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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet CFLEWM Project	
Solicitation No. - N° de l'invitation W8476-196070/A	**Date** 2019-02-04
Client Reference No. - N° de référence du client W8476-196070	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-015-27182
File No. - N° de dossier 015qe.W8476-196070	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2019-05-13**	**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: Picknell, Christine	**Buyer Id - Id de l'acheteur** 015qe
Telephone No. - N° de téléphone (819) 420-1761 ( )	**FAX No. - N° de FAX** (819) 956-6907
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** -	

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée See Herein	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N°de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature**	**Date**

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

Canada

Canadian Forces Land Electronic Warfare Modernization

-

Letter of Interest

TABLE OF CONTENTS

PURPOSE AND CONTENTS OF THIS LETTER OF INTEREST

This is the Letter of Interest (LOI) pertaining to the Canadian Forces Land Electronic Warfare Modernization (CFLEWM) 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 CFLEWM 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: CFLEWM Solution

ANNEX A: CFLEWM Requirement
ANNEX B: High Level Mandatory Requirements
ANNEX C: Sustainment Approach
ANNEX D: Information Requested From Industry

PART I: LETTER OF INTEREST PROCESS

1. INTRODUCTION

The CFLEWM 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 CFLEWM capabilities, future developments within industry, and how similarly large corporate organizations are changing to meet their evolving electronic 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 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: Christine Picknell and Eliane Barnett

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

Please insert "CFLEWM LOI" 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 LOI 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 envelope containing the response if submitted on USB keys via mail.

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

2.9 Fairness Monitor

Should a future CFLEWM 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:

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

vii. providing feedback to Canada on fairness issues; and

viii. 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: CFLEWM SOLUTION

1. CFLEWM SOLUTION BACKGROUND

The Canadian Armed Forces requires an effectively commanded land based Electronic Warfare capability which can sense and act within the electromagnetic (EM) spectrum, provide electromagnetic protection by shielding friendly forces from threats, and be an enduring capability through appropriate sustainment mechanisms.

These capabilities will contribute to gaining the initiative and surprising the enemy by selectively exploiting or denying adversarial use of the electromagnetic spectrum in order to understand the potential adversary's intent, prevent them from gaining a clear understanding of the operational environment, and ensure that they cannot impede friendly manoeuvre through the use of electromagnetic triggers.

The CFLEWM Project is currently in the Options Analysis Phase, with a preferred option expected to be identified and selected by summer 2020. 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 CFLEWM infrastructure and service solutions;

b. 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

c. seeking information to assist the DND/CAF in potentially grouping some of the deliverables, 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 CFLEWM Solution 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 International Restrictions.

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. This possible requirement will be further articulated in follow on industry engagement.

5. OFFICIAL LANGUAGES

Any future contract for a CFLEWM solution may require the Contractor to provide all documentation along with technical and client support in both official languages.

6. ENGAGEMENT APPROACH

6.1 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. It is envisaged that an industry day will be held in summer 2019, dates are to be determined and posted as an amendment to this LOI. A more detailed RFI will follow the LOI process, responses to the LOI will assist in developing the Industry Day and RFI.

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.

ANNEX A – REQUIREMENT

Canadian Forces Land Electronic Warfare Modernization (CFLEWM)

1. GENERAL

The Canadian Armed Forces (CAF) has a requirement to acquire and support capabilities outlined in the CFLEWM project and institutionalize them within the Canadian Army (CA).

2. BACKGROUND

The capability delivered by CFLEWM will be a key contributor to four of the eight core missions identified in Strong, Secure and Engaged (SSE). It will complement other CAF Joint, Land, Naval and Air systems currently in and entering service. The key to operating in the present and future Electromagnetic Environment (EME) battlespace is the ability to integrate the five operational functions of; Command, Sense, Act, Shield and Sustain into a comprehensive Electronic Warfare (EW) capability. This capability will reduce an adversary's effectiveness to act within the EME by limiting their ability to respond and manoeuvre, while simultaneously maintaining the CAF's capability to conduct continuous operations. The CFLEWM delivered capability is expected to operate in a very complex EME and enable a Commander the ability to understand, act and control the EME battlespace while providing protection from hostile Electromagnetic (EM) threats and minimize fratricide interference with friendly forces systems. The preferred option is to procure developed systems (commonly referred to as a Military-Of-The-Shelf (MOTS)) which meet the list of High Level Mandatory Requirements (HLMR). The requirement for industry will be to supply the major components of CFLEWM, and provide long-term In-Service Support (ISS) for the system. Additionally, there is the possibility of managing the integration of supplied components.

