RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
Information Technology Infrastructu

Solicitation No. - N° de l'invitation	Date
W8474-18IT01/A	2018-05-30
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
W8474-18IT01	PW-$$QE-450-26842
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
450qe.W8474-18IT01	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2018-07-17

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

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

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Guilderson, Greg	450qe
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 956-0564 ( )	( ) -

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

DEPARTMENT OF NATIONAL DEFENCE
2 Constellation Drive
OTTAWA
Ontario
K2G 5J9
Canada

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

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

Signature **Date**

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

Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM Destination	Plant/Usine	Delivery Req. Livraison Req.	Del. Offered Liv. offerte
1	Information Technology Infrastructu	W8474	W8474	1	Each	$	$	See Herein	

Information Technology Infrastructure in Support of Command and Control

-

Letter of Interest

TABLE OF CONTENTS

PURPOSE AND CONTENTS OF THIS LETTER OF INTEREST

This is the Letter of Interest (LOI) pertaining to the Information Technology Infrastructure in Support of Command and Control (ITI in Sp of C2) Project for the Department of National Defence (DND) and the Canadian Armed Forces (CAF). The purpose of this LOI is to inform and prepare industry for potential procurement opportunities concerning the ITI in Sp of C2 Project and seek input and contribution regarding the project's scope, requirements, schedule, risks and potential costs. The general contents of this LOI document are:

PART I: Letter of Interest Process: Information about the Letter of Interest Process and the procedure for industry to follow for responding to this Letter of Interest.

PART II: ITI in SP of C2 Solution

PART III: Questions to Industry: Questions asked to solicit feedback from industry that will help DND/CAF define its requirements and business case.

ANNEX A: ITI in Sp of C2 Project Background
ANNEX B: Mission Environment and Operational Scenarios
ANNEX C: Preliminary Statement of Requirements
ANNEX D: Feedback from Industry
ANNEX E: Acronyms

PART I: LETTER OF INTEREST PROCESS

1. INTRODUCTION

This is the LOI pertaining to the DND ITI in Sp of C2 Project for DND and the CAF. The purpose of this LOI is to inform and prepare industry for potential procurement opportunities concerning the ITI in Sp of C2 Project and seek input and contribution regarding the project's scope, requirements, risks and potential costs.

The ITI in Sp of C2 Project is in early Options Analysis Phase, meaning that the business case and justification for the project are still being developed. As such, no decisions on concepts, technologies or solution approaches have been made. The aim of the Options Analysis Phase is to ensure that departmental senior management can make an informed decision on the best way to define the Project (i.e., conduct the Definition Phase) and, if deemed appropriate, implement the project to achieve the required capability.

The intent is to actively engage and consult industry throughout the Options Analysis and Definition Phases to ensure a successful project end-state. Feedback from industry will assist the DND/CAF project team to define:

a. the Statement of Requirements (SOR) in a manner that is understandable by industry and meaningful to the DND/CAF operational context, thus contributing to better describing the business needs;

b. the "art of the possible" regarding Information Technology (IT) capabilities, future developments within industry, and how similarly large corporate organizations are changing to meet their evolving IT needs, leading to a better definition of the SOR, budget and schedule required to meet the project objectives (both technological and industrial/procurement);

c. the impact on people, processes and technologies of various solutions proposed and the organizational changes that will be required to support each conceptual solution;

d. the nature and sources of project costs, including the need for Definition Phase tasks, Implementation Phase costs and long-term In-Service Support (ISS); and,

e. the most appropriate procurement strategy that is amenable to industry which delivers the right equipment to the DND/CAF in a timely manner, secures best value for Canada, leverages the purchases to create jobs and growth, and streamlines procurement processes.

Suppliers will not be contacted by DND/CAF as a result of this LOI. The Contracting Authority detailed in section 2.7 may communicate with industry to seek more information on responses. Any future industry engagement activity or procurement will be publicly posted.

1.1 Nature of this Letter of Interest

This is not a bid solicitation. This LOI will not result in the award of any contract nor will this LOI result in the creation of any source list. Potential suppliers of any goods or services described in this LOI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this LOI. Therefore, whether or not a potential supplier responds to this LOI will not preclude that supplier from participating in any future procurement.

Also, the procurement of any of the goods and services described in this LOI will not necessarily follow this LOI. This LOI is simply intended to solicit feedback from industry with respect to the subject matter described in this LOI.

2. INSTRUCTIONS FOR RESPONDING TO THIS LETTER OF INTEREST

2.1 Nature and Format of Responses Requested

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

Responses will not be used for competitive or comparative evaluation purposes, and thus the response format is not as rigorously defined as would normally be for an RFP. However, for ease of use and in order for the greatest value to be gained from responses, Canada requests that respondents follow the structure outlined in section 2.6.

2.2 Response Costs

Canada will not reimburse any organization for expenses incurred in responding to this LOI.

2.3 Treatment of Responses

Use of Responses: Responses will not be formally evaluated; however, the responses received may be used by Canada to develop and/or modify the procurement approach. Canada will review all responses received. Canada may, at its discretion, review responses received after the LOI closing date.

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

Confidentiality: Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the requirements of the Access to Information Act.

2.4 Communication with Industry

The Contracting Authority may communicate with industry to seek more information regarding any response.

2.5 Contents of the LOI

The information contained in this document remains a work in progress and respondents should not assume that new requirements will not be added to any bid solicitation that is ultimately published by Canada. Respondents should also not assume that none of the requirements will be deleted or revised. Comments regarding any aspect of the requirement are welcome. This LOI also contains specific questions addressed to industry.

2.6 Format of Responses

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

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

i. the title of the respondent's response and the volume number;

ii. the name and address of the respondent;

iii. the name, address and telephone number of the respondent's contact;

iv. the date; and,

v. the LOI number.

Number of Copies: Canada requests that respondents submit their response in unprotected (i.e. no password) PDF format (2003 or later) by email, if the size of the document is less than six Megabytes (MB), to: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca Otherwise, Canada requests that respondents save a copy of their unprotected PDF (2003 or later) document onto two USB memory drives and mail them to the Contracting Officer(s) specified in section 2.7.

Responses to this LOI may be in either of Canada's official languages, English or French.

2.7 Enquiries

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

Contracting Authority: Greg Guilderson or Jeff Moore

Public Services and Procurement Canada
Place du Portage III, 8C2
11 Laurier Street
Gatineau, Quebec K1A 0S5
819-956-0564
Email address: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Please insert "ITI in Sp of C2" in the subject line. Failure to do so may result in delays receiving a response.

The use of email is the preferred method of communication.

2.8 Submission of Responses

Time and Place for Submission of Responses: Organizations interested in providing a response should deliver it to the Contracting Officer identified on page 1 of this LOI document by the closing time and date indicated on page 1 of this solicitation document.

The LOI closing date is not the deadline for comments or input. Comments and input will be accepted any time up to the time when/if a follow-on solicitation is published.

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

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

2.9 Fairness Monitor

Should a future ITI in Sp of C2 solution procurement process occur, Canada will engage the services of an organization to act as an independent, third-party Fairness Monitor. The role of the Fairness Monitor will be to provide an attestation of assurance on the fairness, openness, and transparency of the monitored activities.

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

i. observing all or part of the procurement process (including, but not limited to, the engagement and contemplated RFP processes);

ii. providing feedback to Canada on fairness issues; and

iii. attesting to the fairness of the procurement process.

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

PART II: ITI IN SP OF C2 SOLUTION

1. ITI IN SP OF C2 SOLUTION BACKGROUND

DND/CAF has a requirement to implement a secure, integrated Secret-level IT infrastructure that will converge and reduce the number of DND/CAF Secret networks, provide enhanced connectivity and information sharing capabilities within the DND/CAF and with our mission partners, and readily evolve to meet future challenges. This IT infrastructure will enable Commanders across the CAF to exercise C2, including at deployed headquarters, using the latest available technologies to provide optimal support capabilities.

The DND/CAF will deliver this new capability through the ITI in Sp of C2 Project, which will, among others, strive to leverage industry capabilities and efficiencies to deliver services to the maximum extent possible.

The ITI in Sp of C2 Project is currently in the Options Analysis Phase, with a preferred implementation option expected to be identified and selected by June 2019. This will be followed by a Definition Phase and then an Implementation Phase; Initial Operational Capability (IOC) is planned for June 2025, and Full Operational Capability (FOC) by September 2027.

2. OBJECTIVE OF THIS LOI

This LOI is being issued with the objective of:

a. consulting industry to better understand available and emerging commercial IT infrastructure and service solutions;
b. seeking information from industry on the price and availability of commercial IT infrastructure and service solutions;
c. seeking information to assist the DND/CAF in developing their requirement and assist in the internal planning and approval process that may potentially lead to a solicitation; and,
d. seeking information to assist the DND/CAF in potentially grouping some of the deliverables listed in Annex C, so that a vendor or team of vendors can provide an integrated solution for a coherent sub-grouping of deliverables.

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

3. SECURITY REQUIREMENTS

There are no security requirements associated with this LOI.

Any future procurement actions undertaken in support of the ITI in Sp of C2 Solution will require suppliers to be registered in the Controlled Goods Program, and may require suppliers to hold a Level II (Secret) clearance and potentially Level III (Top Secret) clearance issued by their respective national security agency. Some of the suppliers may also need to meet GC requirements for providing products and services with (classified) Canadian Eyes Only (CEO) restrictions.

More info on the Controlled Goods Program here:
https://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html

4. NATIONAL SECURITY EXCEPTION

In order to protect national security interests, Canada will invoke its right under national and international trade agreements to use a National Security Exception (NSE) for this procurement. An NSE allows Canada to remove a procurement from some or all of the obligations of the relevant trade agreement where Canada considers it necessary to do so in order to protect its national security or other related interests specified in the text of the national security exceptions.

5. INDUSTRIAL AND TECHNOLOGICAL BENEFITS (ITB) POLICY

This requirement is exempt from the international trade agreements and falls within the framework of the Defence Procurement Strategy announced on February 5, 2014. Therefore, the ITB Policy with Value Proposition may be applied to this procurement. The ITB Policy is administered by Innovation, Science and Economic Development Canada (ISED).

5.1 Application of the Industrial and Technological Benefits (ITB) Policy

The Industrial and Technological Benefits (ITB) Policy may be applied on the Information Technology Infrastructure in Support of Command and Control (ITI in SP of C2) project. Engagement with industry through the Letter of Innterest (LOI) will help determine the application of the ITB Policy and how Canada could leverage opportunities for economic benefit through this procurement.

5.2 The ITB Policy including Value Proposition

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

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

For more information about the ITB Policy, please visit www.canada.ca/itb.

5.2.1 Key Industrial Capabilities

To maximize the economic impact that can be leveraged through the VP, Canada will look to use the ITB Policy to motivate defence contractors to invest in Key Industrial Capabilities (KICs). KICs align with Canada's defence policy, *Strong, Secure, Engaged*, and the *Innovation and Skills Plan* by supporting the development of skills and fostering innovation in Canada's defence sector. The KICs represent areas of emerging technology with the potential for rapid growth and significant opportunities, established capabilities where Canada is globally competitive, and areas where domestic capacity is essential to national security.

