and/or networks COP that enable drill down into the detailed representation of the cybersecurity posture. The COP provides:

a. Tailorable and customizable dashboards – Role based platforms;

b. An ability for time based analyses to detect threats and changes to the environment over time;

c. An ability to push fused information and actionable intelligence down, including to the tactical edge;

d. An ability to push fused information up to improve decision making and provide status of information of adversary networks; and

e. An ability to update security policy and threat intelligence based on attacks detected across the network to be able to protect systems from adversary TTPs.

4.4.1.1 Situational Awareness

To improve security situational awareness, better organizations practice real-time Active Cyber Defence (ACD) which is the process of personnel taking an active and involved role in identifying and countering threats to systems. The function of ACD is to provide sensing, sense-making, decision-making and acting in cyber-relevant time in order to provide cyberspace defence before an adversary is able to bring about their desired effect. In contrast, a Passive Defence adds software or hardware to the system for the purpose of increasing security without consistent input from personnel. These are also called proactive versus reactive cyber defences - and good security organizations practice both. ACD makes use of big data analytics, data science, Machine and Deep Learning (ML/DL), AI and many other processes and technologies. These security functions will be centralized at DND/CAF Cyber Security Operations Centre that performs defence against unauthorized activity within Command Network, including monitoring, detection, analysis, and response and restoration activities.

4.4.2 Security Orchestration Automation Response (SOAR)

A Security Orchestration Automation Response (SOAR) platform is used to perform task allocation, work-ticket and workflow management associated with controlling, monitoring and managing work and priorities, and the life cycle of security incidents and operations. Used through the COP by the appropriate Cyber Operators and Managers, SOAR performs the following functions:

a. Provide unified access to the functionality provided by CD-DAR;

Draft

b. **Orchestration** — How different technologies (both security-specific and non-security specific) are integrated to work together:

    i. Organize tasks around the authorities, levels of expertise and working preferences of participating Cyber Operators, commanders, support staff and other roles, and

    ii. Permit concurrent execution of tasks by authorized personnel;

c. **Automation** — How to make machines do task-oriented "human work". Support and promote the most appropriate use of manually-processed, user-triggered and computer-triggered tasks to maximize user productivity;

d. **Incident management and collaboration** — End-to-end management of an incident by people. Permit authorized and concurrent access and execution of tasks locally, nationally and internationally, including locations under disadvantaged conditions; and

e. **Dashboards and reporting** — Visualizations and capabilities for collecting and reporting on metrics and other information.

4.4.2.1 Response Actions

The final step in any cyber-attack is to limit and repair the damage and close the intrusion. This can involve manual actions (e.g., restoring data and systems from a reference point, reconfiguring the firewall, whitelists and/or blacklists) or automated action, such as shutting down a service or network link using prepared scripts, traditional network management tools or advanced Software Defined Networking (SDN). As noted, the Decision Layer retrieves prior responses for similar anomalies. The system will present options. As the system is operated over time, the library of code for preprogrammed automated and semi-automated (i.e., man-in-the-loop) responses will be expanded, particularly when SDN is adopted. The Action Layer will constitute a library of scripts (playbooks) that affect the decision.

4.4.2.2 Incident Response (IR) Management

Incident Response (IR) managers need to be able to prioritize and focus on the critical events teams encounter every day. They need help coordinating and informing interdisciplinary teams that include members from other stakeholder organizations. When an event becomes a crisis, the IR team needs to be able to quickly and accurately answer questions while focusing on solving the problem at hand. Furthermore, they need comprehensive reporting and analysis functions that turn data into actionable information that drive responses and process improvement. They need capabilities such as, but not limited to:

a. Timeline features that provide a sophisticated, flexible and customizable view of pending and completed tasks that provides valuable insight status which in turn may be used to drive accountability;

b. Customizable dashboards to provide graphical ways to access and visualize and convert data to actionable information; and

Draft

c. Analytic dashboards presenting impact-based metrics across the organization – they help organizations measure the impact of security operations on mitigating risks or improving security postures.

An Incident Response platform helps resolve incident response challenges such as, but not limited to:

a. Understanding both internal and external threats;

b. Building a standard, documented and repeatable IR plan;

c. Proactively test and improve IR processes;

d. Leveraging threat intelligence;

e. Streamlining incident investigation, triage and response including maintaining legal chain of custody to recover data;

f. Managing and tracking the status in real-time of any incident including major ones in order to report and brief the Commander, interested groups and 3rd parties on the most current status;

g. Orchestrating and automating IR across people, process and technology involving multiple systems or accounts;

h. Incorporating Dynamic Risk Assessment and Risk Management into the process;

i. Protection against unauthorized whitelist changes, unauthorized software installation and blockading unauthorized software execution by device;

j. Documentation of how to correct a vulnerability;

k. Automatic installation of patches for all products and systems;

l. Administer security events to involve access based on trust level authorization, facility access and system level access via key training authorization and key credential authorization requirements and on correction of security-related behaviour deficiencies via automated security checks;

m. For file security conditions, enforcement of specified file types and protection to the confidentiality, integrity, and authenticity of data at rest, in transit, or in process via cryptography;

n. For anomalous activities, Endpoint Detection and Response (EDR) capabilities to respond to the installation of malware in the form of Advanced Persistent Threat (APT) on an endpoint device; and

o. Response actions will be reported on a standard, tailored, scheduled, on-demand and event-driven basis. Information on when threats have been detected for the first-time and the time to remediation information will be provided accordingly.

Key features of an IR platform are to provide Courses of Action (COAs) to help orchestrate solutions using workflows and to provide playbooks that automate responses.

Draft

4.4.2.3 Automated Policy Generation

CD-DAR learns the normal behaviour of DND/CAF systems and automatically generates or updates security policies when it discovers abnormal behaviour that has never been previously detected. The operator can choose to deploy the policies to some or all of the distributed agents, which can then take the appropriate actions, including to local end point security or network wide security enforcement.

4.4.2.4 Dynamic Defensive Cyber Operations Playbooks

Playbooks specify and automate the detailed steps, guidance or best practices for dealing with findings, while at the same time ensuring cohesive experience across teams. CD-DAR will include a pre-defined set of playbooks that can be shared amongst OGD and allied partners, and the ability to customize existing or create new ones. These playbooks can adapt to real time incident conditions to keep pace with continuously evolving complexity and sophistication of APT or adversary TTPs.

Dynamic DCO playbooks enable a level of incident response far beyond that of traditional static ones. They orchestrate people, process, and automate technology where it makes sense to empower and augment Cyber security analysts, making them faster, more efficient, and more effective. Dynamic DCO playbooks support driving down the Mean-Time-To-Remediation without sacrificing accuracy.

As incidents progress, CD-DAR re-evaluates the response plan, automatically enriches incident data, and adds or removes tasks to ensure the plan is appropriate for the incident. With Dynamic Playbooks, CD-DAR can automatically change the response plan based on threat intelligence and re-categorization of the incident.

Before an analyst even opens an incident, repetitive initial steps to triage, assign, and enrich incidents intelligently are already completed. Dynamic playbooks automatically retrieve information from connected systems, and then use that information to change ownership, enrich artifacts, and ensure analysts have relevant data at their fingertips.

4.4.2.5 Visual Playbook Editor

Cyber security analysts in organizations are the experts who know the organization's data driven, intelligence-based processes and what actions to take. A Visual Playbook Editor (VPE) provides easy to use wizards for analysts to create or customize DCOs playbooks based on their day to day data-driven processes, to create prescriptive analytics that can automate evidence-driven decisions and orchestrate automated courses of action in the organization's cyber ecosystem. The VPE allows both developers and non-developers to easily build and customize complex DCOs playbooks using the drag-and-drop feature – the VPE automatically generates all supporting code in real time.

4.4.3 Operational Training

CD-DAR operational training will be a key artifact to train and on-board new CD-DAR capability users. The objective of CD-DAR operational training is not to generate new Cyber Operators, but rather to instruct trained Cyber Operators on how to effectively and efficiently use CD-DAR to achieve DND/CAF DCO missions and operations. Access to CD-DAR functionality being role-based, commanders, executives and managers will fittingly gain the requisite

Draft

knowledge in using the CD-DAR capability commensurate to their respective DCO roles and responsibilities. Recurring CD-DAR operational training will be integrated to the Cyber Operator training program. Refer to Paragraph 4.7.2.4 for details regarding the training environment.

Initially a trainee will be exposed to simple scenarios with a limited amount of data to observe and a limited amount of actions to take, but as they gain expertise the training system will be able to increase the granularity of the data and actions accordingly. Keeping the user incentivized to train more frequently and with a purpose to continuously learn new skills regardless of their current skill level and to increase the speed of their Cyber Observe, Orient, Decide and Act (OODA) loop to make it faster than the attacker's is definitely a challenge.

4.4.4 Cyber Security Monitoring

CD-DAR will continuously monitor the network 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.

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 are performed through CD-DAR. Cyber security monitoring will implement the first five (5) Centre for Internet Security Critical Security Controls (CSC), through interactions with CDR. These minimum essential CSCs are:

a. Inventory of authorized and unauthorized devices;
b. Inventory of authorized and unauthorized software;
c. Secure configuration of end-user devices;
d. Continuous vulnerability assessment and remediation; and
e. Controlled use of Administrative privileges.

CD-DAR will, as much as possible, automate the detection and identification of threats, the conduct of analysis necessary to determine the type of threat, the development and recommendation of the best COA to support Commanders' decisions and selecting the proportionate measures to deal with such threat. This cyber response development lifecycle is duly represented in Figure 7 below. CD-DAR also alerts and reports changes to the baseline to DCO staff and helps them assess changes and anomalies to the system.

Draft

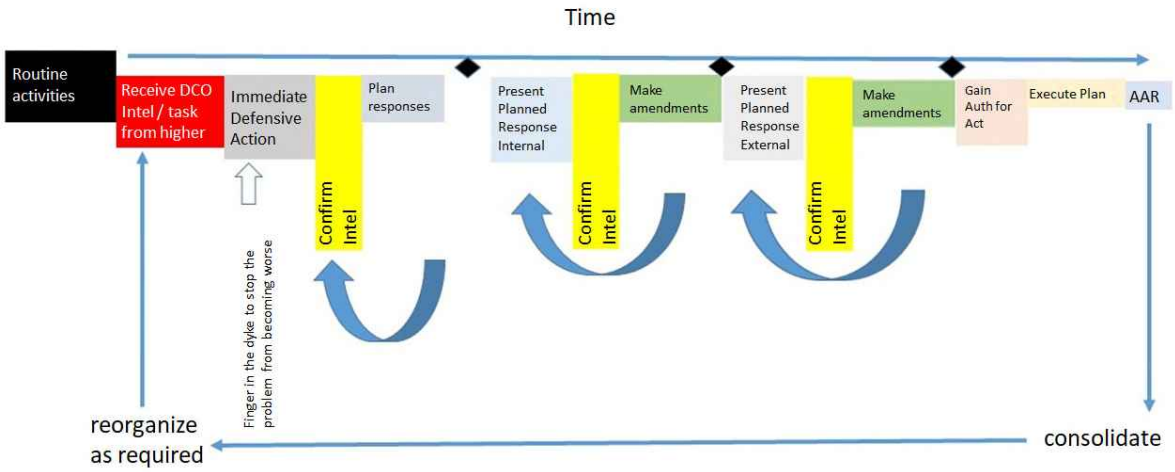


Figure 7 – Cyber Response Development Lifecycle

4.4.4.1 Machine Learning (ML)

A key function of cyber security monitoring is the ability to suggest COAs for countermeasures based on the threat being analyzed. Data on events / anomalies are presented to cyber analysts for analyses and to initiate remediation actions. ML can be incorporated in two ways – detection and response. In detection, anomalies may be real problems and require action or simply identify unusual behaviour. Behaviour which is deemed anomalous but not malicious is used to update the classification in the supervised machine learning analytical engine. This helps to refine the classification and reduce the number of false positives, where "positive" in this sense means the assertion of anomalous behaviour. In response, the user is encouraged to record the analysis they perform in response to a similar anomaly (i.e., a report from the same analytical app and/or network link, component, or computer application) and what action was taken. The analysts or an automated system can then consult the record of prior responses to accelerate the determination of future responses.