3. PROJECT SCOPE

CFLEWM will combine elements from each of the five operational functions; Command, Sense, Act, Shield and Sustain into a comprehensive capability as outlined in Figure 1 below.

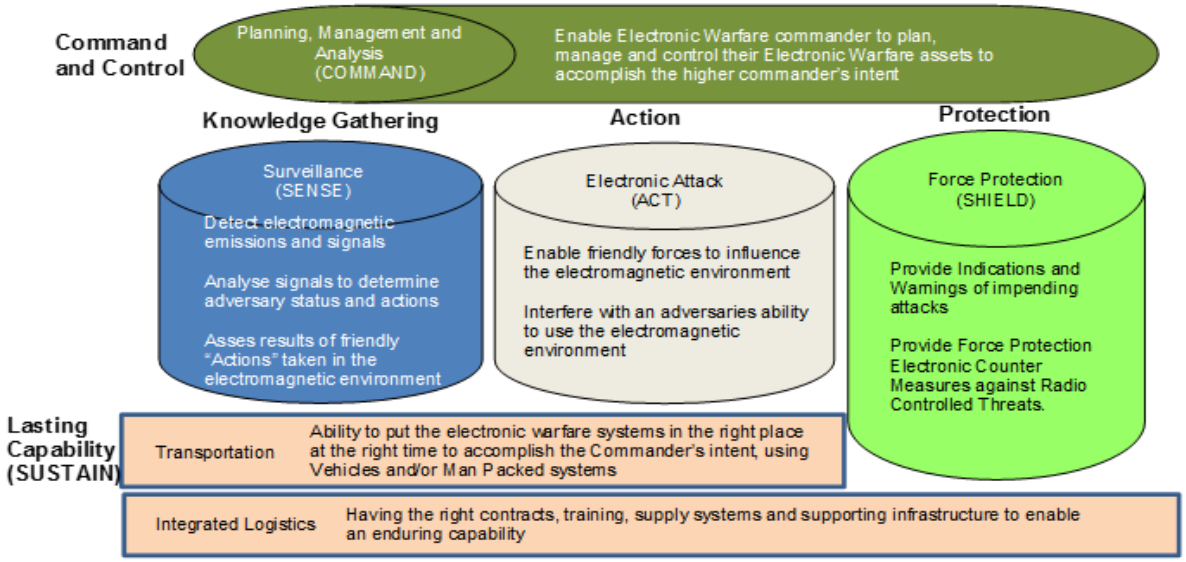

Figure 1: A Comprehensive Land Electronic Warfare Capability

The CFLEWM project scope is expected to include the following system capabilities:

a) It must have an effective command capability which includes: the ability to understand the EME; importing and exporting data to/from, strategic, joint and allied partners; allow EW and Cyber Electromagnetic Activities (CEMA) to be efficiently planned, executed and controlled; allow both centralised and distributed operations; and minimize friendly force interference;

b) It must sense Signals of Interest (SoI) and allow them to be classified, analysed, exploited and geographically located. This includes the ability to import/export data about the EME to/from the command system;

c) It must be able to act within the EME by allowing the execution of offensive EM non-kinetic actions, the ability to interfere with adversarial use of the EM spectrum, be linked to the sense function to allow an assessment of friendly actions in the EME, and be controlled both locally by the operator and remotely from the command system;

d) It must be able to simultaneously detect, identify, target, geographically locate, and engage (suppress)1 current and emerging EME threats, and allow data about the EME to be imported/exported to/from the command system;

e) It must be institutionalized within CA doctrine, training, and support in order to ensure an enduring capability;

f) It must support both mounted and dismounted operations;

g) It must be interoperable with the Five Eye allies/partners (US, UK, AUS, NZ);

h) It must be flexible enough to adapt to new types/categories of signals and threats while supporting the range of friendly force operations in a dynamic and controllable fashion;

i) It must include Integrated Logistics Support (ILS) and spare parts;

j) It must provide In Service Support (ISS); and

k) It must provide project management and engineering services.