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

The definitions for the relevant KICs for this project are:

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

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

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

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

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

6. OFFICIAL LANGUAGES

Any future contract for an ITI in Sp of C2 solution may require the Contractor to provide all documentation along with technical and client support in both official languages.

7. ENGAGEMENT APPROACH

7.1 Industry Engagement

The industry engagement process begins with this LOI and will conclude when an official Request for Information, RFP or other competitive process is distributed to suppliers.

This LOI is posted on Buyandsell.gc.ca as a chance for industry to share with PSPC and DND information on the current marketplace, available technology and supplier capabilities.

As DND/CAF is in the early Options Analysis Phase of this procurement, the Industry Engagement approach beyond this phase is still in development.

PART III: QUESTIONS TO INDUSTRY

1. QUESTIONS TO INDUSTRY

1.1 Areas of Interest

1.1.1 Which of the capabilities listed in Annex A - Section 5 (Project Capabilities and Technologies of Interest) would you be interested in providing and/or supporting, and in what specific role(s) (e.g., system integrator, component provider, site installer, verification and validation, training provider, in-service support provider, etc.)?

1.1.2 Are there other capabilities not listed at Annex A – Section 5, which you would recommend be considered by the project team and would be interested in providing and/or supporting and, if so, in what specific role(s) (e.g., system integrator, component provider, site installer, verification and validation, training provider, in-service support provider, etc.)?

1.2 Experience

1.2.1 With respect to the capabilities that you listed at Section 1.1:

a. Do you have experience in providing those or similar capabilities for an IT infrastructure supporting between 25,000 and 50,000 users, across widely geographically separated campuses? If not, what is the maximum user size IT infrastructure that you have been involved in?

b. Do you have experience in delivering those or similar capabilities in the classified environment? If not, do you have any experience in delivering other IT infrastructure solutions in the classified environment?

c. Where applicable for the above, please provide a summary of your role(s) (e.g., system integrator, component provider, site installer, verification and validation, training provider, in-service support provider, etc.), experience, and examples of projects and/or contracts (maximum of three examples for each, if applicable) with the name and type of customer(s) (private industry, government entity).

1.3 Recommended Solutions

1.3.1 What is your vision for a solution(s) in year 2025 that would meet specific or all project' requirements and capabilities, as described at in Annex C – Section 2 (General Requirements and Deliverables)?

1.3.2 What are your solution proposal(s)? Please describe in general terms how the proposed solutions would meet specific project requirements, including their pros and cons, and provide relevant recommendations as applicable.

1.3.3 What portions of IT infrastructure would you recommend the DND/CAF provide of the design and/or actual equipment?

1.3.4 What portions of IT infrastructure would you recommend the DND/CAF implement as part of the overall solution?

1.3.5 Which IT infrastructure capabilities would you recommend be grouped together as a package for the delivered solution?

1.3.6 What would be the implementation strategy that you recommend? Would you recommend a phased delivery approach? How would you transition from the old systems to the new system while ensuring continuous operations?

1.3.7 Are there specific IT technology trends that you would recommend the DND/CAF investigate that could potentially better enable the delivery of the capabilities listed in Annex A?

1.3.8 Please provide relevant product sheets for your proposed products and solutions, if available.

1.4 Cloud Technology

1.4.1 In the context of a cloud solution for a classified environment:

a. What would your recommendation(s), including pros and cons, be for using a Public, Private, and Hybrid cloud as a full or partial solution?

b. Would you be able to provide dedicated infrastructure to the DND/CAF in a Public cloud environment (i.e., Virtual Private Cloud)? If yes, please explain how.

c. If applicable, please explain how your solution would automatically and dynamically leverage the Public cloud to support and/or augment a DND/CAF Private cloud in a Hybrid environment.

d. How would the DND/CAF be able to monitor your solution(s) and the data owned by DND/CAF to meet the authoritative control requirement?

e. How would the DND/CAF, specifically our network operation centre and system administrators, be able to access the configuration and status of all IT equipment and software?

f. What would your recommended strategy be to migrate DND/CAF data from our network to your cloud solution?

g. What would the recommended exit strategy be to migrate data off of your infrastructure/solution if/when the contract expires?

h. In the event of data leakage, how would the DND/CAF have access to your sites to perform clean-up (i.e., erase data/disk)?

1.5 Identity, Credential and Access Management and Data Centric Security Service

1.5.1 In the context of Identity, Credential and Access Management (ICAM) capability listed in Annex A:

a. Please describe what type of services you provide and explain how each one of them functions.

b. How would your ICAM solution work with a Public Key Infrastructure (PKI) based authentication/credentials system? What kind of interface change would be required to integrate with an existing PKI system?

c. How would your ICAM solution impact the Active Directory configuration and deployment?

d. How would your ICAM solution work in the contexts of Access Control List (ACL), Role Based Access Control (RBAC), Attribute Based Access Control (ABAC) and Policy Based Access control (PBAC)?

e. Does your ICAM solution provide multiple factor credentials access? If yes, please explain how.

f. Does your solution work in a centralized or distributed (e.g. approx. 15- 20 locations) environment? What are the pros, cons and limitations of a centralized vs distributed solution?

1.5.2 In the context of DCSS (Data Centric Security Service):

a. What classifications of data (Unclassified, Secret, etc.) is currently approved to be protected using your data centric approach and product(s)? Are there any advancements in development that would increase the current protection/classification capabilities? If yes, please explain.

b. What approach are you taking to secure information at rest and in transit?

c. What are the constraints/limitations of your DCSS system?

d. What standards have been or are being used in the development of the DCSS (including metadata)?

e. How would your system interoperate with other domains who do not have a similar capability or with domains that use a different DCSS solution?

f. Would your system be interoperable with a solution such as GCDOCS?

g. How would your system work in a temporarily disconnected environment?

h. Could the encryption method used by the system be upgraded independent of the system itself?

i. What is the granularity of the policy rules which can be created? Is this adaptable to specific data sets?

j. What approach has been taken to auditing transactions handled by the DCSS system? Does this integrate with Security Incident Event Management (SIEM) or is it a standalone application?

k. What are the standard roles required to administer your DCSS system? Does the system support separation of duties and flexible workflows for administrative role assignment?

l. Does your solution work in a centralized or distributed (e.g. approx. 15- 20 locations) environment? What are the pros, cons and limitations of a centralized vs. distributed solution?

m. How would your solution interoperate with legacy data? Is there a tool to migrate legacy data to the new environment? Please quantify the effort required to migrate the legacy data (low, medium, high, very high) and describe the process.

1.6 DND/CAF Cost Drivers

1.6.1 What are the key cost drivers, to DND/CAF, for a full solution and for individual elements?

1.6.2 What is the cost modelling for your solution(s), including the key metrics used to determine cost? Do you have tiered costing based on volume?

1.6.3 What information would be required to enable you to provide more substantive cost estimates?

1.6.4 Please provide Rough Order of Magnitude (ROM) cost estimates (separated into project management, engineering services and scheduled duration, and materiel/software costs) for your proposed solution including, if applicable:

a. development of detailed system specifications;

b. development of detailed system design;

c. creation and deployment of a test & development environment;

d. development and deployment of a prototype/prototypes, where applicable;

e. security assessment & approval;

f. training needs assessment;

g. any additional hardware or software;

h. other configuration/setup/installation/deployment;

i. miscellaneous engineering services;

j. operating costs that would be incurred by DND/CAF (including the expected number of personnel required to support/analyze data to deliver capability); and

k. in-service support and maintenance costs that would be incurred by DND/CAF.

1.6.5 If possible, please provide ROM costs for a fully outsourced in-service support solution (including expected number of personnel required to provide support on a 24 hours/7 days basis)?

1.6.6 Which in-service support services would you provide on an annual basis? Can you provide ROM annual cost estimates and, where applicable, annual licensing and maintenance fees.

1.7 Risk

1.7.1 Do you foresee other risk areas not listed in the following table?

Technical Risks	Security Risks	External Risks	Organizational Risks	Project Management Risks
• Requirements • Technology • Innovation • Integration • Complexity and Interfaces • Functionality • Performance and Reliability • Quality	• Personnel • Physical • Information • Information Technology • Industrial • Contract	• Operational • Subcontractors and Suppliers • Regulatory • Market • Customer/Client • Weather/Environment	• Project Dependencies • Resources: - Human Resources - Funding - Training - Infrastructure • Prioritization • Legal	• Scope • Schedule • Estimating • Planning • Controlling • Communication

1.7.2 Based on your experience, how would you quantify each identified risk, using a Low, Medium or High scale?

1.7.3 Which five capabilities from those described in Annex A - section 5 would you rate as the highest risk from a technical perspective? Please list from highest to lowest and provide a short justification.

1.8 Contracting

1.8.1 What delivery approach (e.g., buy, lease or combination) would you recommend for delivering the IT infrastructure and proposed solution(s)? Please explain why.

1.8.2 What contracting approach (e.g., single contract under one prime, multiple contracts under a single or multiple primes) would you recommend for delivering the IT infrastructure? Please explain why.

1.8.3 What contract(s) length (including option years) would you recommend for leased portions of the IT infrastructure? Please explain why.

1.8.4 What delivery and contracting approaches would you recommend for in-service support after deployment, including duration period and options? Please explain why.

1.8.5 What delivery and contracting approaches would you recommend for training support after deployment, including duration period and options? Please explain why.

1.9 Evaluation

1.9.1 What technical evaluation approach would you recommend for evaluating supplier proposals? Please explain why.

1.10 Industrial Technical Benefits (ITB) and Value Proposition (VP) Industry Engagement Questions

Defence Sector

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

1.10.1 Based on the technical specifications put forward by the Department of National Defence, describe what Direct Work activities, in the KICs identified in section 5.2.1, your company would foresee undertaking in Canada for the production and the sustainment of the ITI in SP of C2 project?

Supplier Development

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

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

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

Skills Development and Training

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

1.10.4 What types of Skills Development and Training investments would produce the maximum benefit to Canada (defence or commercial sector)?

a. Examples:
    i. Work integrated learning programs (e.g., co-operative education; work placements);
    ii. Apprenticeship programs;
    iii. A new or existing skills development program at or through a post-secondary institution (e.g. coding and programming, network engineering, and software development and integration);
    iv. Support for security certifications (e.g.: Top Secret, ITAR) or cybersecurity compliance certifications for Canadian companies, especially small and medium-sized businesses.

Research and Development (R&D)

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

1.10.5 Are there opportunities to partner with Canadian post-secondary or publicly-funded research institutions to perform Direct Work on the ITI in SP of C2 project?

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

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

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

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

Export

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

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

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

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

Other Questions

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

1.10.13 Comparatively to price and technical merit, Value Proposition typically has a weight of 10% of the overall bid evaluation. What is your view on the weighting of the Value Proposition for the ITI in SP of C2 project?

1.10.14 Within the Value Proposition, what are your recommended minimum percentages of weighting for each of the Value Proposition pillars (i.e. Defence Sector, Supplier Development, Skills and Training, R&D, and Exports)?