A machine learning analytics engine that learns the normal behaviour of the systems over time and correlates events from various sensory domains together to establish a baseline of the system. The continuous supervised machine learning is augmented with inputs from human operators to add to the accuracy of the engine.

4.4.4.2 Asset Management

CD-DAR requires operator and machine-to-machine interfaces to access information in the CMDB (integrated within CDR if a DND/CAF CMDB does not exist by the time CD-DAR delivers its capability). This includes the ability to populate the CMDB and retrieve information for use by other applications and platforms. The CMDB is 'the source of ground truth' for the network. It contains the list of all authorized hardware and software components, and authorized configurations. Populating it is both a manual and automated process with as much as possible being done with automation through both passive and active means as part of Asset Discovery. Active means can include an agent that runs on the client or agentless. Agentless combines active system scans, both non-credentialed and credentialed scans with passive ones that monitor network traffic to fingerprint the devices and components using advanced analytics including

Draft

ML. Some legacy equipment may be too fragile or not support active means. Manual information like system owner, and their contact information, location, and date of last audit are examples of attributes that must be entered manually. CD-DAR also needs the ability to manually override or enter all the information that is normally populated through automated means. For example, a Commander may accept the risk of deviating from an entity's approved configuration for operational imperatives. In such situations, CD-DAR must be able to recognize the deviation as an authorized configuration for the specific entity to alleviate false alerts, or that the system automatically change the specific entity back to its original configuration.

4.4.4.3 Compliance Management

Where technical security controls are in place, the Cyber Operator must be able to quickly and easily report out on the entities' compliance status across any compliance standard, whether for daily reporting or to meet an auditor's or executive's request, via the Cyber Common Operating Picture. This functionality will allow a Security Officer to identify compliance gaps, and monitor their remediation.

4.4.4.4 Vulnerability Management

Software and configuration vulnerabilities can be compared to standard configuration hardening guides such as STIGs and Centre for Internet Security Benchmarks, which can be done automatically using vulnerability scanners. However, these scanners are unable to detect hardware vulnerabilities or other broad classes of vulnerabilities (e.g., architectural, people, trust relationships).

When it comes to vulnerability management, security practitioners continue to struggle to identify which of hundreds and even thousands of vulnerabilities in their network are actually putting them at risk. Traditional approaches don't take into account all the risk factors and other mitigating security controls when prioritizing risk. This leaves security teams without a good understanding of how their network and threats impact system risk potentially wasting resource and effort on issues attackers may never find or want to exploit. A typical vulnerability management workflow: Detection – Prioritization – Remediation – Track/Monitor.

CD-DAR's vulnerability management capability will include functionalities such as, but not limited to:

a. A single pane of glass to view the cyber environment's entire risk profile, including vulnerabilities and potential attack vectors in an interactive visual model;
b. Reduce patching needs by pinpointing imminent threats to the mission;
c. Collaboration with DEFSOC to use efficient patching alternatives, improve mitigation and remediation techniques, and report patching status / completion; and
d. Automate tracking, analysis and communication of risk assessment progress.

4.4.4.5 Expected and Unexpected User behaviours

4.4.4.5.1 Identity and Access Management

Today's mission success is dependent on the secure availability of software resources, including applications, data, and other services. Identity and Access Management (IAM) processes and

Draft

solutions are the first line of defence for ensuring secure access to network hardware and software services.

A good IAM solution makes use of Role-Based-Access-Control (RBAC) and Least Privilege, but can also provide full service identity management (for example Google's model), isolate, monitor, record and control privileged sessions on critical systems, databases, virtual machines, containers and others.

CD-DAR will assess and remediate expected and unexpected behaviours and intrusions in real-time. It will do this by learning the normal behavioural patterns of each network, device or user, correlating the data to spot deviations that indicate real-time threats or attacks and quarantining and/or remediating them. It will use the latest classified and unclassified cyber threat intelligence in conjunction with machine learning to evolve and learn attack patterns. The real-time outputs will be used to remediate threats before adversaries achieve their objectives.

State-of-the-art behavioural detection is done with big data analytics on virtual machines with scalable processing resources in both computing power and memory. Refer to Paragraph 4.6.2 for more information on big data analytics.

4.4.5 Cyber Defence Analysis and Decision Support

A new and innovative approach to cyber defence operations is required, one that ties preventing security incidents into detection and response that spans people, process and technology elements that is more focused on operational relevance, reducing adversary dwell time and impeding their progress, and speeding incident response activities. It needs to create a more dynamic environment that methodically and aggressively drives active investigations for intrusions by continuously updating security detection controls with new threat intelligence (received from OGDs, Allies and Industry partners) with active real-time searches augmented by searches over historical data for intruder activity.

The aim is to unify and integrate a holistic approach to cyber security that significantly reduces operational cyber risk exposure. It allows for constant automated improvement of security controls and enables the sharing of other organizations hunting procedures and partial automation to gather information for human review, and as warranted approval from senior leadership or a local commander.

Initially, Cyber analysts will still be 'in-the-loop' with regards to making decisions and executing COAs. As AI technologies improve, people will transition to 'on-the-loop' with regard to verifying and validating the automated analytics, decision-making (identification and selection of viable COAs), and response execution. Corrections to the automation are captured and used as feedback to increase the accuracy and efficiency of the DCOs. These help security analysts to augment and even automate their understanding of a threat, making them smarter about the latest attacks and freeing them up to focus on other priorities. CD-DAR will continuously self-tune to reduce the number of false positive and false negative alerts.

4.4.5.1 Security Monitoring

CD-DAR will support continuous monitoring of the network security posture, to get a clear visual picture of the organization's security risk exposure by using a comprehensive dashboard, views with key and impact-based security metrics, key performance metrics, static and dynamic thresholds, and trending indicators.

Draft

The security monitoring engine will allow to quickly gather and link multitudes of information from different devices in the cyber environment, such as end points, network devices, etc., to make risk-based decisions on whether to elevate an alert of interest to an incident, which will kick off the incident response process. It will allow for better tracking of single events that may not warrant further review, but when looked at in combination with other events of interest using big data analytics, the single event may warrant further investigation. This allows the correlation and predictive analytics, including behavioural across the entire Cyber Kill Chain to reduce and identify “false negatives” which do more damage than the “false positives”.

4.4.5.2 Cyber Threat Hunting

Cyber Threat Hunting consists in proactively and iteratively searching through networks to detect and isolate threats that evade existing security solutions and establish persistence in networks. Hunting analysts have to rely on manual or computer-assisted techniques, as opposed to automated detections from security tools such as Security Information and Event Management (SIEM). Hunting has two main goals: 1) improve automated detection and response by modelling new ways of detecting malicious activity and then turning those models into new and effective detections and responses using orchestration and automation; and 2) force network intruders to be as close to 100% perfect 100% of the time to keep persistence in the networks.

Effective and efficient hunting requires analysts with a mix of skillsets and experiences that are applied in a systematic way to detect and eradicate malicious and persistent threats from the network. Threat hunters must place themselves in the same frame of mind as the attacker, meaning that they know what to look for based on what would be done next if they were performing the attack. Therefore, hunting analysts need to be offensively trained. Threat hunters ought to collaborate with qualified incident responders who know how to rapidly take action to contain an attack.

The output of the hunt ends with the creation, documentation and typical automation of repeatable procedures/playbooks.

4.4.5.3 Endpoint Detection and Response

CD-DAR will enable DCOs to achieve comprehensive endpoint visibility, improve their ability to detect malicious activities and simplify security incident response. Endpoint agents are usually integrated with big data analytics, threat intelligence and security monitoring platforms. Endpoint agents support the ability to collect endpoint telemetry data such as running processes, registry settings, files currently opened, active network connections, hardware details like current Central Processing Unit (CPU) and memory usage, and user accounts in use, etc. for big data analytics processing. The endpoint agents will also support response actions and the ability to collect forensic data like memory or hard drive images and files to support forensic investigations.

4.4.5.4 Threat Intelligence

Threat Intelligence (TI) is defined as evidence-based knowledge, such as context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the response to that menace or hazard.

Draft

Qualitative types of TI focus on providing newsfeed-like services on the campaigns, tools, techniques, and motivations of attackers. Conversely, quantitative sources – blacklists of domains Uniform Resource Locators (URL), IPs, TTPs, location-based mitigation, protocol anomaly-based filtering, malformed packet removal including malicious payloads and rate limiting (to gracefully manage non-malicious demand spikes) – are usable in real-time by monitoring systems and help detect and block activity with known bad sites.

Various sources of TI include both classified and unclassified government variants (e.g. the Department of Homeland Security (DHS) Enhanced Cyber Security Services (ECS) and Automated Indicator Sharing (AIS)), Open Source, paid commercial feeds, and custom developed TI from industry.

The following Use Cases describe some of the ways CD-DAR will utilize Threat Intelligence:

a. **Curated Intelligence** – Turn threat data into TI through context and automatically prioritize based on user-defined scoring and relevance;

b. **Attack Trends** – Investigate attacks and track over time using the data to improve DND/CAF's defensive posture and DCO;

c. **Intelligence Pivoting** – Utilize campaign, malware and indicator knowledge to identify related attacks and adversaries that may affect missions and operations;

d. **Investigations** – Support scoping and remediation by correlating artifacts of an investigation with a threat library of related indicators and context;

e. **Threat Hunting** – Empower Cyber Operators to proactively search for malicious or anomalous activity that has not yet been identified by DND/CAF automated security tools;

f. **Improve Incident Response** – Gain global visibility into adversary TTPs to improve remediation quality, coverage, and speed;

g. **Strengthen Security Appliances** – Make security tools (e.g., firewall, Intrusion Detection Systems (IDS), SIEM, etc.), sensor and other devices smarter with the most accurate and relevant threat data; and

h. **TI Efficacy –** Retrospectively evaluate the accuracy, speed and relevance of TI sources versus the relevance of their information to incidents experienced.

4.4.5.4.1 External Threat Intelligence

DND/CAF should use proactive quantitative type feeds, e.g., the Dark Web, to obtain highly valuable threat intelligence, quite often relevant to a broad spectrum of potential targets, both organizations and individuals, otherwise not accessible through conventional monitoring.

Collecting and analyzing available intelligence from the dark web presents a new opportunity to understand and potentially pre-empt attacks. CD-DAR can use this kind of information to quantify risk, and ultimately, determine what actions Cyber analysts might need to take to address them.

Threat intelligence gathered from the dark web is a window into the motivations, methods, and tactics of threat actors. To make the best use of dark web intelligence, DCOs should be alerted

Draft

only when new and relevant information emerges, and be able to quickly determine if what's appeared requires further investigation or escalation to drive more efficient decision making.

4.4.5.5 Cyber Risk Assessment

CD-DAR will use Dynamic Risk Management (DRM) to recommend individual response actions or complete courses of action, and assess their effectiveness, costs and side effects with respect to mission objectives as part of the workflow for incident responses. Adding DRM to the workflow for those incidents that require it (i.e., those that exceed a certain risk score) will ensure that the recommended responses or complete course of action (including assessment of their effectiveness, cost and side effects to the mission objectives) are addressed before the incident proceeds to the next step in the response process. CD-DAR will need to support the automated enrichment of incidents with any available Dynamic Risk Assessment (DRA) information to add context. A flexible framework will allow users to diversify their asset and identity groups such that higher priorities can be placed on those that have a more critical mission impact if compromised.

4.4.5.6 Malware Reverse Engineering

Security analysts reverse engineer malware with the goals of understanding their exploitation techniques, obfuscation approaches, encryption methods, C2 communications, attribution, categorization and clustering and/or many others. Tools necessary to support analysts will be integrated within the Cyber Integrated Test Environment (CITE) Lab (refer to Section 4.7.2.3 for more details), and examples include: Full packet capture (Packet Capture (PCAP), security appliances, big data analytics, etc.); Signature/Pattern matching; Threat intelligence sources; Disassemblers; Emulators/Virtualization; Fuzzing/Symbolic execution; and Sandboxes.