The Department of National Defence (DND) can provide as Government Furnished Equipment any system platforms that may be required for all CFLEWM variants. Potential Bidders need to consider hardware, software, and integration costs for CFLEWM specific equipment when it comes to merging with GFE.

4. ROLE AND FUNCTION

The role of CFLEWM is to provide an effectively commanded land based Electronic Warfare capability which can sense and act within the EME, including the ability to interfere with adversarial use of the EME, provide protection by shielding friendly forces from electromagnetic threats, and be an enduring capability through appropriate sustainment mechanisms.

[1] An example of suppress can be defined as inhibiting the link between the trigger person and the Radio Controlled trigger of an IED so the IED has a dramatically reduced probability of detonation

5. CONSTRAINTS

The proposals must provide a fully integrated capability across the complete list of preliminary HLMRs contained within Annex B.

6. REQUIREMENTS

The CFLEWM project is predicated on a set of high level functional and performance requirements. The list of preliminary HLMR that a proposed system must meet is contained within Annex B.

ANNEX B – HIGH LEVEL MANDATORY REQUIREMENTS

Canadian Forces Land Electronic Warfare Modernization (CFLEWM)

1. GENERAL

This annex contains the preliminary High Level Mandatory Requirements (HLMR) for the CFLEWM project. In order to be considered proposals must meet all of the mandatory elements specified in paragraphs 2.3.

2. CAPABILITY DESCRIPTION

The Canadian Armed Forces (CAF) requires an effectively commanded land based Electronic Warfare capability which can sense and act within the electromagnetic spectrum, provide protection by shielding friendly forces from electromagnetic threats, and be an enduring capability through appropriate sustainment mechanisms.

2.1 Aim, Role and Employment

The role of the capability delivered by CFLEWM is to allow the battlespace commander to manoeuvre in the EM spectrum. This includes ensuring freedom of action by protecting CAF land elements from EM threats and facilitating an understanding of the EME to enable exploitation for friendly force benefit and denying its use to adversaries.

Modern operations are conducted at a high tempo and are very complex. In addition they are almost always joint and/or multi-national. Therefore, it is critical to establish and maintain the Commander's situational awareness so their manoeuvre in the EME has maximum flexibility. CFLEWM will deliver a comprehensive and highly effective capability that incorporates all five operational functions; Command, Sense, Act, Shield and Sustain. This will significantly enhance a commander's ability to use the EME and contribute to effective Command and Control over his forces.

The Canadian Army's new EW capability may be deployed on a variety of mission types spanning the spectrum of conflict – from peacetime military engagements up to major combat operations. Canada is an active international partner meaning this capability will often be employed within coalition environments making it essential that this new capability has the flexibility to be interoperable with key FVEY partners.

2.2 Organization

The organizational structure for the SHIELD capability will be based on the deployed unit sizes in accordance with SSE. The COMMAND, SENSE, and ACT will be based on our existing EW units. The final future organizational structure that will be supported by CFLEWM is under development and will be determined by the ongoing Force 2021 working groups.

2.3 High Level Mandatory Requirements (HLMR)

Each HLMR has an opening descriptive followed by the detailed requirements.

2.3.1 EW Command

2.3.1.1 Understanding the EME

The command system must be able to ingest all internal and external EW/Cyber Electromagnetic Activities (CEMA) data and display a visual Spectrum Common Operating Picture (SCOP) that, with minimal training, can be understood by command and staff personnel.

2.3.1.2 Exporting and Importing Data

The command system must be able to export and import EW/CEMA data with strategic, joint and allied partners in a format or formats they can ingest.

2.3.1.3 Planning EW Operations

The command system must allow EW operations planning using the SCOP and other tools which can create products in standard military formats. These products will be exported to: the sense, act and shield systems, as well as the in-service combined arms command support systems.

2.3.1.4 Execute and Control EW Operations

The command system must allow EW operations to be conducted using a combination of automated, centralized and distributed processes.

2.3.1.5 Analyze Friendly Force Interference

The command system must be able to determine/quantify the risk of EW operations interfering with friendly force systems.