ANNEX A: ITI IN SP OF C2 PROJECT BACKGROUND

1 INTRODUCTION

This Annex provides a general, high-level description of the ITI in Sp of C2 Project so that potential suppliers may estimate and gauge the scope and degree of complexity involved. Suppliers are asked to review this information with a view to providing an understanding of solution cost drivers and how the quantitative descriptors described below can be used to indicate solution costs for each performance specification/requirement defined in Annex C.

More detailed information will be provided to suppliers at a later stage in the industry engagement process.

2 PROJECT DESCRIPTION

The ITI in Sp of C2 Project will implement a secure, integrated Secret-level IT infrastructure that will converge and reduce the number of DND/CAF Secret networks, provide enhanced connectivity and information sharing capabilities within the DND/CAF and with our mission partners, and readily evolve to meet future challenges. The project will enable commanders across the CAF to exercise C2, including at deployed headquarters, using the latest available technologies to provide optimal support capabilities. To achieve its objectives, the project will leverage industry capabilities and efficiencies to deliver services to the maximum extent possible. The project is expected to identify a preferred implementation option by end-June 2019, which will be followed by the Definition Phase and then the Implementation Phase; IOC is planned in June 2025, and FOC in September 2027.

The ITI in Sp of C2 Project will redesign and recapitalize the capabilities, services and governance of the current C2 Secret IT infrastructure, with the aim of addressing core deficiencies and meet the Chief of the Defence Staff's (CDS) vision of an integrated C2 Information System (C2IS). It will upgrade the C2 Secret IT infrastructure to provide users with secure integrated, and timely access to all operational and business information they need and have a right to, interoperate with government agencies, allies, and other partners, support data intensive services, such as data fusion and targeting, and readily evolve to meet future challenges. This will be realized by implementing a cohesive and integrated Secret-level IT infrastructure that will converge and reduce the number of disparate Secret networks and provide enhanced connectivity to make it easier to share and exchange data, video, multimedia and telephony within the DND/CAF and with our mission partners, including across security domains.

The project will provide the enduring information processing and exchange capabilities for the national Secret-level C2 systems connecting DND/CAF entities across the country. This connectivity will enable commanders across the CAF to exercise C2, including through collection and processing of information from a wide variety of sources, planning and making decisions, directing, coordinating, and controlling forces in order to gain operational advantage over adversaries.

In addition, the project will enable the connectivity to specified deployed entities at the operational and tactical levels both in Canada and abroad. For example, these may include a CAF Joint Task Force (JTF) headquarter deployed as part of a coalition in the Middle East, a Regional JTF (RJFT) deployed headquarter providing disaster assistance in British Columbia, or a frigate deployed on Operation ARTEMIS in the Arabian Sea. In any of these deployed missions, there will be an episodic environment established for the mission commander to exercise C2 over assigned forces. These deployed networks will generally be established by the lead RJTF, lead nation or command, and require both reach-back connectivity to the DND/CAF C2 Secret IT infrastructure, and interoperability with other deployed networks. The architecture of these deployed networks will comply with the Canadian Deployed Mission Network (CDMN), United States (US) Mission Partner Environment (MPE), and North Atlantic Treaty Organization (NATO) Federated Mission Network (FMN). The ITI in Sp of C2 Project will provide connectivity to those Canadian deployed elements and associated deployed networks to support the national C2 functions of the CDS, Commander Canadian Joint Operations Command (CJOC), and

Canadian national contingent Commanders. This capability will provide robust access to services and authoritative information sources residing on DND/CAF, GC, US (including the North American Aerospace Defense Command (NORAD)), Five-Eyes (FVEY) and NATO networks, which may be unavailable on the mission network. The project will provide the IT infrastructure component to enable technical and information interoperability; and, provide reliable, timely, and secure information exchange and processing services. Connectivity to these deployed entities will be achievable via a variety of different means, including the Internet, satellite communications, and strategic radio systems (note: the provision of new satellite and strategic radio system communications systems is out of scope for this project).

Of note, the project will leverage, to the maximum extent possible, existing and planned DND/CAF engineering initiatives to minimize any risk(s) associated with the design, implementation and integration of the new C2 Secret IT infrastructure (e.g., Cross Domain Solutions (CxDS)). The designs and capabilities developed thus far will be made available to suppliers for use as required/appropriate.

3 IMPLEMENTATION STRATEGY

Initial analysis has determined that the project will most likely need to use a Build/Buy Hybrid procurement approach to meet project objectives. Under the Build/Buy Hybrid approach, the DND/CAF will partner with industry to design, build, implement and integrate the new Secret IT infrastructure, but retain the lead system integrator role and the ability to provide and mandate key solutions for part of the infrastructure.

Procurement specifics (e.g., national security exception requirements, single or multiple contracts, etc.) will be identified as the capability options are further analysed.

4 CURRENT SECRET IT INFRASTRUCTURE – QUANTITATIVE DESCRIPTORS

The following quantitative descriptors approximate the current DND/CAF Secret IT infrastructure (including stand-alone networks) and are intended to provide a baseline overview to set a starting point for analysis, keeping in mind the capability growth and improvements planned under this project within the size and capability constraints applicable to the DND/CAF:

- Users: 15,000
- Software applications: 150
- Miscellaneous Servers: 1,000
- Workstations (thick and thin clients): 10,000
- Routers and switches: 800
- Points of presence (urban and remote): 125
- Domestic data centres (2): 60 Petabytes each
- Deployed data centres (typical - 10-15 at any given time): 100 Terabytes in each location
- Bandwidth - Urban sites: 20 Megabits per Second (Mbps)
- Bandwidth – Desktop: 100 Mbps

5 PROJECT CAPABILITIES AND TECHNOLOGIES OF INTERESTS

Among others, the ITI in Sp of C2 Project will be looking at the following capabilities and technologies as potential solutions to achieve project objectives (noting that operating in the classified domain imposes a number of security conditions with respect to the use of some capabilities and technologies):

a. Cloud computing (including surge capabilities):

- Public cloud
- Private cloud
- Hybrid cloud
- IT as a Service (ITaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Application containers
- Microsoft Office 365

b. Data centres:

- Software defined (virtualization)
- Centralized and distributed
- Storage solutions
- Backup and recovery solutions
- Archiving solutions

c. Microsoft Active Directory

d. ICAM

- Digital identity service[1]
- Credentialing service[2]
- Privilege Management service[3]
- Authentication service[4]
- Authorization and Access service[5]
- Cryptography service[6]
- Auditing and Reporting service[7]

e. ABAC and RBAC

f. PKI

g. Digital/Individual Rights Management

h. Microsoft Exchange email services

i. Web services

j. Chat services

k. Voice over Internet Protocol (VoIP) services

l. Secure Video Tele-Conferencing (SVTC) services (conference rooms and desktop)

m. Real-time Full Motion Video (FMV) support

n. Host Protection

- Management
- Host Firewall
- Host Application Control
- Host Authentication
- Host Integrity check
- Host Intrusion Prevention System
- Malware Protection

- Port Control
- Device Control
- Removable Media Encryption
- File/Folder Encryption
- Full Disk Encryption
- File Label Checking
- Message Label Checking
- Remote Wipe
- Secure Configuration Compliance
- Rogue Host Detection

o. Networking:

- Dynamic routing
- Multicast
- Wireless Local Area Networks
- Virtualized networking
- Software Define Networking (SDN)
- Network Function Virtualization (NFV)
- Quality of Service (QoS)
- Network Monitoring
- Network optimization
- Integration with low bandwidth site (i.e., connected via satellite)

p. Encryption of classified data at rest, using either, or both, Government Off-the-Shelf (GOTS) and Commercial Off-the-Shelf (COTS) (i.e., Commercial Solutions for Classified (CSfC)) systems

q. Encryption of classified data in transit, using either or both GOTS and COTS (i.e., CSfC) systems

r. Labelling of data (i.e., metadata and security markings of documents down to paragraph level)

s. Information Exchange Gateway (IEG) within the Secret domain (email, chat, web, file sharing, Internet Protocol (IP) telephony, SVTC services, directory services exchanges, and specialized applications)

t. Transfer CxDS within the Secret domain and across security levels (email, chat, web, file sharing, IP telephony, SVTC services, directory services exchanges, and specialized applications)[8]

u. Multi-level security system (an enhanced reliability user accessing unclassified data on the secret infrastructure)

v. End-users devices:

- Access CxDS[9]
- Thick client
- Thin client (Virtual Hosted Desktops/Virtual Desktop Infrastructure (VHD/VDI))

w. Business continuity services

x. Disaster recovery services

y. Information Technology Infrastructure Library (ITIL) processes and COTS supporting tools:

- Asset management (Hardware and Software)
- Configuration management
- Change management
- Release management

- Etc.

z. Centralized management and monitoring system:

- Network monitoring and management
- Data Center monitoring and management

aa. Integrated Logistic Support (ILS)

- Training
- ISS

Notes:

[1] Digital identity is the representation of identity in a digital environment. Digital Identity Services comprise the processes required to capture and validate information to uniquely identify an individual, determine suitability/fitness, and create and manage a digital identity throughout the life cycle.

[2] Credentialing is the process of binding an identity to a physical or electronic credential, which can subsequently be used as a proxy for the identity or proof of having particular attributes.

[3] Privilege Management comprises the set of processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual‘s access profile. These attributes are features of an individual that can be used as the basis for determining access decisions to both physical and logical resources. It governs the management of the data that constitutes the user‘s privileges and other attributes, including the storage, organization and access to information.

[4] Authentication is the process of verifying that a claimed identity is genuine and based on valid credentials. Authentication typically leads to a mutually shared level of assurance by the relying parties regarding the identity. Authentication may occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, PKI and/or other techniques.

[5] Authorization and Access are the processes of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities. It ensures individuals can only use those resources they are entitled to use and then only for approved purposes, enforcing security policies that govern access throughout the enterprise.

[6] Cryptography supports the use and management of ciphers including encryption and decryption processes to ensure the confidentiality and integrity of data, including necessary functions such as Key History and Key Escrow. Cryptography is often used to secure communications initiated by humans and Non-Person Entities (NPE).

[7] Auditing and Reporting addresses the review and examination of records and activities to assess the adequacy of system controls and the presentation of logged data in a meaningful context.

[8] Transfer CxDS are high assurance technologies which securely enable the transfer or access to information between security domains by employing robust content inspection and flow enforcement. CxDS provide the lowest risk, National Security Agency/Communications Security Establishment (NSA/CSE) endorsed, means to connect different security domains.

[9] Access CxDS provide users with a single computing environment to access multiple security domains. For example, a user accessing two security domains could have a Defence Wide Area Network (DWAN) and a Consolidated Secret Network Infrastructure (CSNI) desktop displayed on a single screen. Users can move between security domains in the same manner they switch between Internet browser windows. Each domain remains independent as no information is transferred or accessible outside of its domain.