In the future, more AI based approaches will make use of specialized cybersecurity coalitions, resilient security defined platforms, smart security data, cybersecurity intelligent things and cognitive / sentient security analytics.

4.4.5.7 Distributed Denial of Service

CD-DAR will seek to provide the ability to repudiate malicious traffic targeted at an entity (human or non-human) before it goes over the transport network, while still allowing normal network traffic to transit the network to the intended entity and other users/assets, thereby providing network resiliency that allows both the network and intended entity to operate through the cyber-attack with no noticeable performance degradation.

4.4.6 CD-DAR Integration

The Command Network security architecture is composed of many custom and COTS tools and security appliances the CD-DAR Project Prime System Integrator (PSI) will need to integrate in CD-DAR capability. Such tools will be identified in Definition Phase of the project, and may include SIEM products, Threat Intelligence, Threat Hunting, Security Analysts, Data Mining/Big Data, Machine Learning, Malware Analysis tools, Packet Capture, Continuous Integration /

Draft

Continuous Deployment (CI/CD) Pipeline, SecDevOps[14], incident tracking and reporting, security operations platform and others. These tools must provide a mutually supportive architecture that uses common protocol languages like STIX, TAXII and others, but also support scripting tools and automation. Additionally, CD-DAR will need a robust incident tracking capability to support unique network defence requirements such as the following:

a. Allowing consistent and complete information capture across incidents for each state of the incident lifecycle tiers like triage, analysis, response, closure, and reporting;

b. Recording structured information from analysts (incident category, time reported), semi-structured data (impacted users, impacted systems) and unstructured information (analyst narrative), along with time-stamped notes;

c. Protecting sensitive details from constituents, thereby avoiding compromise of any insider threat cases or word getting out about an incident prematurely or to wrong parties;

d. Protecting details about cases even if the general constituency is compromised;

e. Supporting escalation and role-based access control for different sections within the CFNOC/DEFSOC;

f. Supporting long-term trending and metrics;

g. Incorporating artifacts or pointers to artifacts, such as events or malware samples; and

h. Using simulation to practice and debug the workflow and incident response process in the CITE lab that may not contain any security hardware without affecting the metric collection and reporting statistic for the production environment.

4.4.7 Cyber Data Repository (CDR)

The Cyber Data Repository (CDR) acts as the authoritative cyber entity and event data, horizontally scalable data warehouse for the DND/CAF cyberspace. It holds both structured and unstructured data from various existing sources, e.g., DND (ITSM / DEFSOC, CMDB, STIG, and other network operations source), OGDs (SSC, CSE, Public Safety, etc.), allies (FVEYs and NATO partners) or other trusted third-party sources, 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.

All data and 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.

[14] SecDevOps refers to the inclusion of security efforts and best practices into Continuous Integration and Continuous Deployment.

Draft

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.

4.4.7.1 Data Collection

Data collection should not be done in-line with control communications. Packets should be captured, using a dedicated passive capture device, and through a tap into virtualized systems. This passive method means that CD-DAR would not add latency to communications and not constitute an additional attack surface. Sample data sources include:

a. Network Data Plane, e.g., packets, flows, logs, various IDS, etc.;

b. Network Control Plane, e.g., packets, flows, logs, various IDS, etc.;

c. Physical Security, e.g., physical security sensors, Badge access systems, Video, Sound, etc.; and

d. Application Layer, e.g., anomaly indicators in enterprise and networks application data such as image or video data feeds, etc.

4.4.8 Cyber Entity and Event Discovery

CD-DAR will establish and maintain an authoritative cyber entity inventory and configuration database of all cyber entities (hardware and software) within Command Network. In doing so, CD-DAR must have the ability to discover, collect and store all data related to cyber entities and cyber events, and store it within the CDR. This will form the foundational baseline against which CD-DAR will compare new cyber entities, whether authorized or not, and be able to detect malicious attempts to infiltrate DND/CAF networks. Such intrusion attempts can derive from email attachments or small devices with connectivity capabilities. CD-DAR must be able to defend against such attacks, identify the foreign entity and log the intrusion event.

The CD-DAR capability will allow for entity discovery scans to run on a pre-defined routine basis, automatically as the result of cyber entity data modifications, in response to alerts from monitoring systems, or on demand from a Cyber Operator. The system will make use of: 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. Any new cyber entity attempting to access Command Network will be logged and analyzed to determine if it poses any threat. And authorized newly logged entities will be continuously tracked in the CDR and monitored to ensure safe operations for Command Network. The CD-DAR capability will also include provision for exception mechanism to accept legitimate but non-standard changes to ITI assets in the interest of CAF operational primacy.

Regardless of the source, authoritative data will be digitized in a manner that permits CD-DAR information systems to automatically compare actual and authoritative data rapidly enough to detect unauthorized situations within the system effectiveness timelines defined in the CD-DAR Statement of Operational Requirements (SOR).

Draft

4.4.8.1 Asset Discovery

To be an effective DCO, DND/CAF need to know who and what is connected to its network environments, including cloud and on-premises, at all times.

Asset discovery is performed through both active and passive discovery as well as by leveraging agents on the clients where possible. It may not be possible or practical to put an agent on every client (e.g., IoT or legacy device). Agentless asset discovery combines active system scans, both non-credentialed and credentialed scans with passive ones that monitor network traffic to fingerprint the devices and components using advanced analytics, including ML.

Passive scanning uses sflow and netflow data collection of all connected assets as well as their connectivity status to other devices in the network environment. This approach not only identifies known assets, but unknown assets as well.

In addition to asset discovery, adapters will be leveraged to collect system information for validation (compliance) of security patch level and configuration. Network and asset vulnerability scanners and secure configuration tools will be leveraged to manage and monitor the status of the network as devices (hardware and software) are introduced and removed, as well as their configuration on the network that may introduce attack vectors for adversaries.

Network based monitoring of assets as opposed to agent based, ensures that as assets connect to the network they are identified and tagged. Agents on devices enable monitoring of configuration changes and policy violations that cannot be seen from the network. CD-DAR will blend these approaches to provide a holistic view of all assets connected to the network and enable the ability to quickly respond to rogue or misconfigured assets before they expose the entire network to threats.

4.5 Innovation

This section presents concept and technologies the CD-DAR Project is likely to integrate into the capability or consider as a potential evolution during the in-service phase.

4.5.1 Operation Mentor and Capability Development (OMCD)

Typical DND/CAF IM/IT systems are sustained through the procurement of annual hardware maintenance and software licensing fees, perhaps complete with some engineering services performed either by DIMEI and/or contracted to a third party.

CD-DAR is an operational capability comprised of People, Operational (Business) processes and Technology, all of which are equally important. Failure of any one of these components could result in severe impact to mission success. Consequently, the concept of the Operation Mentor and Capability Development (OMCD) emerged, consisting of a small dedicated team of military, public service and cyber operations and technical contracted subject matter experts co-located with the delivered capability. The OMCD will plan and manage the sustainment and evolution of CD-DAR as a capability by:

a. Supporting ongoing cyber security operations and DCO, as required;

Draft

b. Leading and coordinating business modifications/transformation of CD-DAR Cyber security and DCO capabilities towards becoming a NIST[15] maturity level 5 cyber security and defence operational capability;

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

d. Supporting development and coordination of cyber security and DCO individual and collective training;

e. Supporting Cyber Operations exercises and experimentation;

f. Sustaining and evolving the CD-DAR ITI and cyber software tools; and

g. Integrating emerging technologies and best practices.

OMCD will be stood up upon achieving Initial Operating Capability and throughout CD-DAR's in-service phase.

IOCs and IOAs

The difference between Indicators of Compromise (IoCs) and Indicators of Attack (IoA) is that "*IoCs are the traditional tactical, often reactive, technical indicator commonly used for detection of threats while IoA is focused upon attribution and intent of threat actors. Another way to conceptualize this is to focus on WHAT (IoCs) and WHY (IoA) of threat contextualization.*"

OPTIV article by Ken Dunham, Senior Director, Technical Cyber Threat Intelligence, 24 January 2019

4.5.2 Big Data Analytics

The volume of security alerts, logs and packets necessary to effectively conduct DCO missions is growing at an exponential rate. The task of detecting anomalous or suspicious network activity has become significantly more challenging, particularly across multiple security domains in DND. Sophisticated and automated analysis is required to efficiently deal with the high volume, high velocity, and high variety of data sources. In addition, this capability may replace or augment the expensive SIEM tool currently used by CFNOC, as it potentially offers greater capabilities than SIEM.

A foundational tenancy for performing analysis of cyber security events is to ensure that traffic records that might be relevant in a cybersecurity context are considered, even when it may require ingestion of large volumes of network events. By recording every action as it takes place, Indicators of Attack (IoAs) show exactly how an adversary slipped into the monitored environment, accessed files, dumped passwords, moved laterally in the network, and perhaps eventually exfiltrated data. IoAs represent a proactive stance in which DCOs are looking for early warning signs that an attack may be underway, such as code execution, persistence, stealth, C2, and lateral movement within a network. Indicators of Compromise (IoCs) include hashes or

[15] National Institute of Standards and Technology (NIST), https://www.nist.gov/.

[16] IoC and IoA: Indicators of Intelligence, OPTIV article by Ken Dunham, Senior Director, Technical Cyber Threat Intelligence, 24 January 2019.

C2 domains or IP addresses which are constantly changing. Because IoCs represent reactive methods of tracking malicious activity, there is a good probability that the network has already been intruded upon by the time the intrusion is detected. In contrast, IoAs are a series of actions that an adversary must conduct in order to succeed; therefore, IoAs are more amenable to discovering the adversary's TTPs. By monitoring these large volumes of data, gathering the indicators and analyzing them, one can determine how a threat actor successfully gains access to the network, and its intent can be inferred. Thus, no prior knowledge or threat intelligence of the specific tools or malware (IoCs) are required to stop the attack while it's still in progress. In fact, IoAs can detect fileless malware or zero day attacks.

4.5.3 Artificial Intelligence

The CD-DAR capabilities will employ advanced security analytics that go far beyond the signature-based approaches currently being used. *Machine Learning* and *Deep 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 may include, but not limited to:

a. Integrated threat intelligence that looks for known bad actors by leveraging global threat intelligence;

b. Behavioural analytics that applies known patterns to discover malicious behaviour; and

c. Anomaly detection using statistical profiling to build a historical baseline to provide alerts on deviations from established baselines that conform to potential attack vectors.

4.5.3.1 Self-Healing Network[17]

Network self-healing is when network problems are resolved without the need for humans to get involved, where a network automation tool can detect and remediate outages, failures, and breaches. Self-healing typically happens through a network monitoring alert triggering some sort of corrective action on the network. [18]

Complex Wide Area Network (WAN) environments such as Command Network, in multiple locations, both enduring and deployed, can overwhelm IT teams. In such environments, even centralized management systems can be too slow and too cumbersome to see and respond to the demands of large numbers of cyber entities (hardware, software and human).

DND/CAF rely on some automation to ensure reliable connections and dependable Defence – Virtual Private Network Infrastructure (D-VPNI) connections, especially since the COVID-19

---

[17] Using AIOps to Enable Self-Healing SD-WAN, by Nirav Shah, NetworkWorld, Dec 8, 2020, https://www.networkworld.com/article/3600139/using-aiops-to-enable-self-healing-sd-wan.html

[18] The Benefits of a Self-Healing Network, by Kevin Jackson, August 29, 2017, https://www.helpsystems.com/blog/benefits-self-healing-network.

pandemic began. However, the system still relies on a team of administrators and systems analysts to keep everything running efficiently, and that approach is neither scalable nor sustainable.

DND/CAF need a solution that can both detect and respond to any sort of impairment, anywhere on the Command Network, and that requires more than simple automation. Leveraging Artificial Intelligence Operations (AIOps) to infuse machine learning into IT operations increases the level of automation. Such a system can automatically observe granular application performance, monitor transactions, and apply big data analytics to make sophisticated decisions, ensuring the best possible connection—combined with the ability to make critical changes when needed to maintain operational supremacy. Adding AIOps enables automatic detection and response across all connections, not only to identify issues, but to also remediate them in real time—before an application or user is impacted. It is also able to learn traffic patterns and then make real time decisions and recommendations to optimize the network based on those patterns.