2.3.2 EW Sense

2.3.2.1. Detect Signal of Interest (SoI)

The sense capability must operate within the specified frequency range and signal types and protocols to be able to detect SoI.

2.3.2.2 Categorise the SoI

The sense system must be able to categorize SoI by identifying the general characteristics of the signals and be able to import/export data to/from the command system.

2.3.2.3 Analyse the SoI

The sense system must be able to conduct detailed analysis of the SoI to enable further exploitation of the signal and be able to import/export data to/from the command system.

2.3.2.4 Exploit the SoI

The sense system must include tools able to exploit the SoI in order to develop intelligence products and be able to import/export data to/from the command system.

2.3.2.5 Geographically Locate SoI

The sense system must be able to internally/externally cooperatively geographically locate SoI and import/export the location data to the command system.

2.3.2.6 Survey the EME

The sense system must be able to develop a general awareness of the EME and import/export the EME data to/from the command system.

2.3.2.7 Record SoI

The sense system must be capable of recording the SoI for further analysis

2.3.3 EW Act

2.3.3.1 Execute Non-Kinetic Actions

The act system must be capable of executing offensive non-kinetic CEMA operations.

2.3.3.2 Target Adversarial use of the EME

The act system must be able to operate within the frequency range, power levels, signal types and protocols of adversarial systems in order to interfere with their use of the EME.

2.3.3.3. System Interoperability

The act system must be configurable to minimize adverse effects and interference on other national and allied electronic systems (i.e. Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance, Counter Unmanned Aerial Systems capability, Allied systems, and vehicle vetronics).

2.3.3.4 Control of Act System

The act system must have the capability to be controlled; autonomously, locally by the operator and remotely by the command system.

2.3.3.5 Act Configuration

The act system must be configurable to counter new and evolving threats through acquirable software and development tools that will allow the rapid development of new configuration files.

2.3.4. EW Shield

2.3.4.1 Control of Shield System

The shield system must have the capability to be controlled; autonomously, locally by the operator and remotely by the command system.

2.3.4.2 Detect EM Threats

The shield system must have the ability to detect the EME and identify threat devices such

as Radio Controlled Improvised Explosive Device triggers.

2.3.4.3 Target EM Threats

The shield system must be able to operate within the frequency range and signal types of the threat triggers in order to be able to target the devices.

2.3.4.4 Geographically Locate

The shield system must be able to internally and externally cooperatively geographically locate threat device signal and be able to import/export the location data to the command system.

2.3.4.5 Suppress EME Threats

The shield system must be able to inhibit the link between EME threat devices and dramatically reduce the probability of their intended operation at a minimum safe distance.

2.3.4.6 Record EME

The shield system must have the ability to analyse and assess the EME autonomously, locally by the operator, and remotely by the command system to facilitate the identification of changes to threat devices and/or adversary Tactics, Techniques, and Procedures through logs and recordings.

2.3.4.7 Shield System Interoperability

The shield system must be configurable to minimize adverse interference with other electronic systems.

2.3.4.8 Shield Configuration

The shield system must be configurable to counter new and evolving EM threat signals, through acquirable software and development tools that will allow rapid development of new configuration files.

2.3.5 EW Sustain

2.3.5.1 EW Training

The capability must have the ability to support individual training and be interoperate with collective training systems (i.e. simulation).

2.3.5.2 Support to Operations

The capability must be able to support both mounted and dismounted operations in an integrated fashion.

2.3.5.3 In Service Support

The capability must include in-service support contracts which include ILS, training, and engineering support.

2.3.6 Common

2.3.6.1 Compatibility

The capability must be able to operate in a coalition environment by allowing EW data to be fed into and leveraged from the Five Eyes partners.

2.3.6.2 Flexibility

The system must be capable in a wide range of deployment environments, locations and be able to perform against threat signal types by changing frequency bands, power levels and configuration files in a timely manner.

ANNEX C – SUSTAINMENT APPROACH

Canadian Forces Land Electronic Warfare Modernization (CFLEWM)

1. GENERAL

The overall in-service support concept will rely on an initial interim support period immediately followed by a long term In-Service Support (ISS) period. It is expected that the requirement for ISS will be competed at the same time as the acquisition requirement.