6 PROJECT STATUS

The project is being conducted in accordance with the DND standard project framework and is currently in the Options Analysis Phase. The Options Analysis Phase will investigate and evaluate the broad options identified during the previous Identification Phase, complete the Business Case Analysis, and then recommend a preferred option for moving the project to implementation (note that the preferred option could be a variant of, and/or even different from, the currently proposed options, should the Options Analysis Phase investigations, including inputs from industry and other stakeholders, justify it).

The project has identified the following three options for investigation:

Option 1 – More than One Secret Network. A single Secret integrated network may not be possible based on available technological solutions, security policies or non-acceptable risks. In this option, the 25 or more classified networks would be consolidated into a single networking infrastructure supporting multiple (but a reduced number of) Secret-level security domains (i.e., caveats and sensitive Communities of Interest (COIs)), with security domains isolated from one another (e.g., through dedicated unencrypted IT components and virtual separation where appropriate). Users would use a single terminal to access the separate security domains but require a separate login for each of them. Using that single terminal, users would be able to view data from multiple Secret-level domains concurrently once logged into them, but would need to use the (automated) IEGs and CxDS to move information across the security domains. All users would require a Level II (Secret) security clearance.

Accurate, binded data labelling, through metadata tagging, would ensure that security classification, dissemination, handling and COI restrictions are enforced. An ICAM capability would enable user access to networks, applications, and services across the various networks. Support for the system would be streamlined as this consolidation would generate efficiencies and improve security.

Option 2 – **Single Secret Network.** In this option, the 25 or more classified networks would be consolidated into a single networking infrastructure supporting multiple, but a reduced number of, Secret-level security domains (i.e., caveats and sensitive COIs), with security domain separation enforced at the information level as opposed to system level (e.g., no requirement for dedicated unencrypted IT components or virtual separation). Security domains and COI separation would be enforced based on user credentials, access policies and restrictions, and authorization mechanisms. Users would have a single terminal, single login to the multiple security domains, and have concurrent access to all Secret data to which they are authorized from that single login, including moving information across security domains where appropriate. All users would have a Level II (Secret) security clearance.

This option would significantly shorten the time required to find, access, analyze, process and share critical operational and situational information. This enhanced capability would significantly improve commanders' ability to make decisions and increase the quality and speed of staff analysis, in order to gain operational advantage over adversaries. A data-centric security service would ensure that security classification, dissemination, handling and COI restrictions are enforced such that data access would be carefully controlled based on each user's security privileges and need-to-know. An ICAM system would enable user access to networks, applications, and services. Support for the system would be streamlined, as a single Secret networking infrastructure would be more efficient to manage and secure.

Option 3 – **Single Secret Networking Infrastructure Providing Services to Secret Users and Users without a Security Clearance.** In this option, the 25 or more classified networks would be consolidated into a single networking infrastructure supporting multiple, but a reduced number of, Secret-level security domains (i.e., caveats and sensitive COIs), with security domain separation enforced at the information level as opposed to system level (e.g., no requirement for dedicated unencrypted IT components or virtual separation). Security domains and COI separation would be enforced based on user credentials, access policies and restrictions, and authorization mechanisms.

Users with a Secret-level security clearance would have a single terminal, single login to the multiple security domains, and have concurrent access to all Secret data to which they are authorized from that single login, including moving information across security domains, where appropriate. Additionally, users without a Secret-level security clearance would have the ability to access Unclassified data held on the Secret networking infrastructure without gaining awareness of classified information, to support C2 activities conducted on Unclassified applications. This option would enable the migration of existing C2 support capabilities from the Unclassified to Secret networking infrastructures, and facilitate C2 processes spanning both security-levels without a requirement to clear all users operating at the Unclassified-level.

This multi-level access and security system would further shorten the time required for a user to find, access, analyze, process and share critical operational and situational information (both Secret and Unclassified) from a single terminal. This enhanced capability would also further improve commanders' ability to make decisions and increase the quality and speed of staff analysis, in order to gain operational advantage over adversaries. This capability would also ensure that uncleared users would be able to access only unclassified information residing on the Secret networking infrastructure. Infrastructure enhancements could be minimized by reusing existing DWAN infrastructure and CxDS. Key C2 support activities and capabilities operating at the Unclassified-level could be migrated to the new system, enhancing operational security by keeping relevant sensitive information at the Secret-level.

7 OPTIONS ANALYSIS PHASE ACTIVITIES

Options Analysis Phase activities will be conducted in accordance with the DND standard project framework, more specifically the DND Project Approval Directive.

This will include the evaluation of each viable option against the following rated criteria:

Description	Associated Measure(s) or Basis for Assessment and Rationale as necessary
Strategic Alignment	How does each option measure against the strategic outcomes?
Business Outcome Alignment	How does each option measure against the desired business outcomes?
Indicative Costs	What is the indicative implementation cost of each option? What is the indicative total cost of ownership, for the life of the system, for each option?
Cost-Benefit Analysis	How do the cost benefits that will be accrued from each option compare? (Cost-effectiveness, Displaced or Avoided costs)
Implementation and Capacity	How does each option compare with respect to DND/CAF (human resources, processes, knowledge, materials, and infrastructure) capacity to successfully implement?
Risk Assessment	How does the risk profile of each option compare?
Benchmarks	How do the options compare with respect to industry-standards or allied forces' benchmarks?
Policy and Standard Considerations	How do the options compare regarding their impact on existing DND/CAF policies and standards (i.e., security, privacy, accessibility, Information Management, and Enterprise Architecture)?

Overall, the focus of the Options Analysis Phase work will be on the development and completion of:

a. the Business Case Analysis, supported by a preliminary SOR developed in consultation with operational stakeholders and industry, and cost data generated with the assistance of industry;

b. a substantive plan on how the Definition Phase will be conducted (including costs), including an integrated Defence Procurement Strategy (DPS) that is based on the evidence and experience gained from the industry engagement conducted during the Options Analysis Phase;

c. an indicative plan on how the Implementation Phase will be conducted (including costs); and,

d. an indicative plan on how the post implementation ISS and operations will be conducted (including costs).

With this work completed, the project will be brought for review, endorsement, and approval to the Defence Capability Board (DCB), DND Programme Management Board (PMB), Independent Review Panel for Defence Acquisition (IRPDA), and ultimately Treasury Board.

ANNEX B: MISSION ENVIRONMENT AND OPERATIONAL SCENARIOS

1 INTRODUCTION

1.1 Background

Canada's Defence Policy, Strong, Secure, Engaged, defines the CAF's core missions and defines the requirement for the CAF to execute concurrent operations.

The Minister of National Defence (MND) Mandate Letter also directs the CAF to be equipped and prepared, if called upon, to protect Canadian sovereignty, defend North America, provide disaster relief, conduct search and rescue, support United Nations peace operations, and contribute to the security of our allies and to allied and coalition operations abroad.

To fulfill these roles, the CAF must be an effective, agile, responsive, well-trained and well-equipped, modern military force with the core capabilities and flexibility to successfully address both conventional and asymmetric threats, including terrorism, insurgencies and cyber-attacks. Furthermore, the CAF must have the necessary capabilities to make a meaningful contribution across the full spectrum of operations, from humanitarian assistance to collective defence.

2 MISSION ENVIRONMENTS

2.1 CAF Core Mission and Concurrent Operation Requirements

Canada's Defence Policy, *Strong, Secure, Engaged,* specifies the CAF core mission and concurrent operations requirements (i.e., the mission support capabilities that the delivered IT infrastructure must fundamentally be able to support).

2.1.1 CAF Core Mission Requirements

- Detect, deter and defend against threats to or attacks on Canada.
- Detect, deter and defend against threats to or attacks on North America in partnership with the United States, including through NORAD.
- Lead and/or contribute forces to NATO and coalition efforts to deter and defeat adversaries, including terrorists, to support global stability.
- Lead and/or contribute to international peace operations and stabilization missions with the United Nations, NATO and other multilateral partners.
- Engage in capacity building to support the security of other nations and their ability to contribute to security abroad.
- Provide assistance to civil authorities and law enforcement, including counter-terrorism, in support of national security and the security of Canadians abroad.
- Provide assistance to civil authorities and non-governmental partners in responding to international and domestic disasters or major emergencies.
- Conduct search and rescue operations.

2.1.2 CAF Concurrent Operation Requirements

- Defend Canada, including responding concurrently to multiple domestic emergencies in support of civilian authorities.
- Meet its NORAD obligations, with new capacity in some areas.

- Meet commitments to NATO Allies under Article 5 of the North Atlantic Treaty.
- Contribute to international peace and stability through:
  - Two sustained deployments of ~500-1500 personnel, including one as a lead nation;
  - One time-limited deployment of ~500-1500 personnel (6-9 months duration);
  - Two sustained deployments of ~100-500 personnel and;
  - Two time-limited deployments (6-9 months) of ~100-500 personnel;
  - One Disaster Assistance Response Team (DART) deployment, with scalable additional support; and
  - One Non-Combatant Evacuation Operation, with scalable additional support.

2.2 Operating Environment

2.2.1 Access to the network, by commanders and staff across the country, will be from a variety of environments, including office space, operations rooms, and deployed locations, using workstations appropriate to the user's working environment (desktop computers, thin-client terminals, laptops, ruggedized laptops, etc.).

2.2.2 Royal Canadian Navy (RCN) afloat and Royal Canadian Air Force (RCAF) aloft assets will access the network through supporting RCN and RCAF infrastructure, respectively, which will allow users in these environments to gain access to the network. Similarly, Canadian Special Operations Forces Command (CANSOFCOM) assets will connect through unique infrastructure, appropriate to their location and mission.

2.2.3 ITI in Sp of C2 data centre assets will operate in an environmentally controlled physical environment, in a small number of key locations.

2.2.4 Networking infrastructure will be installed in all buildings where there are users. In these buildings, equipment spaces (communications closets) will be heated, but may not be air conditioned. In addition, connectivity will be extended to deployed headquarters, which may be in temporary structures including sea containers, vehicles (including trailers) and tents, which will offer some environmental protection, including air conditioning.

2.2.5 Access to the network by support personnel, will be from regional support locations, which will be located in office environments. Support personnel will also help users, at their work spaces, if required, and work on networking infrastructure wherever it is located. Some support personnel will be present in deployed locations.

2.2.6 The system will operate in the cyber environment with cyber-attack threats emanating from both asymmetric and conventional military forces. These threats could originate from state and non-state actors and affect both domestic and expeditionary operations. Additionally, although the network will not have direct Internet connectivity, it will be subject to externally originated cyber-attacks that have migrated into the classified network via other networks (for example, via an allied or other government department's network). It will also be vulnerable to internally originated cyber-attacks from ill-intended users, which may be promulgated by a memory stick or any other data transfer mechanism.

2.2.7 Connectivity between sites will be achieved via commercial means. As such, the classified networks will have a dependency on these communications assets, which have their vulnerabilities from both physical and virtual threats.

2.2.8 The Secret-level data stored on the network will be a valuable target for adversary attacks. It would provide information about CAF capabilities and posture as well as insight regarding DND/CAF knowledge of adversary activities, equipment and readiness. Detailed information regarding the configuration and status of the IT Services and IT Assets within the IT infrastructure will also be a valuable target for adversary cyber-attacks.