An integrated AIOps system is able to consume and process large data sets to detect even minor WAN impairment and then introduce a sensible response to protect application performance, ensuring the application is available to users whenever they need it. The result combines reliability, connectivity, application prioritization, and performance Service Level Agreements (SLA) with WAN impairment functions to normalize, balance, or correct traffic, creating a self-healing WAN solution. Metrics achievable through the use of Machine Learning include:

a. Precision = $\frac{\text{Total number of true positive predictions}}{\text{Total number of predictions}}$

   The larger the number of false positives, the less precise the system is;

b. Recall = Total number of true positive predictions made from the total number of true positives present in the population/collection.

   The larger the number of false positives, the smaller the Recall;

c. Mean Time to Detect (MTTD); and

d. Mean Time to Respond (MTTR).

CD-DAR is the centralized management console to visualize and orchestrate connectivity, as well as manage advanced routing and security functions, all through the same pane of glass. When CFNOC is optimized with its own AI, it will be able to sift through mountains of data provided by individual AI-enabled devices to see, detect, and respond to anomalies and threats.

4.6 In Service Support (ISS) Environment

As of the time of writing of this version of the CONOPS, the CD-DAR CONSUP has not yet been updated, nor have the below identified responsible organizations for each level of support been conferred with or confirmed.

This section describes at a high level the roles and responsibilities of support organizations at each level of support. Further details are provided in the CONSUP.

Draft

4.6.1 1st Level Support

4.6.1.1 National Service Desk and Service Management Centres (SMCs):

4.6.1.1.1 Roles & Responsibilities

Once end users contact the Service Desk, it makes perfect sense that the Service Desk attempts to collect as much information and diagnostics about the incident as possible, and even resolves the issue on the spot, if possible. This will reduce resolution time for all minor incidents, and first-contact resolutions consequently increase end user satisfaction.

The 1st Level Support staff will be managed by the Service Desk Supervisor, who will also serve as the escalation point, if needed. If 1st Level Support is not able to resolve the incident right away, it will escalate the incident to 2nd Level Support.

4.6.2 2nd Level Support

4.6.2.1 7 Communication Group

4.6.2.1.1 Roles & Responsibilities

The 2nd Level Support is a role generally composed of staff with greater technical skills than those of 1st Level. They should have enough time on their hands to devote themselves to incident diagnosis and resolution. 2nd Level Support will pay a visit to the end user if required, something that Service Desk staff cannot do.

4.6.2.2 Operation Mentor and Capability Development (OMCD)

4.6.2.2.1 Roles & Responsibilities

For OMCD to holistically plan and manage the sustainment and evolution of CD-DAR as a capability, functional and technical support functions must be tightly integrated. OMCD technical responsibilities will include, but not be limited to:

a. Supporting ongoing cyber security operations and DCO, as required;
b. Leading and coordinating technical modifications/transformation of CD-DAR Cyber security and DCO capabilities;
c. Mentoring Cyber systems maintainers at all levels to improve skills and maintain proficiency;
d. Supporting development and coordination of cyber systems maintenance training;
e. Supporting Cyber Operations exercises and experimentation;
f. Sustaining and evolving the CD-DAR ITI and cyber software tools; and
g. Integrating emerging technologies and best practices.

Draft

A professional services contract agreement (likely from the Original Equipment Manufacturer (OEM) / PSI) will be established to complement the OMCD in the provision of services such as, but not limited to:

a. In-country, end-to end support services for the CD-DAR solution, to ensure continuous operation, monitoring and support of any or all components of the CD-DAR solution;

b. Access to dedicated expert security engineers and analysts; and

c. Access to support and product development teams, on an as required basis.

4.6.2.2.2 CD-DAR Training, Exercise and Experimentation Environment

Having a realistic training environment that can mimic any operational network, as well as the attacker's environment, is a significant challenge. DND/CAF has initiated a capital project for the delivery of a Cyber Operational Training Environment (COTE). CD-DAR recurring training would normally integrate into COTE, however the project has evidenced limited progress and is at risk of being cancelled. In such event, the CITE Lab discussed at Paragraph 4.7.2.3 could configured to support the conduct of CD-DAR recurring training until a DND/CAF Cyber Program training environment is established. The CD-DAR training environment will encompass capabilities such as, but limited to: a network simulator, an interactive CD-DAR user interface, a scoring mechanism and a cybersecurity red team agent.

A Professional Development Needs Analysis (PDNA) will be conducted in Definition Phase which will further look the requirements for a training environment, along with CD-DAR operations and maintenance personnel individual and collective training requirements.

As CITE will provide an accurate representation of the production domains, it can be used very effectively for training cyber-operators, operations staff and other positions that need to develop and improve cybersecurity skills and experience without posing a risk to the production environment.

A complete snapshot of the Integration environment can be used for destructive (e.g. Red/Blue Team) exercises and quickly restored to repeat training scenarios. Or just portions of the environment can be cloned into training enclaves for specialized, targeted training and evaluation.

CITE can also be used for training and experimenting through exercises carried out internally within DND/CAF, or externally with OGDs and allies/partners like at CWIX and Bold Quest.

4.6.2.3 Cyber Integrated Test Environment (Post Implementation)

The Cyber Integration Test Environment (CITE) is not a single environment but a purpose built set of environments, comprised of mostly virtual infrastructure, with specific roles engaged in evaluation of products and technologies in sandbox enclaves, component development activity, integration and verification, training, exercises and experimentation support (refer to paragraph 4.7.2.2.2 above for details), CD-DAR solution release to production and finally ISS. In addition to its Test and Evaluation (T&E) activities, CITE will provide support for a standalone cyber-forensics lab. These environments are depicted in Figure 8. Additional information about the various roles of CITE may be found in the CD-DAR – CITE Cyber Security Engineering CONOPS.

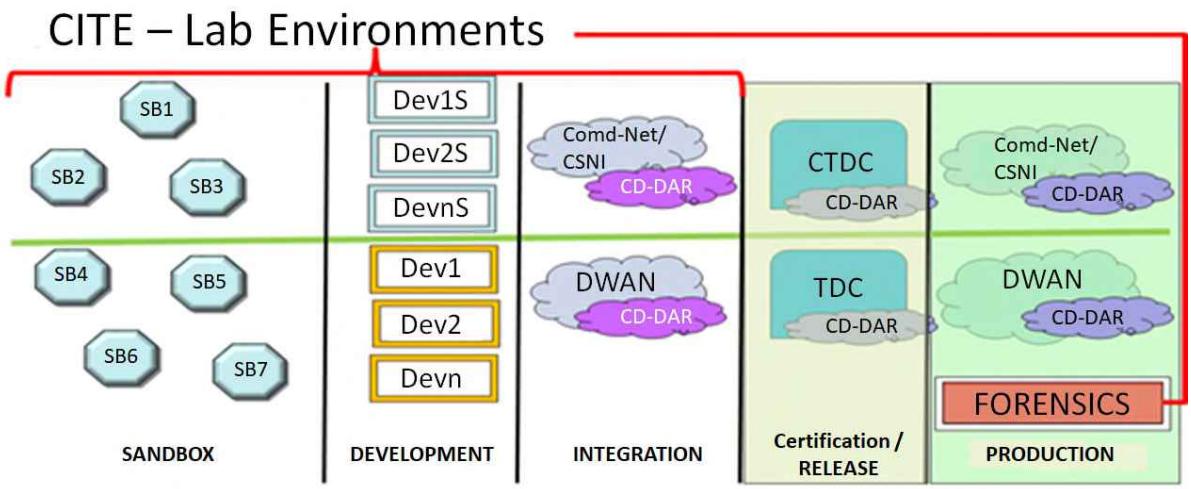


Figure 8 – CITE Lab Environments

CITE will serve several purposes over the lifetime of the Project, and beyond as a primary means of providing ISS for the sustainment and enhancement of the delivered capabilities (Operational processes and Technologies) and to support training and skills development (People).

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

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

b. The integration of cybersecurity capabilities, tools and technologies to protect information systems, data and infrastructure, while satisfying the strict needs for safety, security and availability;

c. The transition to a continuous monitoring of the information system environment to effectively and efficiently detect and prevent cybersecurity events;

d. The process improvements to respond and recover from cybersecurity events and attacks including advanced and persistent attacks from criminal groups and nation-state adversaries; and

e. The process to assess and improve the resilience of information systems ability to operate and perform the DND/CAF mission even when affected by a cybersecurity event or attack.

CITE will provide an environment that:

a. Accurately simulates the performance of all DND/CAF Comd-Net Extensions and Interfaces, both static and deployed, and identified deployable DWAN systems, and provides a configuration managed baseline representation of each facet of these networks;

Draft

b. Provides, within the DND/CAF Cyber Domains under evaluation, reliable and accurate performance evaluations of:
    i. New hardware and/or software,
    ii. Configuration changes to existing installed HW and/or SW,
    iii. Additions or changes to the nature and number of authorized users,
    iv. Additions or changes to points of presence and their locations,
    v. Effects on data throughput and/or bandwidth at any point within the networks,
    vi. The collection of system log data and SIEM data, and
    vii. The distribution of system log data and SIEM data;
c. Integrates with existing or planned DND/CAF IM/IT test and evaluation systems;
d. Improves Technical Awareness and understanding of how existing DND/CAF Cyber Domains are configured and operating; and
e. Improves Identification of vulnerabilities in the existing DND/CAF Cyber Domains.

4.6.3 3rd Level Support

4.6.3.1 DIMEI

4.6.3.1.1 Roles & Responsibilities

The 3rd Level Support role is reserved to an internal technical group if they possess the required specific knowledge; e.g. network support, database support, hardware maintenance, etc.

In cases where the 3rd Level Support function cannot be provided by DIMEI, cases for which expertise in too narrow a field, e.g. AI engines and algorithms, the required support will be escalated to the 4th-Level Support role an external service provider(s) and/or vendor(s).

4.6.4 4th Level Maintenance

4.6.4.1 3rd party Contracted Services

4.6.4.1.1 Roles & Responsibilities

Engineering support services are required over the in-service life of the CD-DAR capability and could include Technical Investigations and Engineering Studies (TIES), professional services (contractors / consultants), and additional 4th level contractor maintenance capability to address issues unresolved at 3rd level maintenance, or to evolve CD-DAR functionalities.

Draft

5 CONCLUSION

The CD-DAR capability will enable the DND/CF cyber force to defend the CAF's freedom of action and interests in cyberspace, and deliver military effects in and through a contested cyber environment in support of CAF missions and those regions of the global cyberspace used by Canada's allies and partners.

5.1 Operational Impacts

CD-DAR will conduct a complete automated electronic inventory of all network hardware devices and software; provide the ability to identify and track all assets (authorized and unauthorized) connected to Command Network; and assess their attributes for vulnerability, configuration, risk and patch compliance. CD-DAR's single trusted repository for the collection of cyber-related threat intelligence data, and basic system and network data will enable security monitoring and analysis.

The conduct of DND/CAF DCOs will be via a single user interface integrating a set of software tools to effectively automate the detection of cyber-threats, and the handling and traceability of incidents through the entire analysis process, thereby reducing the knowledge and specialization currently required of operators to become proficient.

CD-DAR will offer a central view of the entire network to assess cyber activities, traffic activities, gaps and irregularities, and a complete picture of the cyber threat landscape. It will automate, streamline and simplify procedures alleviating operators' cognitive overload; and enable the conduct of remote forensics and containment/remediation.

CD-DAR will be an integrated, modular, and scalable capability that is interoperable with existing DND/CAF platforms as well as those of OGDs and allies. This new capability will also establish and maintain cyber security, situational awareness, and analysis – all integrated within a system to provide reliable and contextual analysis to support DND/CAF cyber operations decisions and actions.