2. IN-SERVICE SUPPORT (ISS) PRELIMINARY REQUIREMENT

The CFLEWM ISS concept is currently being formulated. However, some assumptions can be made concerning the form and function of the ISS concept:

2.1 The ISS concept will support a complex equipment design. The CFLEWM system design will likely include multiple equipment types across multiple vehicle platforms, static platforms and man-portable configurations.

2.2 The ISS concept will support both physical equipment and software systems. CFLEWM will include an EW-specific Command, Control and Visualization system that will require maintenance, upgrades and improvements throughout the lifespan of the system. Further, each of the equipment and platform configurations will likely have specific graphic User Interfaces, Control systems, ancillary data management systems and Artificial Intelligence systems that will require maintenance upgrades and improvements. Also, physical equipment in various forms and levels of complexity will require maintenance, upgrades and replacement.

2.3 The ISS concept must support deployed operations. Many of the CFLEWM systems will be adversary-facing and will be employed in an expeditionary manner. Therefore, the ISS concept must have sustainment processes that will function in an expeditionary setting.

2.4 The ISS concept must support equipment distributed across the Canadian Army. Some of the equipment and systems of the CFLEWM project will likely be distributed to non-EW units. Therefore, the ISS must provide support to geographically dispersed and technically non-proficient users.

3. AIM

The aim of this annex is to provide the CFLEWM preliminary ISS concept to assist respondents in providing feedback on long-term ISS requirements and strategies.

4. SCOPE

The scope of CFLEWM ISS is an incentivized performance-based allowing the Crown to secure long term in service-support in the following fields:

4.1 Overall Program Management;

4.2 Engineering Support;

4.3 Supply Support;

4.4 Fleet Technical Services;

4.5 Information and Data Management;

4.6 Software improvement and management; and

4.7 Waveform development and management;

5. ISS CONCEPT FRAMEWORK

While the CFLEWM ISS Concept is still under development, the components of the system will likely include, but will not be limited to, the following:

5.1 One or several software sustainment requirements;

5.2 One or several hardware sustainment requirements;

5.3 One or several hardware/platform integration requirements;

5.4 One or several software/hardware integration requirements; and

5.5 One or several software compatibility and integration requirements;

ANNEX D – INFORMATION REQUESTED FROM INDUSTRY

Canadian Forces Land Electronic Warfare Modernization (CFLEWM)

1. GENERAL

This LOI is the first step to engage industry in an iterative information sharing process as part of further RFI development. Potential responders are encouraged to be innovative in their proposed method(s) of capability delivery and sustainment options.

2. INFORMATION REQUESTED

Based on the requirements detailed in this document, this LOI seeks vendors to provide the following information:

2.1. What solutions does your company provide that could help DND realize the capabilities presented in the CFLEWM concept described in Annex A?

2.2. Provide comments regarding the technical feasibility of each HLMR detailed in Annex B.

2.3. If vendors cannot provide the full capability they will provide a plan, including other vendors they could potentially partner with to address all HLMRs.

2.4. Provide a technical description of the proposed solution along with a statement of capability, illustrating how the proposed solution can achieve the HLMR detailed in Annex B.

2.5. Provide any available details about the maturity of proposed solution (i.e. Technology Readiness Level, in service, etc).

2.6. Optionally, provide available rough order of magnitude breakdown for costing details by components listed in Annex A, paragraph 3 Project Scope.

3. SUSTAINMENT

This LOI is seeks vendors to provide suggestions on sustainment as outlined below:

3.1. Provide suggestions on how the capability can be sustained through-out its life cycle.

3.2. Provide feedback on capability sustainment as outlined in Annex C.

3.3. What does your company see as the life expectancy of the capability?

4. INDUSTRIAL AND TECHNOLOGICAL BENEFITS (ITB) POLICY

4.1. Application of the Industrial and Technological Benefits (ITB) Policy

The Industrial and Technological Benefits (ITB) Policy may be applied on the Canadian Forces Land Electronic Warfare Modernization (CFLEWM) project. Engagement with industry through the LOI will help determine the application of the ITB Policy and how Canada could leverage opportunities for economic benefit through this procurement.

4.2. The ITB Policy including Value Proposition

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

4.2.1. 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.

