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

Part - Partie 1 of - de 2
See Part 2 for Clauses and Conditions
Voir Partie 2 pour Clauses et Conditions

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Title - Sujet CFLEWM Project	
Solicitation No. - N° de l'invitation W8476-196070/A	**Amendment No. - N° modif.** 004
Client Reference No. - N° de référence du client W8476-196070	**Date** 2019-07-12
GETS Reference No. - N° de référence 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** 2019-07-18	**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:** -	

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Instructions: See Herein

Instructions: Voir aux présentes

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

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 – Amendment 04

This amendment is raised to:

A. Answer questions from potential suppliers, and;

B. Provide the Industry Day presentation.

A. CFLEWM Industry Day One-On-One Meeting Questions and Answers

Questions related to Industrial and Technological Benefits (ITB) Policy

Q1: What is the weighting value of the Value Proposition (VP)?

A1: The weighting of a VP score relative to price and technical merit scores will be determined on a procurement-by-procurement basis and will generally be at least 10 percent of the overall bid score. Factors that could influence an increase in the weighting of the VP may include alignment with Key Industrial Capabilities (KIC(s)), market capacity in Canada and export capability. Industry is welcome to provide any additional rationale on this matter, which will be considered by Canada.

Q2: Regarding ITB and building links into programs, do you have an area you want industry to invest in?

A2: The introduction of KICs represents a strategic approach to leveraging economic outcomes through upcoming National Defence and major Canadian Coast Guard procurements with a continued focus on innovation, supplier development, exports, and economic growth for the defence industry and associated commercial applications. KICs reflect potential areas of investment in emerging technologies and established domestic capabilities, which are competitive in the global marketplace and essential to national security. With the introduction of KICs, industry will have greater predictability on where to focus investments in preparation for upcoming procurements. Preliminary analysis has identified Cyber Resilience and Artificial Intelligence as KICs applicable to the CFLEWM project. Feedback from industry on the inclusion of these two KICs is welcomed. Further information and the definitions of each KIC can be found at https://www.ic.gc.ca/eic/site/086.nsf/eng/h_00175.html

Q3: Regarding KICs, how does Cyber-resilience relate to the CFLEWM project objectives?

A3: Canada believes that Cyber Resilience is the KIC most closely related to the CFLEWM project as it 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. Investments aimed at supporting this KIC and enhancing Canada's cyber capabilities will help improve Canada's capacity for addressing future threats more broadly in the electronic warfare and defence space. Similarly, Artificial Intelligence has been identified as another KIC related to this procurement. Feedback on the inclusion of the Cyber Resilience and Artificial Intelligence KICs in the delivery of the CFLEWM project is welcomed. Further information and the definitions of each KIC can be found at https://www.ic.gc.ca/eic/site/086.nsf/eng/h_00175.html .

Q4: Regarding ITB, are you looking at a transfer of technology in order to expand the EW industry in Canada?

A4: Transfer of Intellectual Property (IP) is incentivized in the ITB policy and can be used to help satisfy ITB Obligations and Commitments. Further information on IP transfer can be found in the Model Terms and Conditions here: https://www.ic.gc.ca/eic/site/086.nsf/eng/h_00011.html

Q5: What is the mechanism to transfer technology?

A5: ISED incentivizes Intellectual Property (IP) transfer to industry in Canada through the ITB Policy, however ISED does not act as the technical authority or the facilitator of IP transfer. If you have further questions on facilitating IP transfer, please send questions to the CFLEWM project group mailbox.

Q6: Can the potential to export be weighted as part of ITB?

A6: Yes, Exports could be a weighted component of the CFLEWM VP. Industry is invited to provide feedback on the weighting of the Export pillar in the VP. Additionally, bidders may be required to submit an international export strategy as part of their VP, demonstrating that they and their suppliers can leverage the procurement into future export success from a Canadian base. These strategies should identify the international markets that the bidder and their suppliers intend to target and demonstrate that they have the capacity to successfully carry out their plans. The international export strategies of bidders and their suppliers will focus on the future export potential from Canada of the good or service being procured. Success in penetrating global markets from Canada will result in jobs and growth and ensure that Canadians share in long-term success following the procurement.

Questions related to Public Services and Procurement Canada (PSPC)

Q7: Can you conduct site visits?

A7: The policy for site visits is being confirmed and will be communicated at a later date. If approved, all site visits shall include the Fairness Monitor.

Q8: Is Canada willing to accept 5 EYES (FVEY) equivalent security clearances?