ANNEX C: PRELIMINARY STATEMENT OF REQUIREMENTS

1 GENERAL OPERATION

1.1 Concept of Operations (CONOPS)

The system will provide users with secure integrated, and timely access to all operational and business information they need and have a right to, interoperate with government agencies, allies, and other partners, and support data intensive services such as data fusion and targeting. This will be realized by implementing a cohesive and integrated IT Infrastructure that provides enhanced connectivity to make it easier to share and exchange data, video, multimedia and telephony within the DND/CAF and with our partners. Users will be able to exchange relevant information, in near-real time, across all security levels, from Unclassified to Top Secret, within the DND/CAF, and at the Secret-level with GC, US, Five Eyes and NATO partners, using automated information exchange and cross-domain solutions.

This capability will enable commanders across the DND/CAF to more effectively exercise C2, by enabling them and their staff to collect and process information from a wide variety of sources, plan and make decisions, and direct, coordinate, and control forces in order to gain operational advantage over adversaries.

Users will have timely, concurrent access to all the information they are authorized to view from a single terminal, significantly shortening the time required to find, access, analyze and process critical operational and situational information. Users will also be significantly more efficient in their tasks, as time will not be wasted logging-in to multiple systems, through different physical devices and infrastructure, and searching for data in a wide range of repositories. Instead, users would be able to log-in once, enter data once, share it broadly, and easily find information in an integrated information environment.

The system will provide core services (i.e., email, chat, web, file sharing, VoIP, SVTC, directory services) and enable C2 applications and other applications as appropriate. It will permit users to access information from any enduring location, and to disconnect and reconnect as required when on-the-move. It will also extend these services to operational deployments and missions around the globe, while facilitating the exchange of information with the dedicated mission network. It will also provide connectivity with afloat assets through supporting RCN Infrastructure, including the Naval Operations Centres (NOCs), and with aloft assets through supporting RCAF infrastructure found on the Main Operating Bases (MOB). For these afloat and aloft assets, services will be optimized to reflect the low-bandwidth environments within which these assets operate.

Operational security will be enhanced through the implementation of a multi-factor identification, credential, and access management system, which will provide a single system to control user access to networks, applications, and services across the various domains. Using a single credential and authentication will simplify and expedite granting access to the Secret information environment. In addition, operational security will be enhanced by increasing data-focused security, as access to information will be determined for each item of information, reducing the risk of users accessing information they are not authorized to see. In order for this capability to be realized, accurate, and indelible data labelling, through metadata tagging, will be implemented to ensure that security classification, dissemination, handling and COI restrictions are enforced. This will require users to label and categorize all information in the system as it is being generated and stored in the repository.

Access to the system by users will be highly reliable, as availability will be enhanced by the system's ability to recover from or adjust to misfortune and damage as a result of essential computing, networking and storage components redundancy. It will be designed to degrade in pre-determined fashion in adverse conditions in accordance with the commanders' priorities, and will be capable of continuing to provide computing services during loss of connectivity to the system backbone. It will dynamically and automatically adjust to users' changing roles, environments, and computing, networking and storage requirements, including during surge requirement periods (temporary basis).

In addition, the system will enable the connectivity to specified deployed entities at the operational level both in Canada and abroad. For example, this could include a CAF JTF headquarter deployed as part of a coalition in the Middle East, a RJTF deployed headquarters providing disaster assistance in British Columbia, or a frigate deployed on Operation ARTEMIS in the Arabian Sea. The system will provide connectivity to those Canadian deployed elements and associated deployed networks to support the national C2 functions of the CDS, Commander CJOC, and Canadian National Contingent Commanders.

For deployed elements, the system will provide access to services and appropriate authoritative information sources that reside in information environments provided by DND/CAF, GC, US (including NORAD), Five Eyes and NATO, which are unavailable on the mission network. The system will provide a scalable capability including core services, storage, computing and application servers appropriate for the deployed element. The deployed system will remain in theatre for the duration of the operation, and will be able to be built-up or scaled back as required throughout the duration of the mission.

The detailed CONOPS will be developed during the Definition Phase of the project as system design, key performance measures and functional specifications are defined. The detailed CONOPS will include the personnel roles and responsibilities, their process and procedures, and their information exchange requirements.

1.2 Project Scope

Included	Excluded
Classified military C2 and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) networked data, including: telephony, multimedia services, and video, to connect sensors, sensor platforms, communications, and network assets. This includes: black and red Wide Area Networks (WANs), LANs, and IP telephony services.	Top Secret and general purpose unclassified and designated data and voice communications services.
Connectivity achieved via satellite communications systems, including the procurement of additional bandwidth, leveraging existing satellite services.	Acquisition of new satellite communications systems.
Information gateways to extend data and information sharing with our Joint, Interagency, Multi-National and Public (JIMP) partners. This includes CxDS, encompassing both access and data transfer capabilities.	Provision or acquisition of strategic radio frequency communication systems.
Classified collaboration and electronic workspace services including e-mail, chat, and directory services.	Development or enhancement of applications to support C4ISR processes.
Distributed computing services including client hardware, operating systems, file and print sharing, and remote access services.	Procurement of mobile connectivity services or devices.
Production and operations computing services including servers, system management, capacity management, problem and event management, configuration and change management, and data centre services (including storage solutions).	

Data and information security services, including secure labeling, and data-centric security services.	
IT Security services including comprehensive identity, credentialing and access management, network and perimeter security, anti-virus, and commercial encryption services.	
Integrated Logistics Support including training, service support, technical data, etc.	

2 GENERAL DELIVERABLES

2.1 Project deliverables include:

- Implementation of a modernized, standardized and sustainable computing, storage, networking, and core collaboration and electronic workspace enterprise services, allowing access to all services and information from any single point of access.
- Elimination of single points of failure by implementing redundancy for computing, storage and networking services, local access diversity, and disaster recovery capabilities.
- Upgrades to existing IT infrastructure capabilities, including: increasing bandwidth and the user base; implementing multicast, wireless networking, user/role based access, network optimization, and business continuity capabilities; and, improving data and information security services (including, data labelling, and identity and credential access management).
- Minimizing the number of DND/CAF Secret networks, through integration into a unified networking infrastructure supporting both Secret Releasable to Canada and US (Secret CANUS) and Secret CEO domains.
- Implementation of a new operations and service management framework by implementing, among others, asset, configuration, release and deployment, capacity, availability, incident, problem, and network monitoring/operations management.
- Implementation of concurrent access to the Secret and Unclassified Security domains from a single terminal.
- Implementation of new enterprise IEGs and CxDS to increase data and information exchange capabilities across security domains within the DND/CAF and with the GC, allies and partners.
- Enhancement to episodic integration, by increasing reach-back capability, consolidating and upgrading network gateways, and implementing single identities.
- Implementation of a standardized modular episodic headquarters capability, by eliminating duplicate capabilities, and a standard headquarters deployable kit using a modular approach to meet the specific requirements from each Environmental Chief of Staff (ECS).
- Definition of a common enterprise architecture to support integration and evolution.
- Implementation of a full ILS capability.

2.2 Preliminary Requirements

Note: As the project is still in the early stage of requirements definition, the following list is neither complete nor confirmed. Among others, a number of listed items include a “TBC” (i.e., to be confirmed), indicating that the element in question remains opened to discussion with internal stakeholders, and also to industry feedback and suggestions. That said, the enclosed list should provide industry with a general picture of the capabilities that the project aims to implement, noting that there is no assumption at this point in time as to which capabilities would be delivered by industry and government respectively.

2.2.1 The Secret IT infrastructure must provide the computing, networking and storage capabilities required to effectively support the core missions and concurrent operations requirements of Canada’s

Defence Policy - Strong, Secure, Engaged (SSE), over a standardized, unified strategic and operational Secret C2 IT infrastructure core.

2.2.1.1 The Secret IT infrastructure must integrate all specified DND/CAF Secret networks (over 25 Secret networks) onto a single networking infrastructure.

2.2.1.2 The Secret IT infrastructure must provide the required computing, networking and storage capabilities to support users operating at both the Secret CEO and Secret CANUS levels.

2.2.1.3 The Secret IT infrastructure must be able to support at least 25,000 users.

2.2.1.4 The Secret IT infrastructure must allow users to access all required data from a single terminal.

2.2.1.5 The Secret IT infrastructure must provide users a single logon to all services and domains.

2.2.1.6 The Secret IT infrastructure must provide email capabilities.

2.2.1.7 The Secret IT infrastructure must support data, voice, and video.

2.2.1.8 The Secret IT infrastructure must provide chat capabilities.

2.2.1.9 The Secret IT infrastructure must provide web capabilities.

2.2.1.10 The Secret IT infrastructure must provide file sharing capabilities.

2.2.1.11 The Secret IT infrastructure must provide IP telephony capabilities.

2.2.1.12 The Secret IT infrastructure must provide conference room Secure IP SVTC.

2.2.1.13 The Secret IT infrastructure must provide desktop IP SVTC capabilities.

2.2.1.14 The Secret IT infrastructure must provide directory service exchanges.

2.2.1.15 The Secret IT infrastructure must provide an Information Resource Management System (IRMS) and/or be compatible with the legacy CSNI IRMS.

2.2.1.16 The Secret IT infrastructure IP telephony must be interoperable with/or replace the Canadian Defence Red Switch Network (CDRSN), as applicable. (Note: The CDRSN is an extension of the US DRSN, and includes multilevel secure voice and voice-conferencing capabilities.)

2.2.1.17 The Secret IT infrastructure must provide high definition conference room IP SVTC capabilities.

2.2.1.18 The Secret IT infrastructure conference room IP SVTC capabilities must be able to display at least eight (TBC) participants concurrently on a single screen.

2.2.1.19 The Secret IT infrastructure must be able to provide desktop IP SVTC capabilities at all user terminals.

2.2.1.20 The Secret IT infrastructure desktop IP SVTC capabilities must be able to support at least eight (TBC) participants concurrently.

2.2.1.21 The Secret IT infrastructure must support C2 applications migrated from legacy Secret IT infrastructures (e.g., CSNI).

2.2.1.22 The Secret IT infrastructure must support C2 applications used on the Land Command and Control System (LCSS) (or successor) and CDMN (or successor).

2.2.1.23 The Secret IT infrastructure must support SharePoint and other collaboration tools migrated from the legacy Secret IT infrastructures.

2.2.1.24 The Secret IT infrastructure must provide archiving capabilities.

2.2.1.25 The Secret IT infrastructure must provide shared, secure printing capabilities (at least one per site and one per 100 staff - TBC).

2.2.1.26 The Secret IT infrastructure must provide shared scanning capabilities (at least one per site, one per 100 staff - TBC).

2.2.1.27 The Secret IT infrastructure data must be computed and stored in Canada or, where applicable, Canadian controlled locations (e.g., overseas Canadian embassy or theatre headquarters).

2.2.1.28 The Secret IT infrastructure must operate on a 24 hours/7 days basis.

2.2.1.29 The Secret IT infrastructure must include five (TBC) deployable networking, computing and storage core for in-theatre deployment and use, able to operate autonomously in the event of loss of reach-back capability.