5.2 Organizational Impacts

CFNOC remains the lead organization for Cyber Defence within the DND/CAF, whose mission is to gain and maintain cyber superiority within DND/CAF Cyber Area of Responsibility and to ensure that the CAF is able to use its ITI reliably without interruption or interference by adversaries remains unscathed.

CD-DAR's system of processes, software and hardware will be capable of being used by existing DND/CAF operational personnel, including those personnel currently producing and consuming SA information, without excessive training or change to the skills of the available trades or occupations fulfilling those roles. CD-DAR's single, enhanced and integrated user interface streamlines the overall cyber defence operating process, decreases specialized knowledge and training time requirements.

The CD-DAR capability is a "behind-the-scenes" capability that protects the network from unauthorized and malicious infiltration attempts, a capability that is unnoticeable to authorized users of Command Network in their access to, or use of, the network.

Draft

5.3 Impacts during Development and Delivery

Due to the importance of the Cyber Domain to operations and the functioning of the DND/CAF, the risk of any interruption of service would be detrimental to Canada's national security. The new capabilities to be acquired under this Project will necessitate intimate knowledge and interaction with the very core of the DND/CAF ITI. Therefore, the CD-DAR project objectives during development and delivery are to:

a. Disturb day-to-day operations to the minimum extent possible;

b. Where necessary, call upon the DCO community's expertise to:

   i. Refine and validate capability operational and functional requirements,

   ii. Test and evaluate the capability as it evolve throughout the project lifecycle, and

   iii. Support Initial Operational Capability (IOC) and Full Operational Capability (FOC) acceptance testing;

c. Facilitate a smooth and efficient transition of cyber security and defence using the CD-DAR capability through punctual CD-DAR user training and mentoring; and

d. Institutionalize an ISS capability framework to maintain and optimize DCO operational processes, CD-DAR hardware and software tools, and recurring training of personnel to ensure the CD-DAR capability remains available, reliable and operationally relevant throughout its service life.

A fully staffed OMCD will be endowed at IOC, and optimally effective by FOC, to sustain and continuously and holistically evolve the CD-DAR capability (people, operations and tools), while coordinating with OGDs and allies to ensure continued interoperability and synergy of efforts, so the capability continues to operate at peak performance in order to pre-empt growing hostile threats. The OMCD team will also coach, instruct and mentor Cyber Operators, managers and executives through continuous business alignment, skills development, collective training development and exercise coordination, in order to maintain proficiency and achieve their missions.

Draft

Annex A – CFNOC Organizational Interaction Diagrams

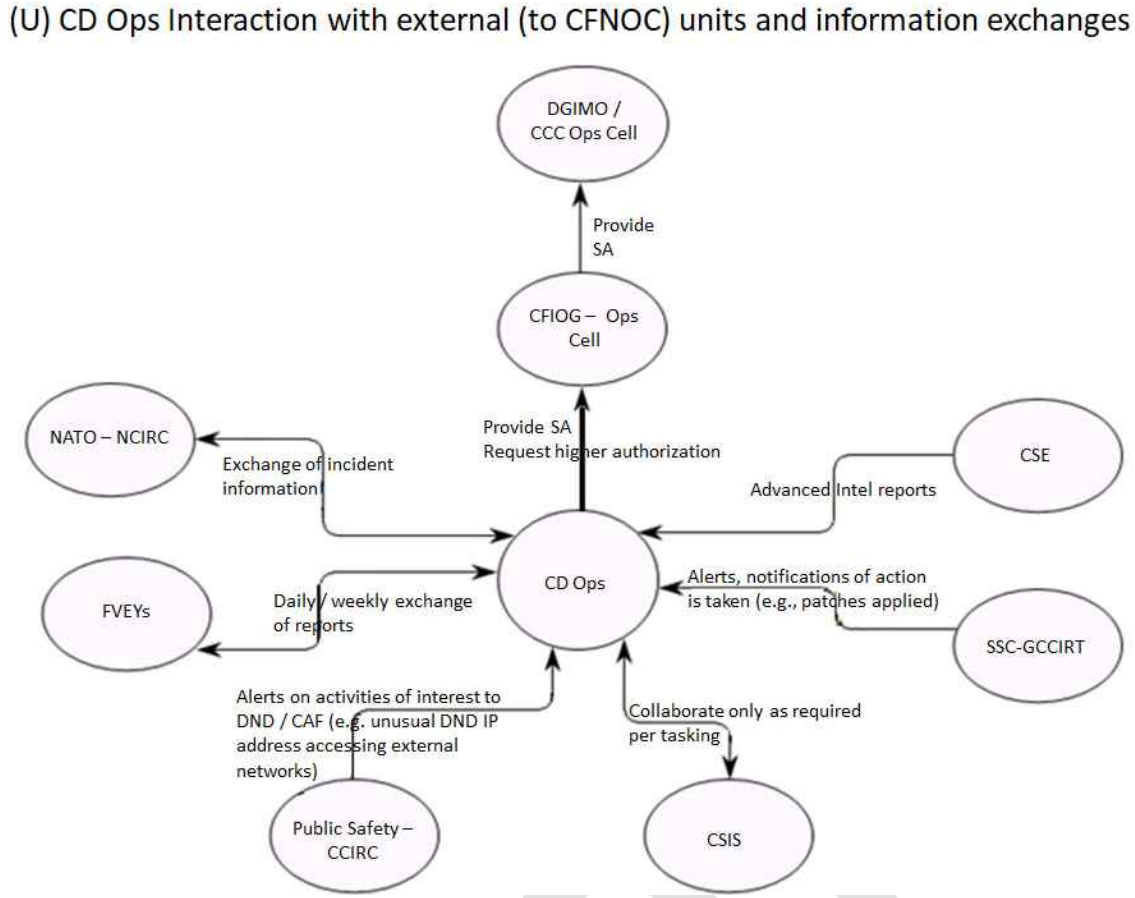


Figure 9 – CD Ops interaction and Int / Info exchange with stakeholders

Draft

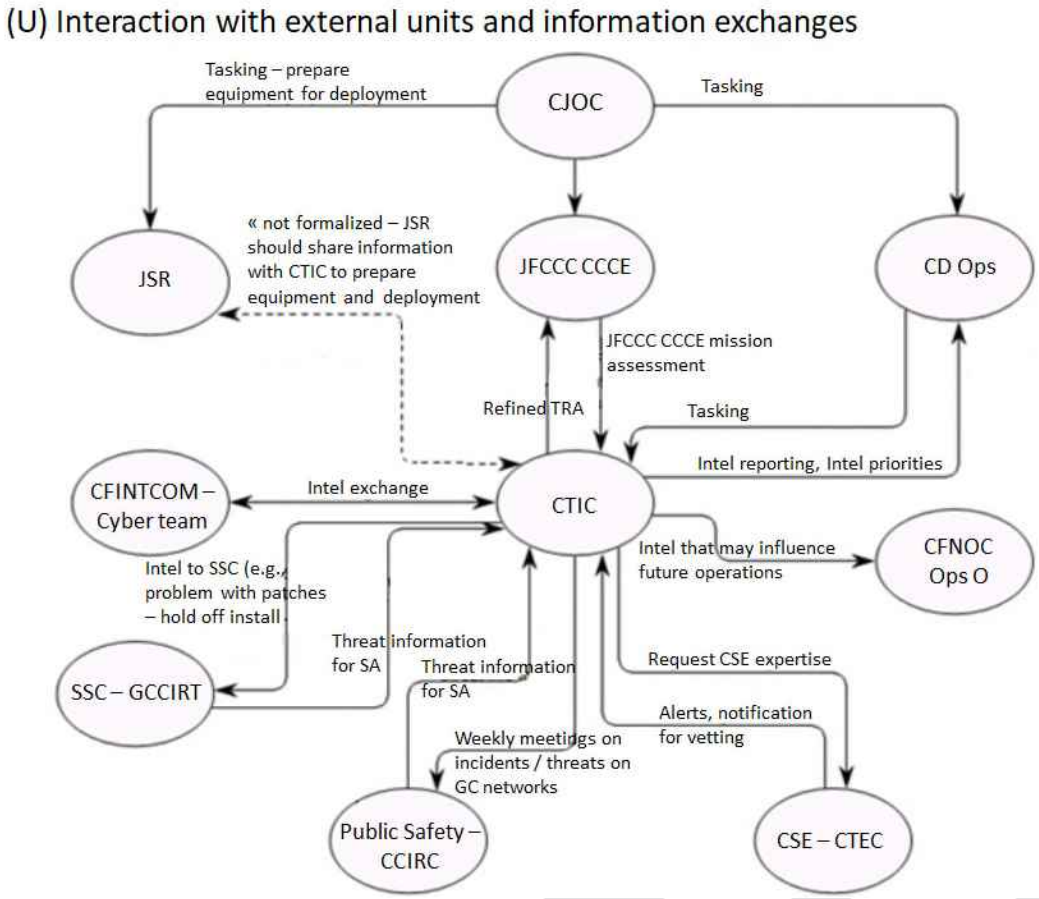


Figure 10 – CTIC interaction and Int / Info exchange with stakeholders

Draft

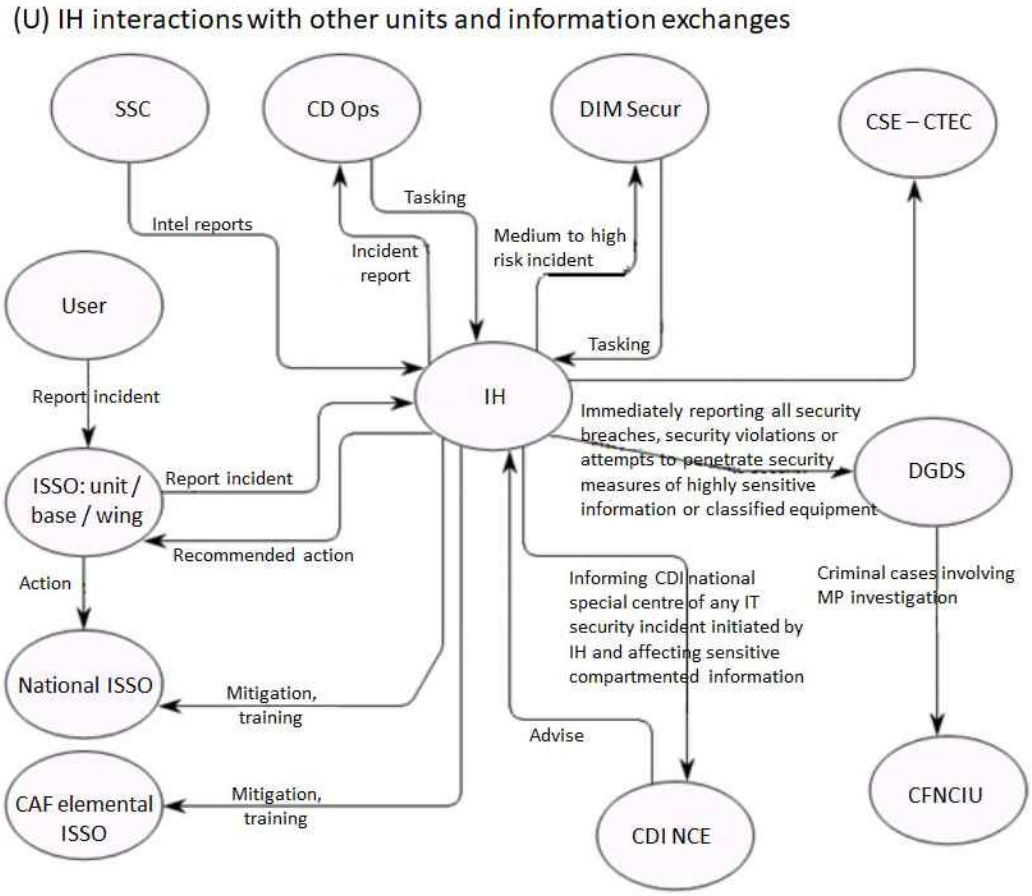


Figure 11 – Incident handling Team interaction and Int / Info exchange with stakeholders