A8: If the individual has a clearance from one of the 5 eyes countries, PSPC's Contract Security Program would be able to accept the clearance. However we would need to complete an assurance with the **designated security authority (DSA)** or by the **national security authority (NSA)** from the originating country.

Q9: From a PSPC perspective, if option 3, DND as design authority, is chosen, are you open to creating a joint project office between DND and industry?

A9: This would be a challenge and a new way of doing business, but we are open to suggestions.

Q10: Do we need to register with Controlled Goods prior to the goods being manufactured or delivered?

A10: If to manufacture the item, the vendor receive blueprints, technical drawing, specs, etc. that are controlled goods, then the vendor must be registered with the program before accessing those controlled goods. Vendors may need to register with controlled goods program prior to the request for proposal.

Q11: Have you determined the response time for the RFI?

A11: No as yet, but it will be months, not weeks.

Q12: Have you considered an Invitation to Qualify (ITQ) process?

A12: Although no decision has been made, it is possible an ITQ process will be employed.

Q13: Will you be releasing a list of Industry Day participants?

A13: No, but suppliers can sign up on the Buy and Sell CFLEWM LOI page as an "Interested Supplier" (https://buyandsell.gc.ca/procurement-data/tender-notice/PW-QE-015-27182/list-of-interested-suppliers). This can be a great way to find partnerships, however, please note that this list is open to the public. Please see all the terms and conditions of this service on Buy and Sell.

Questions for Department of National Defence Project Team (PT)

Q14: What are you looking for as a solution; what exactly are you looking for?

A14: At this point, nothing is off the table, and we are interested is anything you suggest. This is your opportunity to influence our concept and how we move forward.

Q15: Are you interested in solutions no one else has thought about?

A15: Absolutely, we realize that industry might have great ideas on how to proceed; ideas we haven't thought about.

Q16: Are there currently funds available for Risk Reduction?

A16: Currently, there are very limited funds for Risk Reduction and there likely won't be a change until the Project Definition phase.

Q17: Are there labs available for testing, particularly the Land Command Support System (LCSS) lab?

A17: Currently, as we are not part of LCSS, we do not have access to that lab.

Q18: Are you looking for proven systems as these obviously remove innovation?

A18 5: No, we have not asked for proven systems in the LOI and the intent is to encourage innovation.

Q19: Do you have a preferred data structure or format?

A19: We do not have a preferred data structure at this time and are looking at several options. However, we intend to leverage open architectures as much as possible.

Q20: What is the "life expectancy" of the equipment involved?

A20: This has not been decided, but you can give us your thoughts on what is possible in the LOI response.

Q21: Which of the three options are you leaning toward, and when will a decision be made? Have they been weighted?

A21: All three options are viable and we are not leaning toward a particular option at this point and they have not been weighted. The decision will be made around the time of the Request for Information (RFI) release.

Q22: Based on deployment, what technology would sit in each the vehicle? What technology would be in other vehicles?

A22: At this point, we only have a conceptual design of what we want to achieve and we are not close to knowing what equipment will be in each vehicle. However, we are very interested in industry's opinion.

Q23: As it may take some time to get ITAR permissions depending on the frequency range desired, what range are you currently considering?

A23: The frequency range has not been decided yet, but we are interested in industry's opinion on this subject.

Q24: Regarding light, medium, and heavy solutions, do you see equipment moving from vehicle to vehicle, and are you looking for man-pack as well?

A24: Everything is on the table, and yes we will require a man-pack solution as well.

Q25: Can you share anything on classification? Will the data be TS or Secret? Will there be sharing between different classifications? If so, do you want a multi-security communications pipe?

A25: Yes, we envision a cross domain security requirement, and would appreciate feedback from industry on a solution.

Q26: Does the project include reach back and Command and Control (C2) communications?

A26: This has not been clearly defined, but we will need to feed into National level networks. The system will likely include a tactical communication system that is not part of this project and may be provided as Government Furnished Equipment (GFE)/Government Supplied Material (GSM), but that is not confirmed. Nothing is off the table and we would like industry feedback on how to achieve the reach back and C2 communication. Bandwidth may not be the largest issue; it may in fact be cognitive/analysis challenges.

Q27: Have you looked to the FVEY community for a common solution?

A27: We have not looked to the FVEY community for a common solution, as there really isn't a Canadian policy to support this. However, we are in contact with allies in the FVEYS community and have done some joint planning regarding similar projects.