2.2.1.30 The Secret IT infrastructure must be able to integrate with CDMN on new deployments within 24 hours (TBC).

2.2.1.31 The Secret IT infrastructure must support the NATO Core Metadata Specification (NCMS).

2.2.1.32 The Secret IT infrastructure must support all approved DND/CAF metadata specifications complementing the NCMS, where required.

2.2.1.33 The Secret IT infrastructure must support 30% (TBC) computing, networking and storage yearly growth.

2.2.2 The Secret IT infrastructure must provide the DND/CAF enduring, episodic operational, and specified tactical level entities connectivity.

2.2.2.1 The Secret IT infrastructure must interconnect all DND/CAF locations across Canada (estimated at over 400 locations of diverse sizes, some of which may be in a common geographical environment).

2.2.2.2 The Secret IT infrastructure connectivity must leverage existing Shared Services Canada (SSC) and DND/CAF telecommunications services to the maximum extent possible.)

2.2.2.3 The Secret IT infrastructure must provide connectivity and services to episodic strategic and operational systems deployed within and without Canada.

2.2.2.4 The Secret IT infrastructure connectivity to episodic strategic and operational systems must have the capability to use both government and commercial telecommunications services (specified on a case-by-case basis).

2.2.2.5 The Secret IT infrastructure must provide connectivity and services to ships afloat (e.g., frigates) through RCN telecommunications systems.

2.2.2.6 The Secret IT infrastructure must provide connectivity and services to planes aloft (e.g., Aurora) through RCAF telecommunications systems.

2.2.2.7 The Secret IT infrastructure must provide connectivity to DND/CAF permanent establishments and delegations located outside Canada (e.g., NORAD Headquarters, NATO Headquarters, Canadian Defence Liaison Staff (Washington) (CDLS(W)), etc.).

2.2.2.8 The Secret IT infrastructure must provide connectivity to DND/CAF Liaison Officers/staff located within and without Canada.

2.2.2.9 The Secret IT infrastructure must provide connectivity to CAF Military Attachés located within and without Canada.

2.2.2.10 The Secret IT infrastructure must provide connectivity and services to specified tactical level entities (e.g., LCSS, Joint Secure information Service, etc.).

2.2.2.11 The Secret IT infrastructure connectivity to tactical level entities must have the capability to use both government and commercial telecommunications services (specified on a case-by-case basis).

2.2.2.12 The Secret IT infrastructure must implement common interfaces for all connectivity capabilities.

2.2.2.13 The Secret IT infrastructure services must support mobile users who connect and re-connect to the network.

2.2.2.14 The Secret IT infrastructure must provide connectivity to the Government of Canada Secret Infrastructure (GCSI).

2.2.2.15 The Secret IT infrastructure must provide connectivity to SIGNET (C5 or subsequent version).

2.2.2.16 The Secret IT infrastructure must provide connectivity to the US SIPRNet (incl. the NORAD Enterprise Network (NEN)).

2.2.2.17 The Secret IT infrastructure must provide connectivity to the United Kingdom (UK) Secret Local Area Network (LAN) Internet/Joint Command and Control Support System (SLI/JC2SS).

2.2.2.18 The Secret IT infrastructure must provide connectivity to the AUS DSN/JCCS.

2.2.2.19 The Secret IT infrastructure must provide connectivity to the NZL Secret WAN.

2.2.2.20 The Secret IT infrastructure must provide connectivity to the NATO Secret WAN (NSWAN).

2.2.2.21 The Secret IT infrastructure must provide connectivity to the NATO Battlefield Information Collection and Exploitation System (BICES).

2.2.2.22 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of email services.

2.2.2.23 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of chat services.

2.2.2.24 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of web services.

2.2.2.25 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of file sharing services.

2.2.2.26 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of IP telephony services.

2.2.2.27 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of conference room IP SVTC services.

2.2.2.28 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of desktop IP SVTC capabilities services.

2.2.2.29 The Secret IT infrastructure must provide connectivity with adequate bandwidth capacity to support the requirements of directory service exchanges services.

2.2.2.30 The Secret IT infrastructure IP telephony must provide connectivity with adequate bandwidth capacity to the CDRSN (if not discontinued).

2.2.2.31 The Secret IT infrastructure must provide connectivity with sufficient bandwidth capacity to support the requirements of identified C2 applications (e.g., Joint Battlespace Management Capability (JBMC)).

2.2.2.32 The Secret IT infrastructure must provide connectivity with sufficient bandwidth capacity to support the requirements of the Modernized Integrated Database (MIDB). (Note: MIDB is a general military intelligence database.)

2.2.2.33 The Secret IT infrastructure must provide connectivity with sufficient bandwidth capacity to support the requirements of SharePoint and other collaboration services.

2.2.2.34 The Secret IT infrastructure must provide connectivity with sufficient bandwidth capacity to support the exchange of raw and processed sensor data between identified locations, including real-time FMV (e.g., RCAF MOBs, RCN NOCs, Intelligence centres, etc.).

2.2.2.35 The Secret IT infrastructure must provide QoS capabilities able to ensure stringent network performance requirements specified for applicable services and capabilities, such as NORAD tracks, Indications and Warning, and targeting functions, are met.

2.2.2.36 The Secret IT infrastructure must support enduring connectivity to Canadian Forces Station (CFS) Alert (i.e., through a combined satellite and microwave link).

2.2.2.37 The Secret IT infrastructure must support connectivity through multiple satellite hops.

2.2.2.38 The Secret IT infrastructure must provide connectivity to identified enduring IT infrastructure service entities, including but not limited to, user desktop and mobile (e.g., laptop) terminals, platforms/sensors, gateways, printers, servers, and data centres.

2.2.2.39 The Secret IT infrastructure must support both IPv4 and IPv6.

2.2.2.40 The Secret IT infrastructure must support multicasting and broadcasting.

2.2.3 The Secret IT infrastructure must allow the seamless and effective exchange of information with specified partner Secret networks and across security domains.

2.2.3.1 The Secret IT infrastructure must use a secure IEG to exchange data at up to the Secret CANUS level with the US SIPRNet (incl. NEN).

2.2.3.2 The Secret IT infrastructure must use a secure IEG to exchange data at up to the Secret FVEY level with the UK SLI/JC2SS.

2.2.3.3 The Secret IT infrastructure must use a secure IEG to exchange data at up to the Secret FVEY level with the AUS DSN/JCCS.

2.2.3.4 The Secret IT infrastructure must use a secure IEG to exchange data at up to the Secret FVEY level with the New Zealand (NZL) Secret WAN.

2.2.3.5 The Secret IT infrastructure must use a secure CxDS to exchange data at up to the Secret CEO level with the GCSI and SIGNET (C5 or subsequent version).

2.2.3.6 The Secret IT infrastructure must use a secure CxDS to exchange data at up to the NATO Secret level with NSWAN and NATO BICES.

2.2.3.7 The Secret IT infrastructure must use a secure CxDS to exchange unclassified (i.e., Unclassified and Designated) information with DND/CAF and government unclassified infrastructures.

2.2.3.8 The Secret IT infrastructure must use a secure CxDS to exchange data at up to the Secret CEO level with the DND/CAF Top Secret Infrastructure.

2.2.3.9 The Secret IT infrastructure IEG and CxDS must be automated and require no human interaction for all data exchange transactions meeting pre-defined approval criteria (e.g., file type, presence of required confidentiality and general metadata labels, max size, etc.).

2.2.3.10 The Secret IT infrastructure IEG and CxDS must impound data exchange transactions that fall outside pre-defined approval criteria and generate a system alert for the impound action that is both transmittable (e.g., to an operations centre) and recorded in an associated system log.

2.2.3.11 The Secret IT infrastructure IEG and CxDS must have a maximum data latency of 0.5 sec (TBC) (for approved data exchange transactions).

2.2.3.12 The Secret IT infrastructure IEG and CxDS must support data exchange transactions generated through email, chat, web, file sharing, IP telephony, conference room and desktop IP SVTC services, and directory services exchanges, specified C2 applications, and other specified C2 support capabilities (e.g., collaboration services).

2.2.3.13 The Secret IT infrastructure IEG and CxDS must have the capability to prevent specified file types to be transferred.

2.2.3.14 The Secret IT infrastructure IEG must replace or be interoperable with legacy IEG PEGASUS capabilities, whichever is applicable.

2.2.3.15 The Secret IT infrastructure IEG and CxDS must perform virus scans on all file transfers.

2.2.3.16 The Secret IT infrastructure IEG and CxDS must produce audit trail records of all data transfer transactions requests and results.

2.2.4 The Secret IT infrastructure must allow DND/CAF users to concurrently access and display information residing in the Secret (all caveats) and unclassified domains using a single workstation.

2.2.4.1 The Secret IT infrastructure must support secure, concurrent access and display on a single terminal a minimum of six (TBC) different concurrent domains.

2.2.4.2 The Secret IT infrastructure must support secure, concurrent access and display on a single terminal of the Secret CEO, Secret CANUS and DWAN security domains as a baseline capability.

2.2.4.3 The Secret IT infrastructure must also (i.e., in addition to baseline capability) support secure, concurrent access to, and display on a single terminal of NSWAN for specified users.

2.2.4.4 The Secret IT infrastructure must also (i.e., in addition to baseline capability) support secure, concurrent access to, and display on a single terminal of BICES for specified users.

2.2.4.5 The Secret IT infrastructure must also (i.e., in addition to baseline capability) support secure, concurrent access to, and display on a single terminal of the US BICES-X for specified users.

2.2.4.6 The Secret IT infrastructure (single) terminal must display individual security domains on separate child windows contained within a main window.

2.2.4.7 The Secret IT infrastructure (single) terminal must allow users to resize, move, superpose, and minimize/maximize child windows.

2.2.4.8 The Secret IT infrastructure terminal main window must display in top and bottom background banners the most stringent security level and caveat(s) applicable across all security domains accessed (concurrently), including when some or all child windows are minimized.

2.2.4.9 The Secret IT infrastructure child windows must display in a top child window banners the security level and caveat(s) applicable to that child window.

2.2.4.10 The Secret IT infrastructure must use a single network cable/link to connect user terminals to the networking infrastructure (i.e., carry multiple security domains over the same network cable/link).

2.2.4.11 The Secret IT infrastructure must use commercially provided encryption capabilities approved for classified use between user terminals and the networking infrastructure (e.g., to LAN switches).

2.2.5 The Secret IT infrastructure must recover from or adjust to misfortune and damage through redundancy of core components, and degrade gracefully in accordance with commanders' priorities.

2.2.5.1 The Secret IT infrastructure must have an availability rate of 99.999% (TBC)

2.2.5.2 The Secret IT infrastructure must have a Mean Time Between Failure (MTBF) of 30 days (TBC).

2.2.5.3 The Secret IT infrastructure must provide redundant computing, networking (including IEGs and CxDS) and storage capabilities sufficient to ensure CAF C2 and DND/CAF operations continuity.