Based on initial analysis of the CFLEWM project, this procurement encompasses the KICs of **Cyber Resilience, Defence Systems Integration, and Artificial Intelligence**, where Canada has world leading capabilities. Canada will be seeking to motivate high value economic opportunities and partnerships to support the growth of Canada's defence sector, as well as enhance supply chain participation and skills development opportunities for Canadian industry.

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.

Defence Systems Integration

Design and integration of complex military systems that hinge on the seamless linking together of multiple sub-systems to yield an effective operational capability. These capabilities span various military platforms and enable the operation and management of weapons, defensive systems, command and control systems, sensors, decision support systems, electronic warfare devices and a platform's core sub-systems in a tightly coordinated fashion essential under highly stressing combat conditions. These systems need to present information to their operators stemming from multiple sources in a manner that is understandable, secure, and supports decision-making in a complex environment. This definition does not include the various constituent systems (e.g., missile launching systems, radars, electronic warfare systems, etc.) that the work of defence systems integration aims to combine into a cohesive whole. Rather, the definition focuses on the skills and other capabilities needed to perform the integration work, and to create the user interface that is needed in such complex mission systems.

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.

4.3. 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 used in government defence and security applications.

4.3.1. Please describe the production activities or services your company performs in the KICs of Cyber Resilience, Defence Systems Integration, and Artificial Intelligence? Please include which activities are currently performed in Canada?

4.3.2. Based on the High Level Mandatory Requirements put forward by the Department of National Defence, describe what work activities your company would foresee undertaking in Canada for the production and the maintenance of the CFLEWM system? What opportunities and constraints are there to performing this work in Canada?

4.4. 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) in the supply chains of bidders and tier-one suppliers for the CFLEWM project.

4.4.1. In what areas of production and service-provision does your company currently work with Canadian SMBs, and how are these SMBs involved?

4.4.2. What are the opportunities and constraints for Canadian SMBs to provide solutions for the CFLEWM system?

4.5. 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.

Examples of Skills Development and Training activities:

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; and

iv. Support for security certifications (e.g.: Top Secret, ITAR) or cybersecurity compliance certifications for Canadian companies, especially small and medium-sized businesses.

4.5.1. What Skills Development and Training activities does your company currently provide, and could these activities be extended to Canadians working in the KICs of Cyber Resilience, Defence Systems Integration, and Artificial Intelligence?

4.5.2. What Skills Development and Training challenges does your company anticipate within the KICs of Cyber Resilience, Defence Systems Integration, and Artificial Intelligence and how is your company seeking to overcome them?

4.6. 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.

4.6.1. Please describe your company's priority areas for R&D investment? As part of your answer, please identify to what extent these priority areas align with the Cyber Resilience, Defence Systems Integration and Artificial Intelligence KICs identified above?

4.6.2. Recognizing the role that post-secondary institutions and public research institutes play in fostering innovation in Canada, please describe what potential opportunities your company foresees undertaking in Canada with these organizations and what specific research areas you would pursue.

4.7. 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.

4.7.1. What role does the CFLEWM procurement play in positioning your company and its Canadian supply-chain for long-term growth?

4.7.1.1. To what extent can you integrate Canadian companies into your international supply chain?

4.7.1.2. To what extent do opportunities exist in the KICs of Cyber Resilience, Defence Systems Integration, and Artificial Intelligence?

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

4.7.2.1. Please describe any challenges or constraints the company faces in sharing Intellectual Property (IP) with Canadian partners and suppliers?

4.8. Other Questions

Are there other relevant KICs which align with the work to be conducted for the CFLEWM 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.

5. EXPERIENCE

What is your company's experience supporting military requirements?

5.1. Has your company worked on delivering military requirements before?

5.2. What experience does your company have delivering or supporting Electronic Warfare capabilities in a military context?

5.3. What experience does your company have supporting facility access in a military context?

5.4. Has your company had experience with the DND Security Accreditation and Authorization (SA&A) process?

6. ADDITIONAL FACTORS

6.1. What additional factors should be considered by DND in the development of this capability?

6.2. What is your solution to address these factors?

6.3. In your experience, what risks should be considered when implementing this capability?

6.4. What is your solution for mitigating these risks?

7. RESPONSE TEMPLATE

Respondents may use any written format they wish to provide the required information. Each of the questions above must have a response or an explanation of why a response is not possible at this time.