Q28: What innovative ideas are you looking for and what have you seen so far?

A28: The proof of concept for Multi-Function Electronic Warfare (MFEW) has been completed, but we have no particular innovative ideas in mind. We are looking to industry to not only provide ideas on the concept, but to also provide us with possible new ways of looking at the concept.

Q29: Are you looking to field everything at once or are you planning a phased approach?

A29: No decision has been taken yet, but we will have a better idea once the system design is completed.

Q30: Do you have a traceability diagram or road map from what you currently have to where you want to go?

A30: No, however using current doctrine will give some insight. Although the way we will accomplish our tasks have changed, the principles have not. This project is looking at paradigm shift in how we look at the electromagnetic spectrum operations.

Q31: What do you mean by "technological paradigm shift"?

A31: We are referring to the Electromagnetic Spectrum becoming a domain or battlespace in its own. For example, a space that must be contested, controlled and superiority achieved before subsequent physical operations can take place.

Q32: Is CFLEWM ready to get "out front" of LCSS?

A32: We are working closely with all Strong Secure Engage "42" projects. As of yet, no decision on how or if LCSS will be employed. All options are still open.

Q33: Regarding "governance", are you independent and who will be managing the layer of technology required to correctly interface all of the systems involved?

A33: The Canadian Army (CA) is the current lead and work is in progress with Director Land Command Support Project Management (DLCSPM) to complete the high level system design.

Q34: Will an architecture be decided by the RFI release?

A34: Yes, high level system design will heavily influence the selection of an architecture by the time the RFI is issued. Currently, we desire a fully open architecture.

Q35: The Command element of your concept of operations is a large and tough piece. Has anyone “cracked it”, yet?

A35: The United States and Australia have made in roads and we are watching their efforts closely.

Q36: Given the pace of technological change, particularly regarding Artificial Intelligence (AI), how will you handle changing requirements and capabilities between now and the RFP?

A36: Continued engagement with industry between now, the draft RFP, and the RFP will mitigate challenges regarding technological change.

Q37: Are you open to receiving White Papers?

A37: Yes, we are open to receive as much information as possible.

Q38: What is the concept of operations (CONOP) for the multi-function EW asset?

A38: We are not talking about a specific “EW asset” at this time, but rather an EW concept. We are looking for industry guidance, through the LOI responses, which we will use to influence high level system design.

Q39: Regarding non FVEY constraints, what regulations will apply, and what will be the effects on non FVEY offshore supply?

A39: Non FVEY offshore supply will involve additional challenges, on a case by case basis, but we don’t see it as insurmountable.

Q40: If you have a FVEY solution and a similar or equally valid non-FVEY solutions, will you automatically be choosing the FVEY solution?

A40: Not necessarily as we would like to potentially work closely with select NATO nations that may not be FVEY. Security requirement may also dictate who we are able to deal with.

Q41: To what extent should software be programmable by end-users? What are your objectives regarding software modifications?

A41: We are seeking to avoid expensive proprietary updates related to future software needs. Therefore, we want the ability to update or modify algorithms, waveforms, etc. This work would be completed by government subject matter experts as opposed to end-users in the field.

Q42: Do you see a need for jamming at the node/soldier level?

A42: The concept is still open, but we would like to influence the spectrum from all nodes if possible.

Q43: Will Direction Finding (DF) be part of the solution?

A43: Geo-location and DF will likely both be part of the solution.

Q44: Explain the basic difference between options 2 and 3.

A44: Essentially, option 2 sees DND act as the integrator, while option 3 sees DND acting as the Design Authority while contracting an integrator.

Q45: Do you have a communications network that can support the sensors required?

A45: We cannot answer this at the moment, but we are aware that bandwidth may be an issue and also bandwidth may not be the largest issue; it may in fact be cognitive/analysis challenges. We are looking to industry for propose solutions. See Q26 as well.

Q46: Will new equipment and/or vehicles be utilized?

A46: New vehicles will eventually be used. If we can reuse equipment, we will.

Q47: Regarding a dismounted EW capability, do you foresee using man-packs or Unmanned Ground Vehicles (UGV)?

A47: Yes, both man-packs and UGV would be considered as nothing is off the table. Note, we are not looking for specific Force Protection (FP) equipment, but Multi-Function Electronic Warfare (MFEW) will be part of the project that can provide FP and traditional EW capability.

Q48: Do you foresee all EW vehicles being “frontline” vehicles?

A48: Yes, as we see all frontline vehicles with MFEW acting as Electromagnetic (EM) sensors.