Draft

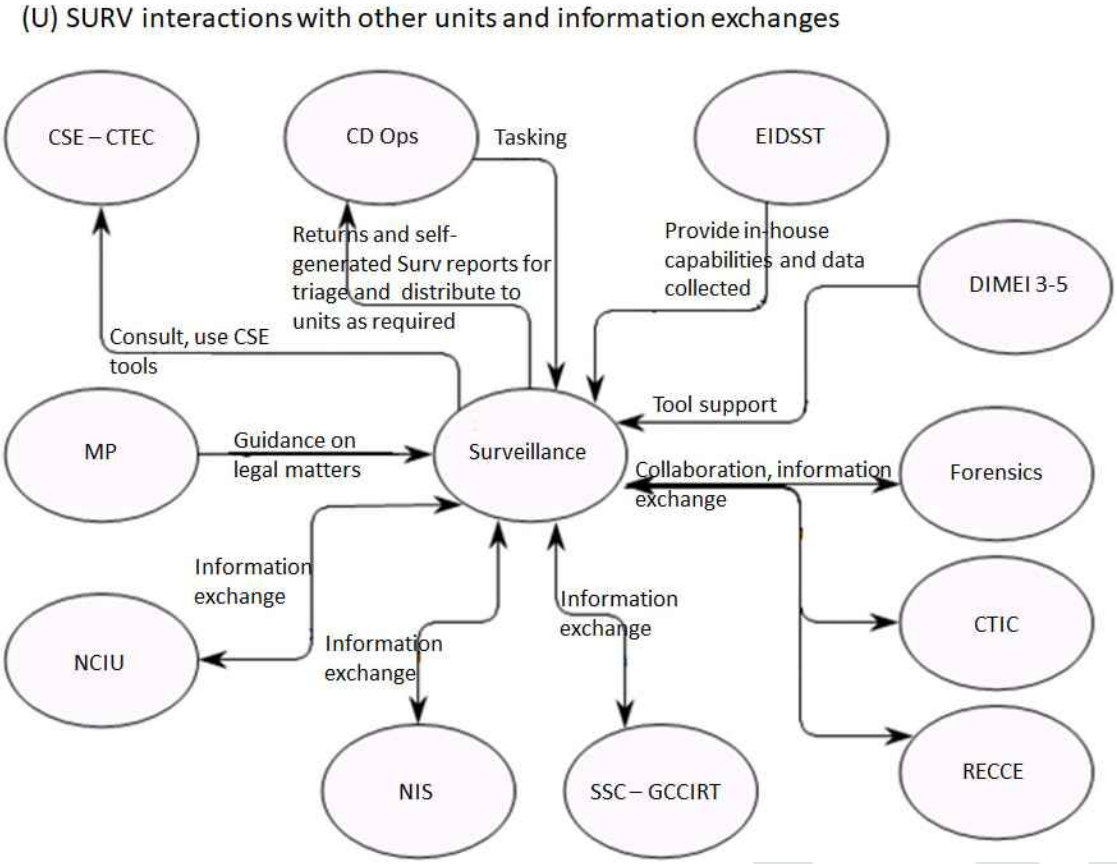


Figure 12 – Surveillance Team interaction and Int / Info exchange with stakeholders

Draft

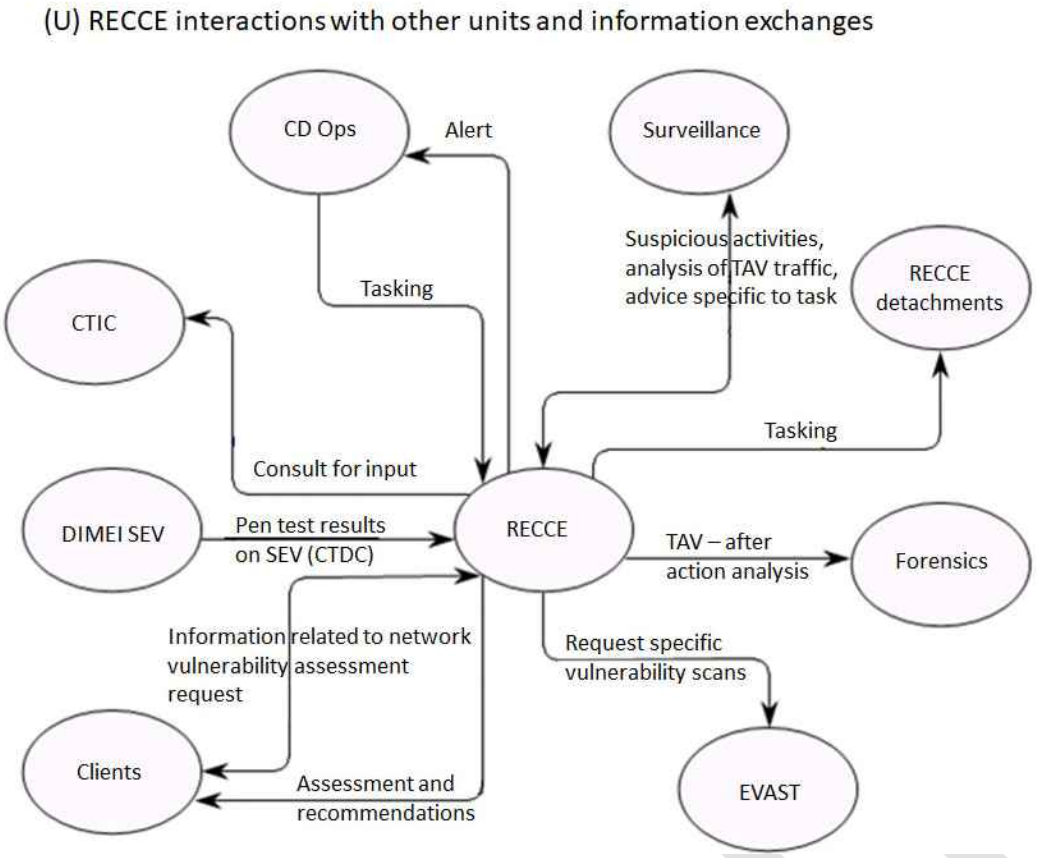


Figure 13 – Reconnaissance Team interaction and Int / Info exchange with stakeholders