2.2.5.4 The Secret IT infrastructure redundant capabilities must meet the specified survivability geographic separation requirements (TBC).

2.2.5.5 The Secret IT infrastructure must include uninterrupted power supplies for all core computing and storage servers.

2.2.5.6 The Secret IT infrastructure must support data synchronization across the network.

2.2.5.7 The Secret IT infrastructure must include a data backup and recovery capability for all data servers.

2.2.5.8 The Secret IT infrastructure must perform a data backup of all data servers on a daily basis.

2.2.5.9 The Secret IT infrastructure must allow recovery of data backed during the previous 30 days within one hour during, and three hours outside, business hours (TBC).

2.2.5.10 The Secret IT infrastructure must allow recovery of data backed during the previous year (but older than 30 days) within one business day (TBC).

2.2.5.11 The Secret IT infrastructure must allow recovery of data backed outside the previous year within three business days (TBC). (Note: This requirement doesn't apply to data that has been formally transferred to Library and Archives Canada).

2.2.5.12 The Secret IT infrastructure must allow specified, essential users to continue performing their C2 duties on location when nodal connectivity is lost (i.e., until restoral of connectivity).

2.2.5.13 The Secret IT infrastructure must include disaster recovery sites for core C2 capabilities.

2.2.6 The Secret IT infrastructure must provide centralized operations and service management life cycle stages based on ITIL best practices, and timely alignment/re-alignment of IT services with operational and business needs.

2.2.6.1 The Secret IT infrastructure must provide a centralized change management capability to support change management processes.

2.2.6.2 The Secret IT infrastructure must provide a centralized service asset configuration monitoring and management capability to support service transition.

2.2.6.3 The Secret IT infrastructure must provide a centralized release and deployment management capability to support service transition.

2.2.6.4 The Secret IT infrastructure must provide a centralized knowledge management capability to support IT service management processes.

2.2.6.5 The Secret IT infrastructure must provide a centralized event management capability to support service operations and associated functions.

2.2.6.6 The Secret IT infrastructure must provide a centralized incident management capability to support service operations and associated functions.

2.2.6.7 The Secret IT infrastructure must provide a centralized problem management capability to support service operations and associated functions.

2.2.6.8 The Secret IT infrastructure must provide a centralized request fulfilment management capability to support service operations and associated functions.

2.2.6.9 The Secret IT infrastructure must provide a centralized service catalogue capability to support the service design aspect of service management life cycle and be able to interface with existing service management tool.

2.2.6.10 The Secret IT infrastructure must provide a centralized capacity planning capability to support IT service management processes.

2.2.6.11 The Secret IT infrastructure must provide a centralized IT service continuity to support the service design aspect of service management life cycle.

2.2.6.12 The Secret IT infrastructure must provide a service desk function operating under existing service management framework.

2.2.6.13 The Secret IT infrastructure must allow IT staff to remotely administrate the infrastructure.

2.2.6.14 The Secret IT infrastructure must allow IT staff to remotely administrate user terminals without closing the user’s session.

2.2.6.15 The Secret IT infrastructure must allow automated software updates.

2.2.6.16 The Secret IT infrastructure must allow remoted software updates.

2.2.7 The Secret IT infrastructure must dynamically and automatically adjust to changing roles, environments, capability, and service requirements

2.2.7.1 The Secret IT infrastructure must include the real-time capability to monitor the health and status of core computing, networking components and storage components.

2.2.7.2 The Secret IT infrastructure must include the real-time capability to produce operator alerts, report, and audit records on the health and status of core computing, networking components and storage components.

2.2.7.3 The Secret IT infrastructure must include the ability to re-align and re-configure core computing, networking and storage services in near-real-time.

2.2.7.4 The Secret IT infrastructure must include the ability to re-align and re-configure user and other entities' roles.

2.2.7.5 The Secret IT infrastructure must include a capability to support temporary computing, networking and storage requirement surges of up to 30% (TBC) in near-real-time.

2.2.7.6 The Secret IT infrastructure must not incur downtime as a result of dynamic adjustments to the allocation and re-allocation of computing, networking and storage resources.

2.2.8 The Secret IT infrastructure must support insertion of new capabilities without impacting other sub-systems or requiring modification to the IT infrastructure system baseline.

2.2.8.1 The Secret IT infrastructure must be designed and implemented using the latest IT technologies and in accordance with the latest IT trends (at end of design time), as applicable within other requirement constraints (e.g., security).

2.2.8.2 The Secret IT infrastructure must comply with the latest government standards, except where conflicting with military standards required to meet CAF C2 mission requirements.

2.2.8.3 The Secret IT infrastructure must comply to the latest commercial standards, except where conflicting with military standards required to meet CAF C2 mission requirements and government standards.

2.2.8.4 The Secret IT infrastructure must not use proprietary technologies on DND owned components, except where deemed unavoidable and specifically approved by DND.

2.2.8.5 The Secret IT infrastructure must use a modular system design wherever possible, except where deemed unavoidable and specifically approved by DND.

2.2.8.6 The Secret IT infrastructure must use commercial, military and government off-the-shelf products wherever available, except where deemed unavoidable and specifically approved by DND.

2.2.8.7 The Secret IT infrastructure must support the insertion of new technologies within six months (TBC) of DND/CAF request.

2.2.8.8 The Secret IT infrastructure must implement new technologies, products and capabilities with minimum disruption to CAF C2 and infrastructure operations.

2.2.8.9 The Secret IT infrastructure must be technologically refreshed every four (4) years (TBC), wherever applicable.

2.2.9 The Secret IT infrastructure must provide and maintain Confidentiality, Availability and Integrity (CIA) of data.

2.2.9.1 The Secret IT Infrastructure must ensure that Secret CEO is only released to Canadian Citizens, and that Secret CANUS is only released to Canadian or American Citizens.

2.2.9.2 The Secret IT infrastructure must comply with DND and GC CIA security policies and standards (including applicable agreements with allied partners).

2.2.9.3 The Secret IT infrastructure must have an Authorization to Operate (ATO) obtained from the DND/CAF through the Security Assessment and Authorization (SA&A) process.

2.2.9.4 The Secret IT infrastructure must use an ICAM capability.

2.2.9.5 The Secret IT infrastructure ICAM capability must use an approved PKI card-based multi-factor authentication.

2.2.9.6 The Secret IT infrastructure must include an approved PKI that provides data integrity and confidentiality, identification and authentication, and non-repudiation capabilities.

2.2.9.7 The Secret IT infrastructure must provide entity authorization capabilities to all resources and enforce dissemination controls and handling instructions.

2.2.9.8 The Secret IT infrastructure must support the creation and use of Communities of Interest (COIs).

2.2.9.9 The Secret IT infrastructure must enforce and support the use of security marking with emails.

2.2.9.10 The Secret IT infrastructure must enforce and support the use of security marking with chat messages.

2.2.9.11 The Secret IT infrastructure must enforce and support the use of security marking with web windows.

2.2.9.12 The Secret IT infrastructure must support and enforce the use of confidentiality metadata labels for all files.

2.2.9.13 The Secret IT infrastructure scanning capabilities must enforce the inclusion of a security label with scanned document.

2.2.9.14 The Secret IT infrastructure confidentiality labels must follow the security markings and formats defined in the National Defence Security Orders and Directives – Standard 6: Security of Information Standards.

2.2.9.15 The Secret IT infrastructure confidentiality metadata label capability must meet the requirements of NATO Allied Data Processing Publication (ADatP) 4774 - Confidentiality Metadata Label Syntax.

2.2.9.16 The Secret IT infrastructure confidentiality metadata label capability must meet the requirements of NATO ADatP-4778 – Metadata Binding Mechanism

2.2.9.17 The Secret IT infrastructure must include cyber defence capabilities.

2.2.9.18 The Secret IT infrastructure must provide signature and behavior-based malware detection and protection.

2.2.9.19 The Secret IT infrastructure must implement DND auditing capabilities.

2.2.9.20 The Secret IT infrastructure must provide DND the capability to produce audit reports and statistics.

2.2.9.21 The Secret IT infrastructure must allow DND ISSOs to access the infrastructure as required in the performance of their duties (e.g., security incident investigation).

2.2.9.22 The Secret IT infrastructure must provide DND the capability to perform forensic evaluations of security incidents.

2.2.9.23 The Secret IT infrastructure must use thin clients as the baseline (i.e., de facto) user terminal, except where specified otherwise (e.g., to support intensive computing requirements, such as local specialized intensive data processing).

2.2.9.24 The Secret IT infrastructure must enable the DND/CAF to restrict external media use and printing privileges for users.

2.2.10 The Secret IT infrastructure must implement a fully Integrated Logistics Support capability.

2.2.10.1 The Secret IT infrastructure must include the personnel required to provide in-service support (structure and contractor/DND/CAF personnel mix TBC in accordance with selected solution).

2.2.10.2 The Secret IT infrastructure must be delivered with all required technical data/publications for operations and support.

2.2.10.3 The Secret IT infrastructure must include the required facilities required to operate and support the system.

2.2.10.4 The Secret IT infrastructure must be delivered with the required spare parts to meet availability requirements for the first two years (2) (TBC) after delivery completion.

2.2.10.5 The Secret IT infrastructure must be delivered with support and test equipment required by DND/CAF personnel to perform their required support functions.

2.2.10.6 The Secret IT infrastructure deliverables must include Unclassified development and Secret pre-deployment facilities for evaluation and pre-integration of new capabilities and technologies.

2.2.10.7 The Secret IT infrastructure must be delivered with a system administrator training package.

2.2.10.8 The Secret IT infrastructure must be delivered with an operations and maintenance training package.

2.2.10.9 The Secret IT infrastructure must be delivered with a theatre deployment training package for operational headquarters CIS Staff Officers.

2.2.10.10 The Secret IT infrastructure must be delivered with an executive-level user training package.

2.2.10.11 The Secret IT infrastructure must be delivered with an advanced user training package (i.e., to provide local support to the executive and general user communities that would not warrant helpdesk-type support).

2.2.10.12 The Secret IT infrastructure must be delivered with a basic user training package.

2.2.10.13 The Secret IT infrastructure must be delivered with initial system administrator training.

2.2.10.14 The Secret IT infrastructure must include initial operations and maintenance training for specified IT personnel.

2.2.10.15 The Secret IT infrastructure must include initial theatre deployment training for specified operational headquarters CIS Staff Officers.

2.2.10.16 The Secret IT infrastructure must include initial executive-level user training for specified senior-level staff.

2.2.10.17 The Secret IT infrastructure must include initial advanced user training for specified personnel.

2.2.10.18 The Secret IT infrastructure must include initial basic user training for specified personnel.

2.2.11 The Secret IT infrastructure must remain under DND/CAF authoritative control.

2.2.11.1 The DND/CAF must be involved throughout the system life-cycle (conceive, design, build, and manage).

2.2.11.2 System/capability delivery must not impact upon the functional, operational, technical and security requirements defined by the DND/CAF authority without the DND/CAF authority's explicit approval and risk acceptance.