Q49: Will the MEWT be part of the project or will it be replaced?

A49: Yes, we envision we will bring forward any MEWT technology that is still relevant at the time, or they may be replaced with a similar capability, or possibly several vehicles acting like a MEWT. No options are off the table.

Q50: Who will be the stakeholder of the installed components?

A50: Regardless of the option chosen, Department of National Defence (DND) will be the “signing authority” for installed equipment.

Q51: Will you employ Foreign Military Sale (FMS) to purchase equipment?

A51: No decision has been made, but using the FMS is a possibility as all options are on the table.

Q52: Regarding a simulation capability, are you looking for full immersion or something else?

A52: We are still open to options and would welcome industry input, but it is unlikely immersive simulation will be required.

Q53; Are you looking at how Artificial Intelligence (AI) can influence/enable the system? Do you still want a “man in the loop”?

A53: Although we see AI assisting in reducing the cognitive burden, we are looking for input from industry on what can be or should be pursued.

Q54: Do the “primes” need to be cleared Top Secret (TS)?

A54: You can assume that a portion of the project will eventually become TS, but we are not there yet.

Q55: Do you have preferred standards and if so, have you looked at interoperability of standards?

A55: No decision on standards has been made. However, we are leaning toward an open architecture. Input from industry on standards would be welcomed in the LOI response.

Q56: Regarding architecture cross-compatibility, do you know how you will handle “no-foreign” testing of specifications? Have you given thought to non-compatibility testing?

A56: Although no decision has been made, we would like to stay as close to FVEY and select NATO partners as possible.

Q57: Given your operational concept, what is the Canadian view on turning sensors off?

A57: From a concept perspective, we want to have the ability to turn the sensor off if required by the operational/tactical situation.

Q58: Do you know of any significant differing views between Canada and the FVEY community?

A58: Not at this time.

Q59: How will SIGINT tie into the project?

A59: Although we are interested in a SIGINT tie in, process and policy wise this can be a challenge. We would welcome industry input.

Q60: Given the speed of threat development, what do you see as the mechanism for a mid-life upgrade or even upgrades done in the field?

A60: We are looking at open architecture to mitigate or avoid expensive upgrade fees. Keeping in mind the need to protect your IP, we are very interesting in being able to upgrade the data “in the box” on our own.

Q61: How is the project funded?

A61: Regarding funding, the project is in the Capital Investment Plan has been aligned with Canada’s Defence Policy, “Strong, Secure, Engaged”.

Q62: How “open” does the In Service Support (ISS) solution have to be; pan-industry?

A62: It will likely be industry to government. We are not really looking at pan-industry at this time.

Q63: Are we interested in buying “Electronic Warfare as a service”?

A63: Although we have not looked at EW as a service, nothing is off the table.

Q64: What threat scenarios are you looking to address?

A64: Like most NATO nations, we are concerned with everything from counter-terrorism to peer adversaries.

Q65: Do you have a preference or aversion to technology with ITAR components?

A65: No we do not have either a preference or aversion, but keep in mind that we would like to avoid a proprietary solution.

Q66: Do you want the source code?

A66: As we want the ability to upgrade the equipment by modifying waveforms, data sets, etc., we would need at a minimum a Software Development Kit (SDK) but the requirement for the source code or access to it will be confirmed at a later date.

Q67: Which “open” standards are you interested in?

A67: We are undecided and looking for industry feedback; however, standards used by allies would likely have an influence.

Q68: From a size perspective, which allied force are you most aligned with?

A68: We are not modelling the project on any current allied force, but we are observing what they are doing throughout the FVEY partners.

Q69: Do you foresee using Military Intelligence Database (MIDB)?

A69: Nothing has been decided in this regard.

Q70: How will you combine the best of what industry has to offer, as articulated in the LOI responses, without developing an unrealistic design?

A70: At the moment, all input from industry is just to inform us of what is possible. This information will impact the high level system design, which in turn will result in a workable solution.

Q71: Are you considering a phased approach?

A71: A key consideration is agility, so a phased approach is not off the table. We are also interested in an “Ever-Green” approach to keep the capability relevant to keep pace with rapid technology changes.

Q72: Regarding technical standards, have you decided how you will satisfy coordination and cooperation requirements?

A72: We are not at that level yet, but are pushing for an open architecture.

Q73: Do you foresee RCAF, RCN, and allied forces feeding into the system?