Draft

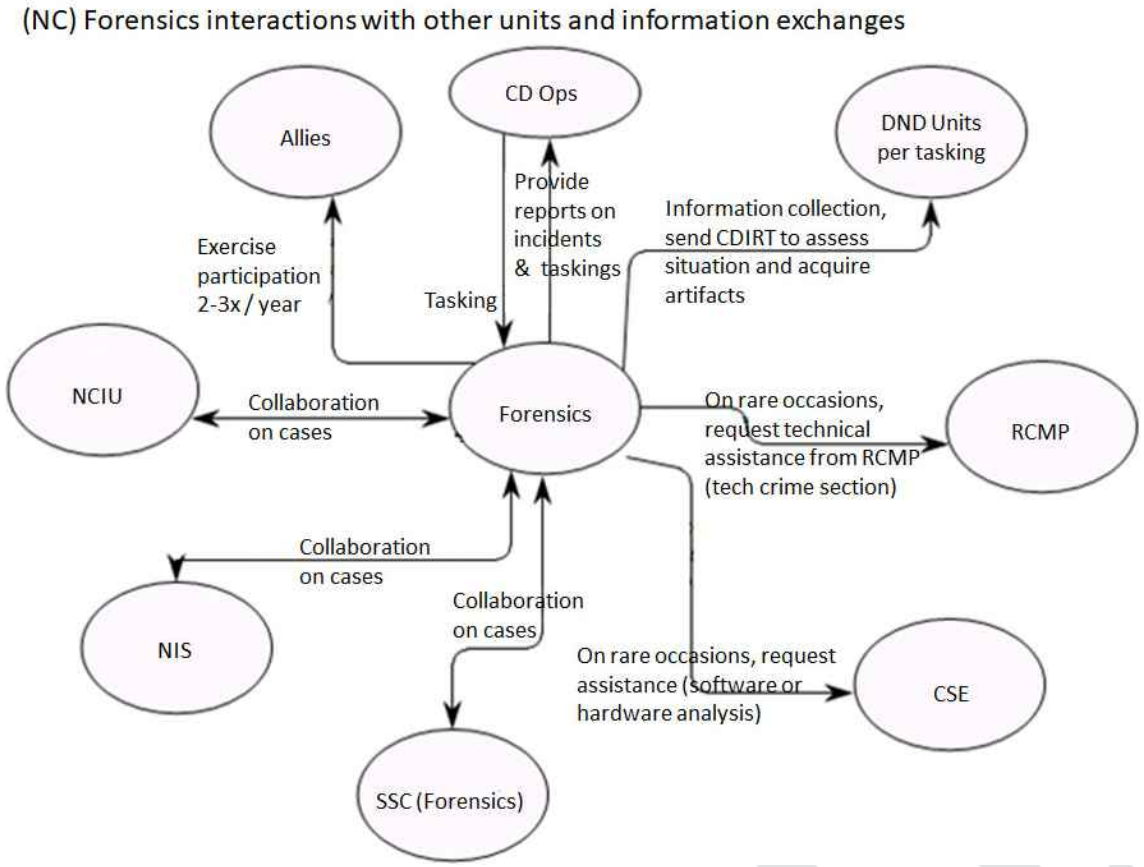


Figure 14 – Forensics Team interaction and Int / Info exchange with stakeholders

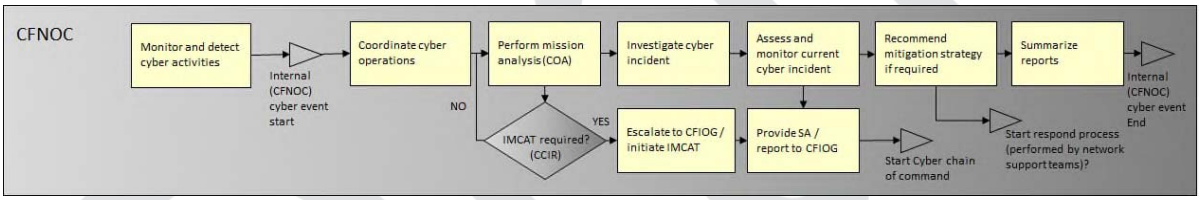


Figure 15 – CD Ops Cyber Event Coordination Workflow

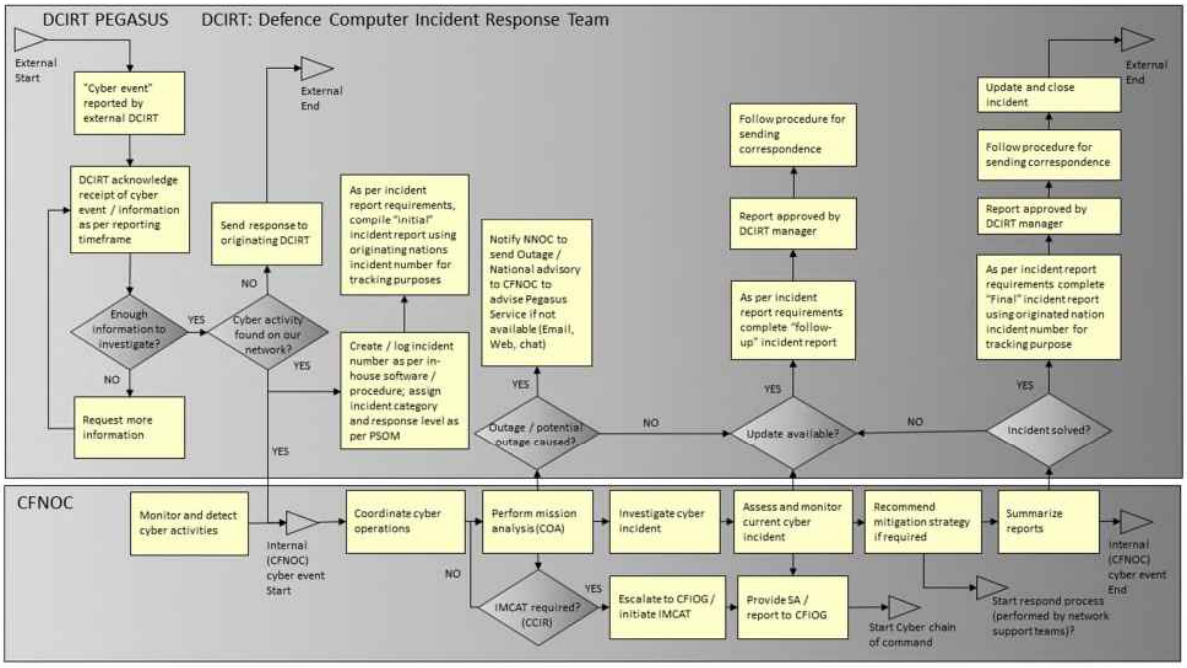


Figure 16 – Cyber Event Management including with FVEY on Pegasus

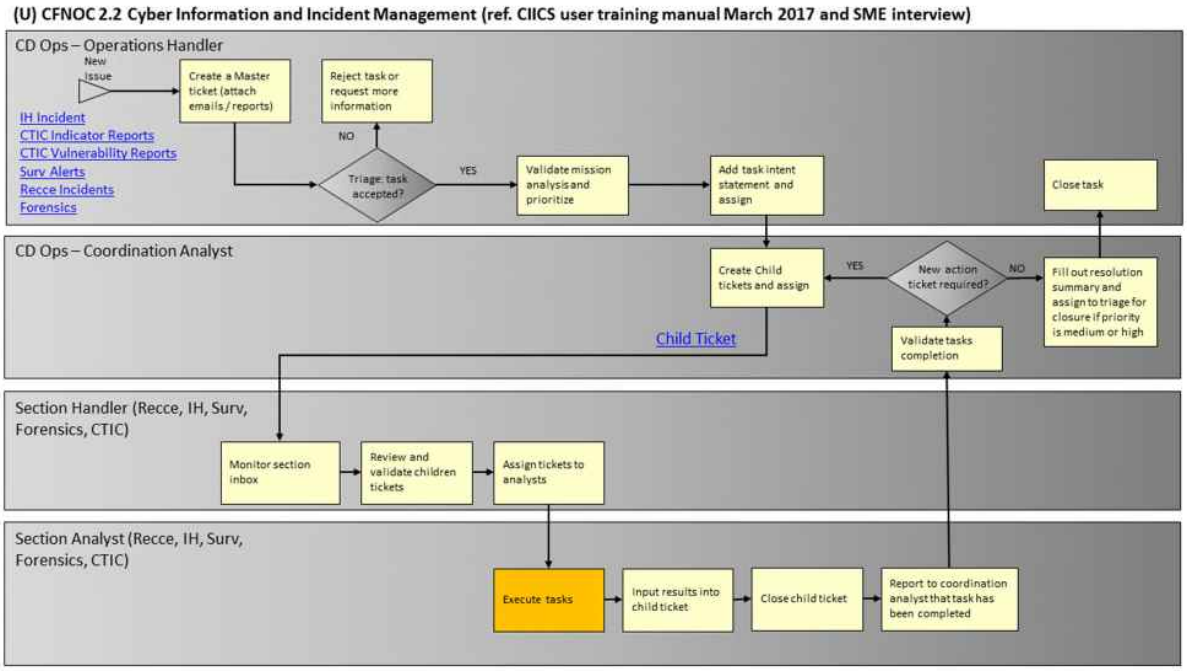


Figure 17 – Cyber Information and Management Workflow

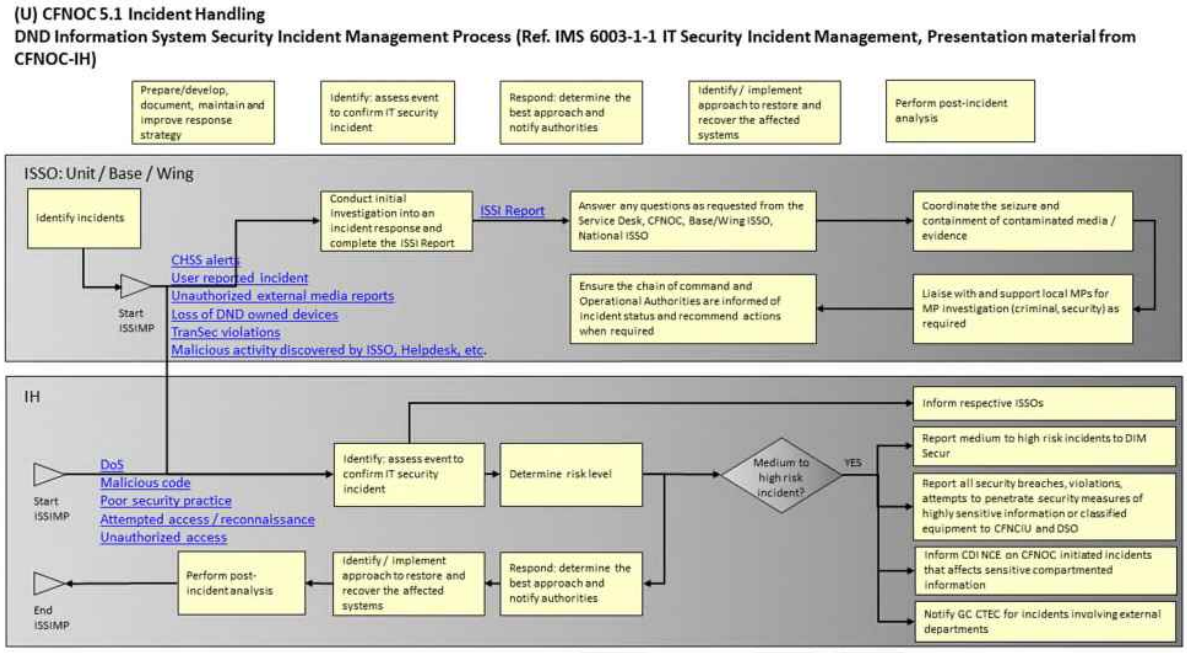


Figure 18 – Incident Handling Workflow

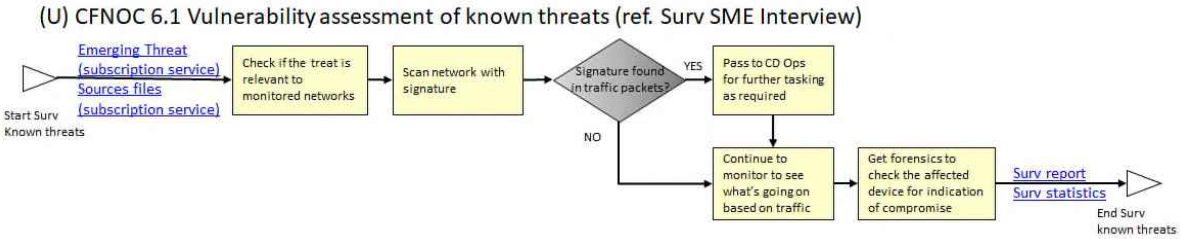


Figure 19 – Assessment of Known Threats Workflow

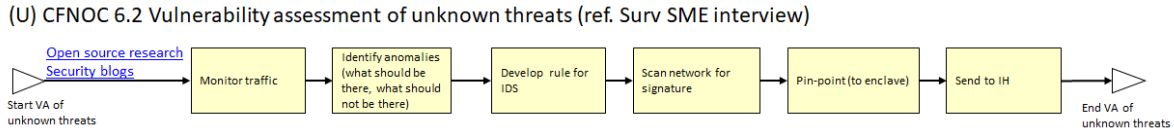


Figure 20 – Assessment of Unknown Threats Workflow

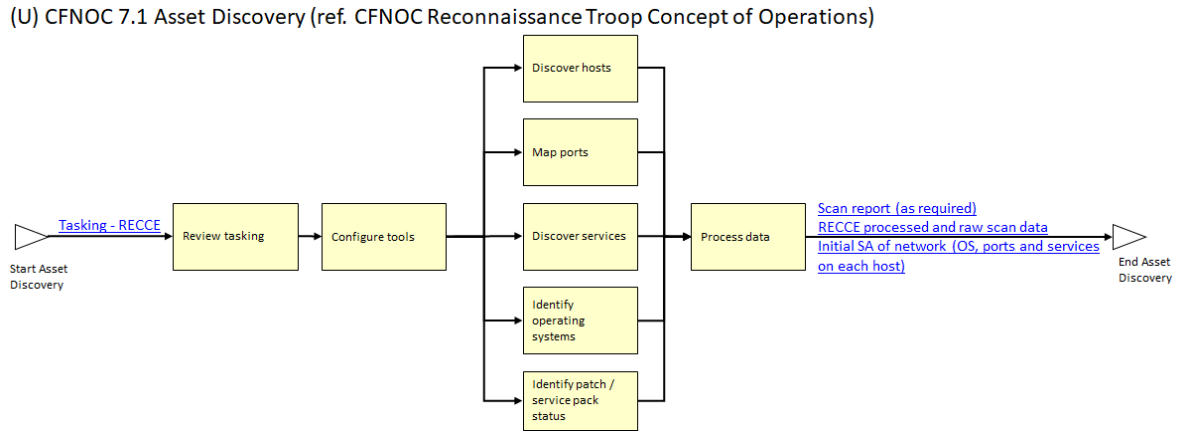


Figure 21 – Asset Discovery Workflow

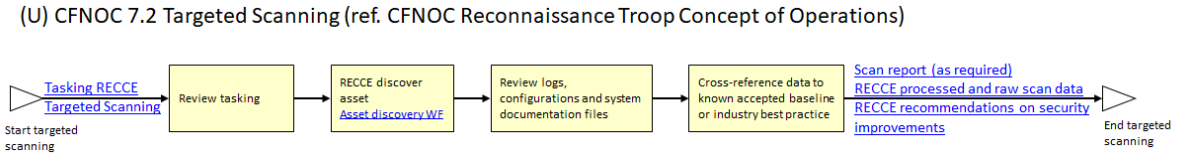


Figure 22 – Target Scanning Workflow

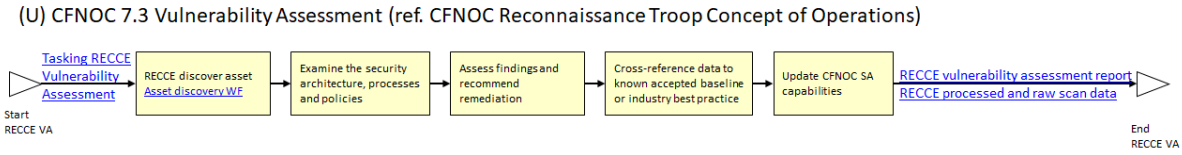


Figure 23 – Vulnerability Assessment Workflow

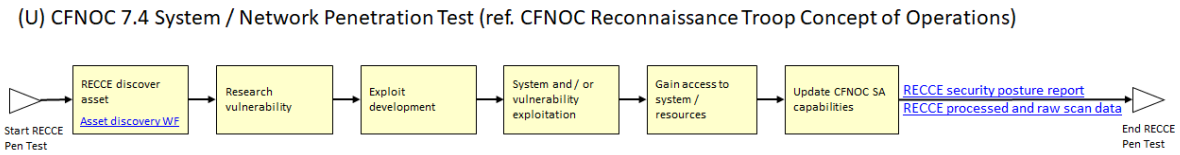


Figure 24 – System/Network Penetration Test Workflow

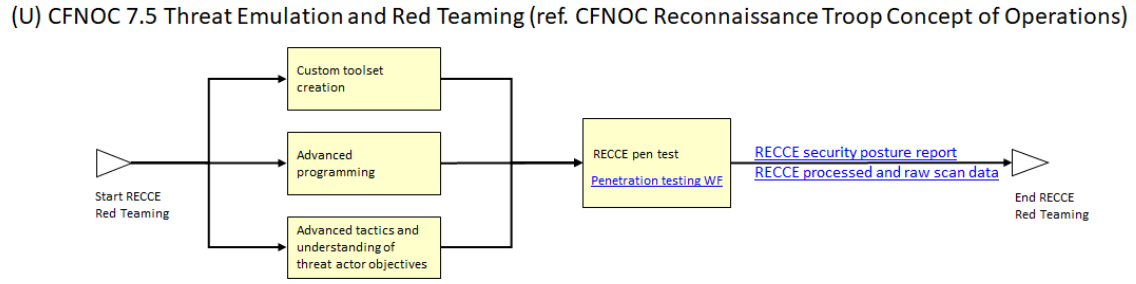


Figure 25 – Test Emulation Workflow

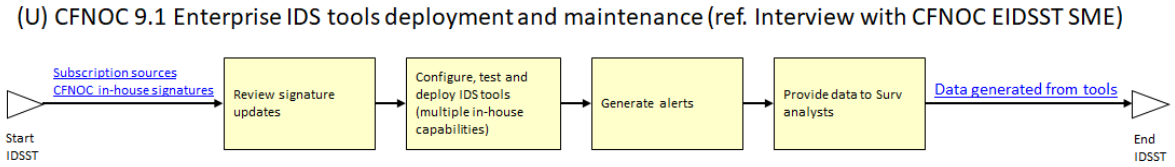


Figure 26 – Enterprise Intrusion Detection System (IDS) Workflow

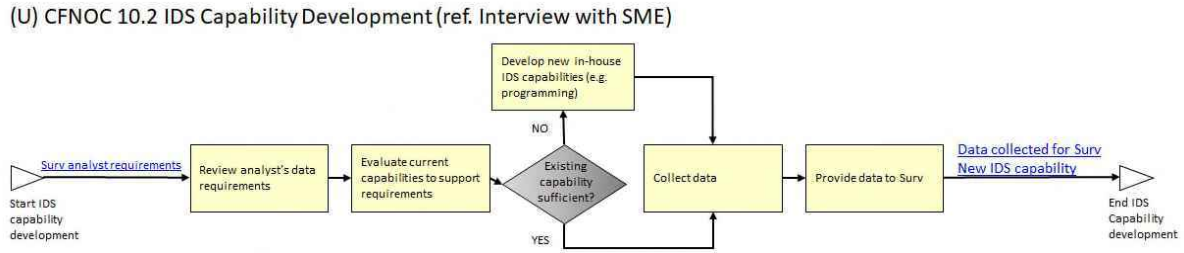


Figure 27 – IDS Capability Development Workflow

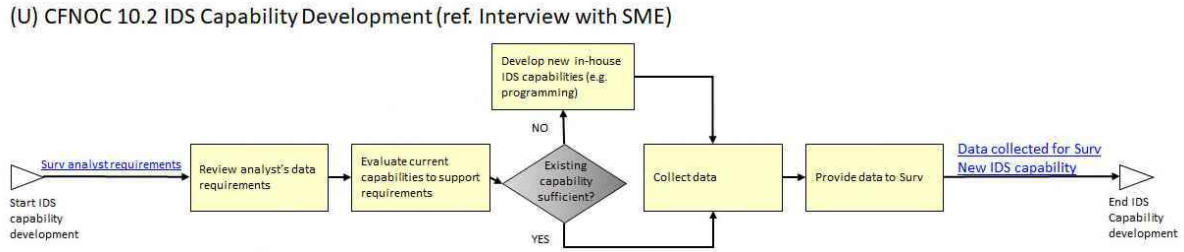


Figure 28 – Enterprise Vulnerability Assessment Workflow

Annex B – Acronyms and Abbreviations

Term	Description
7 Comm Gp	7 Communication Group
ACD	Active Cyber Defence
ACH	Analysis of Competing Hypotheses
ACISS	Army Communication and Information System Specialists
ADM(IM)	Assistant Deputy Minister (Information Management)
AI	Artificial Intelligence
AIOps	AI Operations
AIS	Automated Indicator Sharing
AoCO	Area of Cyber Operations
AOR	Area of Responsibility
APT	Advanced Persistent Threat
ATIS	Aerospace Telecommunications and Information Systems Technicians
AUS/NZ/UK/US	Australia/New Zealand/United Kingdom/United States of America
C Cyber	Chief of Cyberspace Staff
C2	Command and Control
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance
CA	Canadian Army
CAF	Canadian Armed Forces
CANSOFCOM	Canadian Special Operations Forces Command
CCC	Commander Cyber Command
CCCE	Cyber Component Coordination Element
CCCS	Canadian Centre for Cyber Security
CCEB	Combined Communications and Electronics Board
CCIRC	Canadian Cyber Incident Response Centre
CD-DAR	Cyber Defence – Decision Analysis and Response
CD Ops	Cyber Defence Operations
CDI	Chief of Defence Intelligence
CDIRT	Cyber Defence Incident Response Team

Draft

Term	Description
CDR	Cyber Database Repository
CDS	Chief of Defence Staff
CFC	Cyber Force Commander
CFCD	Canadian Forces Cyber Division
CFINTCOM	Canadian Forces Intelligence Command
CFIOG	Canadian Forces Information Operations Group
CFNIS	Canadian Forces National Investigation Service
CFNOC	Canadian Forces Network Operations Centre
CI/CD	Continuous Integration / Continuous Deployment
CIICS	Cyber Information and Incident Sharing System
CIS	Communication Information Systems
CITE	Cyber Integrated Test Environment
CJOC	Canadian Joint Operations Command
CMA	Cyber Mission Assurance
CMDB	Configuration Management Database
COA	Course of Action
CoG	Center of Gravity
Comd-Net	Command Network
COMSEC	Communication Security
CONOPS	Concept of Operations
CONPLAN	Contingency Plan
CONSUP	Concept of Support
COP	Command Operating Picture
COS	Chief of Staff
COTE	Cyber Operational Training Environment
COTS	Commercial off the Shelf
Cpl	Corporal
CPT	Cyber Protection Team
CPU	Central Processing Unit
CR	Change Request

Draft

Term	Description
CSA	Cyber Situational Awareness
CSE	Communications Security Establishment
CSF	Cyber Security Framework
CSIS	Canadian Security Intelligence Service
CSNI	Consolidated Secret Network Infrastructure
CSO	Chief Security Officer
CTDC	Classified Test and Development Centre
CTEC	Cyber Threat Evaluation Centre
CTIC	Cyber Threat Intelligence Cell
CWIX	Coalition Warrior Interoperability eXploration eXperiment eXamination eXercise
D Cyber Ops FD	Director Cyber Operations Force Development
DCA	Departmental COMSEC Authority
DCIO	Defence Chief Information Officer
DCIRT	Defence Computer Incident Response Team
DCO	Defensive Cyber Operations
DCO-DS	Defensive Cyber Operations – Decision Support
DCO-IDM	Defensive Cyber Operations – Internal Defence Measures
DEFSOC	Defence Service Operations Centre
DGDS	Director General Defence Security
DGEAS	Director General Enterprise Application Services
DGICFD	Director General Information Capabilities Force Development
DGIMO	Director General Information Management Operations
DGIMPD	Director General Information Management Project Delivery