2.2.11.3 System/capability delivery must be readily transferable to a different service delivery organization in the event the primary service delivery agency becomes unable to satisfy the requirements identified by the DND/CAF authority.

2.3 Security Classification

2.3.1 The capabilities delivered by the ITI in Sp of C2 Project must be implemented in accordance with the requirements of the Security Assessment & Authorization Guideline (SAAG) process. A complete SAAG process will be conducted prior to implementation, resulting in the promulgation of appropriate direction regarding the implementation of the hardware, software, personnel and procedures necessary to meet the capability security requirements.

2.3.2 Any future procurement actions undertaken in support of the ITI in Sp of C2 Solution will require suppliers to be registered in the Controlled Goods Program, and may require suppliers to hold a Level II (Secret) clearance and potentially Level III (Top Secret) clearance issued by their respective national security agency. Some of the suppliers may also need to meet GC requirement for providing products and services with (classified) Canadian Eyes Only (CEO) restrictions.

2.3.3 Suppliers and their sub-contractors may be required to abide by Non-Disclosure Agreements or other security restrictions during follow-on industry engagement.

2.3.4 Given the risks and threats associated with the CAF C2 capabilities, the supply of many if not most components for this project will need to come from trusted manufacturers (i.e., Supply Chain Integrity). Accordingly, contractual requirements will be imposed on suppliers to provide appropriate assurance of the integrity, availability and confidentiality of CAF Secret C2 infrastructure components and services, and mitigate the threats and vulnerabilities associated with potentially vulnerable or shaped technologies. Section 6 in *Contracting Clauses for Telecommunications Equipment and Services (TSCG-01\G)* provides security clauses that can be included in PSPC contracts, and should be referred to for clarifications on Supply Chain Integrity security considerations.

2.4 Operational Availability

2.4.1 Operational availability will vary from high to very high across specific components/portions of the system. Specifics will be provided once identified at a later date.

2.5 Reliability

2.5.1 Reliability will vary from high to very high across specific components/portions of the system. Specifics will be provided once identified at a later date.

2.6 Environmental Sustainability

2.6.1 The delivered capability must meet DND standards for environmental stewardship.

2.7 Health and Safety

2.7.1 The delivered capability must not generate health or safety concerns for the operators over and above those imposed by the operational environment.

2.7.2 The delivered capability must comply with all the DND/CAF health and safety codes.

2.8 Delivery Requirements

2.8.1 The DND/CAF must be able to exercise authoritative control over the IT infrastructure.

2.8.2 The migration to the new IT infrastructure must not impact C2 continuity.

2.9 Personnel and Training Requirements

2.9.1 As the system replaces an existing capability for the DND/CAF, which will continue to support the same applications that were being used prior to implementation, the training needs for users should be minimal. The most significant change for users will be with respect to data labelling. This task is not currently required at the Secret or Unclassified levels and will place new demands on users. A Training Needs Assessment (TNA) will be conducted by the project team to determine the training required and the preferred delivery mechanism.

2.9.2 For the Network Administrators, the training needs will have to be determined, as the changes to the system configuration and management toolset will not be clearly understood until the Implementation Phase.

2.9.3 Environmental and joint communications advisors (N6/G6/A6/J6) may need training in order to understand the capabilities of the new system, be able to plan for its implementation and deployment, and provide advice to commanders and staff regarding the operational use of the new IT infrastructure.

ANNEX D: FEEDBACK FROM INDUSTRY

1 INTRODUCTION

1.1 Given that so much of the information required to conduct a thorough and meaningful Options Analysis comes from Industry in general and that success of the project will depend entirely on the ability of Industry to support and deliver in some way, the project intends to actively engage and consult Industry throughout the OA and Definition Phases to develop a coherent and effective Defence Procurement Strategy and thus ensure a successful project end-state.

1.2 Feedback from industry will assist the DND/CAF project team to define:

a. the SOR in a manner that is understandable by industry and meaningful to the DND/CAF operational context, and thus contribute to better describing the business needs;

b. the “art of the possible” regarding IT capabilities, future developments within industry, and how similarly large corporate organizations are changing to meet their evolving IT needs, leading to a better definition of the SOR, budget and schedule required to meet the project objectives (both technological and industrial/procurement);

c. the impact on people, processes and technology of various concepts proposed and the organizational changes that will be required to support each conceptual solution;

d. the nature and sources of project costs, including the need for Definition Phase tasks, Implementation Phase costs and long-term ISS; and,

e. the most appropriate procurement strategy that is amenable to industry to deliver the right equipment to the DND/CAF in a timely manner, leveraging the purchases to create jobs and growth, and streamline procurement processes.

2 RESPONSE TO LETTER OF INTEREST

2.1 Industry is invited to respond to this LOI and provide the following information no later than the specified closing date/time. Respondents are asked to consider the following in preparing their response:

a. use the written format of respondent`s choice, but keep the same section numbering to facilitate Canada’s review and analysis of all responses;

b. the number of pages of respondent`s submission is not limited; however, the expected length should not exceed 30 pages single sided standard business format;

c. if the size of the document does not exceed six MB, respondents are asked to submit their response in unprotected (i.e., no password) PDF format by email to: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca, otherwise, respondents are asked to save a copy of their PDF (2003 or later) document onto each of two USB memory drives and mail them to the Contracting Officer(s) specified in section 2.7 of the solicitation;

d. The layout of the submission should follow this proposed format:

1) Section 1: Executive Summary – 1 to 2 pages, summarizing the submission in total.

2) Section 2: Corporate Profile:

a) identify a lead point of contact for the respondent;

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

c) describe intent to be the prime system integrator, a potential subcontractor or a supplier of products and/or services;

d) describe established partnerships with other industries, if any, that would be of benefit to the development of the project capability requirements; and,

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

3) Section 3: Company Background:

a) Ownership - Please indicate whether your company is Canadian owned or foreign owned.

b) Business:

i Size

ii Number of people your company employ

iii Your company's annual revenues

c) Who are your customers?

d) Structure:

i Do you belong to a parent entity?

ii Do you have any subordinate enterprises?

e) History:

i How many years of experience does your company have in delivering Information Management/Information Technology (IM/IT) solutions for a complex network?

ii How many years of experience does your company have in partnering to deliver IM/IT Solution?

f) Locations:

i Where do you have business operations?

ii Where is your organization headquartered?

g) Certifications - Which certifications does your organization hold/meet? International Organization for Standardization (ISO) 9001, Six Sigma, Capability Maturity Model Integration (CMMI), etc.

h) Security Clearance:

i. What is the security clearance of your personnel? How many employees have a Level II (Secret) and Level III (Top Secret) Clearance?

ii. What level of documents is your organization cleared to safeguard?

iii. If your organization and/or personnel don't hold any valid security clearances, are you/they willing to undergo the security clearance/document safeguarding process?

4) Section 4: Observations and Advice - Respondents are asked to provide:

a) comments, remarks, and advice concerning any aspect of the material contained within this LOI, including any areas of concern that would aid in providing a recommendation for improvement; and,

b) what they believe the minimum qualifications required for a company to participate in this project should be.

ANNEX E: ACRONYMS

Acronym	Full Name
ABAC	Attribute Based Access Control
ACL	Access Control List
ATO	Authorization to Operate
BICES	Battlefield Information Collection and Exploitation System
C2	Command and Control
C2IS	Command and Control Information System
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAF	Canadian Armed Forces
CANSOFCOM	Canadian Special Operations Forces Command
CANUS	Canadian-United States
CDLS(W)	Canadian Defence Liaison Staff (Washington)
CDS	Chief of the Defence Staff
CDMN	Canadian Deployed Mission Network
CDRSN	Canadian Defence Red Switch Network
CEO	Canadian Eyes Only
CFS	Canadian Forces Station
CIA	Confidentiality, Integrity, Availability
CIS	Communications and Information System
CJOC	Canadian Joint Operations Command
CMMI	Capability Maturity Model Integration
COI	Community of Interest
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CSE	Communications Security Establishment Canada
CSfC	Commercial Solutions for Classified
CSNI	Consolidated Secret Network Infrastructure
CxDS	Cross Domain Solution
DART	Disaster Assistance Response Team
DCB	Defence Capability Board
DCSS	Data Centric Security Service
DND	Department of National Defence
DPS	Defence Procurement Strategy
DWAN	Defence Wide Area Network
ECS	Environmental Chief of Staff
FMN	Federated Mission Network
FMV	Full Motion Video
FOC	Full Operational Capability
FVEY	Five-Eyes
GC	Government of Canada
GCSI	Government of Canada Secret Infrastructure
GOTS	Government Off-the-Shelf
IaaS	Infrastructure as a Service
ICAM	Identity, Credential, and Access Management
IEG	Information Exchange Gateway
ILS	Integrated Logistics Support
IM/IT	Information Management/Information Technology
IOC	Initial Operational Capability
IP	Internet Protocol

IRMS	Information Resource Management System
IRPDA	Independent Review Panel for Defence Acquisition
ISED	Innovation, Science and Economic Development Canada
ISO	International Organization for Standardization
ISS	In-Service Support
IT	Information Technology
ITaaS	Information Technology as a Service
ITB	Industrial and Technological Benefits
ITI in Sp of C2	Information Technology Infrastructure in Support of Command and Control
ITIL	Information Technology Infrastructure Library
JBMC	Joint Battlespace Management Capability
JIMP	Joint, Interagency, Multi-National and Public
JTF	Joint Task Force
LAN	Local Area Network
LCSS	Land Command and Control System
LOI	Letter of Interest
MB	Megabytes
Mbps	Megabits per Seconds
MIDB	Modernized Integrated Database
MND	Minister of National Defence
MOB	Main Operating Base
MPE	Mission Partner Environment
MTBF	Mean Time Between Failure
NATO	North Atlantic Treaty Organization
NCMS	NATO Core Metadata Standard
NEN	NORAD Enterprise Network
NFV	Network Function Virtualization
NOC	Naval Operations Centre
NORAD	North American Aerospace Defense Command
NSA	National Security Agency
NSE	National Security Exception
NSWAN	NATO Secret Wide Area Network
NZL	New Zealand
OV	Operational View
PaaS	Platform as a Service
PBAC	Policy Based Access Contract
PKI	Public Key Infrastructure
PMB	Project Management Board
PSPC	Public Services and Procurement Canada
QoS	Quality of Service
RBAC	Role Based Access Control
RCAF	Royal Canadian Air Force
RCN	Royal Canadian Navy
RFP	Request for Proposal
RJTF	Regional Joint Task Force
ROM	Rough Order of Magnitude
SA&A	Security Assessment and Authorization
SAAG	Security Assessment & Authorization Guideline
SDN	Software Defined Networking
SIEM	Security Incident Event Management

SLI/JC2SS	Secret LAN Internet/Joint Command and Control Support System
SOR	Statement of Requirements
SSC	Shared Services Canada
SVTC	Secure Video Tele-conferencing
TBC	To be confirmed
TNA	Training Needs Assessment
UK	United Kingdom
US	United States
VDI	Virtual Desktop Infrastructure
VHD	Virtual Hosted Display
VoIP	Voice over Internet Protocol
WAN	Wide Area Network