DGIMTSP	Director General Information Management Technology and Strategic Planning
DHS	Department of Homeland Security
DIM Secur	Director Information Management Security
DIMCD	Director Information Management Capability Development
DIMEI	Director Information Management Engineering and Integration
DL	Deep Learning

Draft

Term	Description
DND	Department of National Defence
DNDAF	DND and CAF Architecture Framework
DPDCC	Director Project Delivery Command and Control
DRA	Dynamic Risk Assessment
DRF	Departmental Results Framework
DRM	Dynamic Risk Management
DTB	Defence Terminology Bank
D-VPNI	Defence – Virtual Private Network Infrastructure
DWAN	Defence Wide Area Network
ECS	Enhanced Cyber Security
EDR	Endpoint Detection and Response
EIDSST	Enterprise Intrusion Detection System Support Team
EITSM	Enterprise Information Technology Service Management
EMSEC	Emission Security
EVAST	Enterprise Vulnerability Assessment Support Team
EW	Electronic Warfare
FD	Force Development
FE	Force Employment
FG	Force Generation
FOC	Full Operational Capability
FP&R	Force Posture and Readiness
FVEY	Five Eyes
GC	Government of Canada
GC-CIRT	Government of Canada – Cyber Incident Response Team
HLMR	High Level Mandatory Requirement
HW	Hardware
IA	Information Assurance
IAM	Identity and Access Management
IDS	Intrusion Detection System
IH	Incident Handling

Draft

Term	Description
IM	Information Management
IM Gp	Information Management Group
IMCAT	Information Management Capability Assessment Team
Info	Information
Int	Intelligence
IoA	Indicator of Attack
IoC	Indicator of Compromise
IOC	Initial Operational Capability
IoT	Internet of Things
IP	Internet Protocol
IPOE	Intelligence Preparation of the Operational Environment
IR	Incident Response
ISS	In-Service Support
ISSO	Information System Security Officer
IT	Information Technology
ITI	Information Technology Infrastructure
ITSM	Information Technology Service Management
JBMC	Joint Battlespace Management Capability
JCOT	Joint Cyber Operations Team
JFCCC	Joint Force Cyber Component Commander
JSR	Joint Signal Regiment
JTF HQ	Joint Task Force Headquarters
KPI	Key Performance Indicator
LLs	Lessons Learned
MA	Mission Assurance
MCpl	Master Corporal
MISP	Malware Information Sharing Platform
ML	Machine Learning
MP	Military Police
NATO	North Atlantic Treaty Organization

Draft

Term	Description
NC	Naval Communicators
NCIO	Naval Combat Information Operators
NCIRC	NATO Computer Incident Response Capability
NCIU	National Counter-Intelligence Unit
NDHQ	National Defence Headquarters
Net Ops	Network Operations
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defence Command
NSA	National Security Agency
NSD	National Service Desk
NSMO	National Service Management Office
NVD	National Vulnerability Database
O&C	Oversight and Compliance
OA	Operational Authority
OEM	Original Equipment Manufacturer
OGD	Other Government Departments
OMCD	Operation Mentor and Capability Development
OODA	Observe Orient Decide Act
OP	Operation
OPCOM	Operational Command
OPCON	Operational Control
OPFOR	Opposing Forces
Ops	Operations
Ops O	Operations Officer
OPSEC	Operational Security
OS	Operating System
OV	Operational View
PAD	Project Approval Directive
PCAP	Packet Capture
PD	Project Director

Draft

Term	Description
PDNA	Professional Development Needs Assessment
Pen Test	Penetration Testing
PGM	Program Guidance Memorandum
PM	Project Manager
PSC	Public Safety Canada
PSI	Prime System Integrator
Pte	Private
RA	Response Action
RBAC	Role-Based-Access-Control
RCAF	Royal Canadian Air Force
RCMP	Royal Canadian Mounted Police
RCN	Royal Canadian Navy
RECCE	Reconnaissance
RFC	Request for Change
RFI	Request for Information
SA	Situational Awareness
SA&A	Security Assessment and Authorization
SDN	Software Defined Network
SGT	Sergeant
SIEM	Security Incident and Event Management
SIGINT	Signals Intelligence
SJS	Strategic Joint Staff
SME	Subject Matter Expert
SOR	Statement of Operational Requirements
SSC	Shared Services Canada
SSE	Strong, Secure, Engaged: Canada's Defence Policy
SEV	Security Engineering Validation
SLA	Service Level Agreement
SMC	Service Management Centre
SOAR	Security Orchestration Automation Response

Draft

Term	Description
SOR	Statement of Operational Requirements
SPA	Security Posture Assessment
STIG	Security Technical Implementation Guides
SW	Software
T&E	Test and Evaluation
TA	Technical Authority
TAV	Technical Assistance Visit
TI	Threat Intelligence
TIES	Technical Investigations and Engineering Studies
TM	Task Management
TRA	Threat Risk Assessment
TranSec	Transmission Security
TSIT	Technical Security Inspection Team
TTPs	Tactics, Techniques, Procedures
UN	United Nations
URL	Uniform Resource Locator
US	United States
VCDS	Vice Chief of Defence Staff
VPE	Visual Playbook Editor
WAN	Wide Area Network
WoG	Whole of Government

Draft