A73: Yes, we will look at all Canadian sources, but at the moment there are too many unknowns about allied interoperability to give a definitive answer.

Q74: Regarding joint interface control document (JICD), will you look to decouple hardware from software?

A74: This has not been decided, but we look forward to industry suggestions.

Q75: Regarding Unmanned Aerial Systems (UAS), what capability are you concerned with?

A75: At this time, we are concerned with micro and mini UAS.

Q76: When you look to counter UAS, etc. are you looking at a “brute force” solution or something more nuanced?

A76: All options are on the table at this point.

Q77: What level of security are you looking for?

A77: At least Secret; however, we can see a need to go from UNCLAS all the way to Top Secret/Special Access (TS/SA).

Q78: Who will integrate equipment to vehicles; DND, a contracted integrator, etc.?

A78: No decision has been made, but it will likely depend on what vehicles are utilized.

Q79: What additional avenues exist to de-risk the project? Is it possible to utilize de-risk activities already completed in the FVEYs?

A79: Further in the project there may be funds to assist in de-risk activities. Currently, we do not know if we could accept previously completed de-risk activities from the FVEYs. We will investigate further.

Q80: Is it anticipated that options 1, 2, and 3 will be fully costed in the RFI?

A80: The costing requirement for which Option(s) will be further articulated in the RFI. See Q 21 for more information.

Q81: How many man-packs will be required?

A81: Unknown as we are still at the concept stage, but we could be looking at approximately x2 Companies for MFEW and x3 Sections of Electronic Support (ES).

Q82: Can you share the technical details of MAESTRO?

A82: No, we cannot share specific technical details, but details relating to the results of MAESTRO will be part of the RFI.

Q83: Will you make a decision about standards by the time the RFP is released.

A83: Most likely.

Q84: Can you say what your objectives are regarding “open-standards”.

A84: Not specifically as we are still collecting relevant information; however, we are very interested in your input.

Q85: Should resultant systems co-exist? In other words, are you looking for equipment that works side-by-side, or are you looking at full interoperability?

A85: Yes, we are looking for full interoperability for the Canadian capability.

Q86: Do you foresee all IP coming exclusively from the primes, or government and sub-contractors as well?

A86: It will ultimately depend on the options chosen, but we can’t exclude anything at the moment.

Q87: Do you see the solution as being a single vehicle type with all the “bells and whistles”, or do you foresee something scalable?

A87: Vehicles will likely have a standard “box”, but we do want the solution to be scalable, i.e. we would like the ability to ramp up or down depending on the task/threat. We are looking for industry guidance in this regard.

Q88: Do you have any information on potential installers?

A88: No, not at this time, but industry can influence this.

Q89: Can you provide us with vehicle integration standards?

A89: Not at this time, but we are looking forward to industry feedback in this regard.

Q90: Given the speed of threat development, can you or will you de-couple the hardware and software development cycles?

A90: It is too early to tell. However, we must react quickly to new threats and changing scenarios. Therefore, we need the ability to upgrade software with new waveforms, algorithms, data sets, etc. that will be produced by government subject matter experts using a SDK type capability.

B. Provide the Industry Day presentation see attached.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME

Canadian Forces Land Electronic Warfare Modernization Project (CFLEWM)

INDUSTRY ENGAGEMENT SESSION

Ottawa, Ontario

June 11th, 2019

Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Canadä

OPENING REMARKS

Colonel C.C. Renahan

Director Land Requirements

DND

Transcript not available

Respect ◆ Integrity ◆ Excellence ◆ Leadership
Serving GOVERNMENT, Serving CANADIANS.

OPENING REMARKS

Ryan Moreira
Deputy Director
Industrial and Technological Benefits Branch
ISEDC
Transcript not available

OPENING REMARKS

Rita Brown

Manager

Electronics, Munitions, and Tactical Systems Procurement
Directorate (EMTPSD)
Acquisitions Branch, PSPC

Transcript not available

PSPC Mandate

- Public Services and Procurement Canada acts as a Common Service Agency for the Government of Canada

- Its activities are directed mainly towards providing other departments, boards, and agencies with services in support of their programs

- Service Delivery includes:
  - Real Property
  - Accounting and Banking
  - Receiver General
  - Informatics and Telecommunications
  - Procurement and Contracting (focus of presentation)
  - Canada Post

Contracting Principles & Objectives

- Integrity
- Competition
- Openness and transparency
- Assist departments/agencies to meet their objectives
- Socio-economic objectives
- Legal and policy framework, including Trade Agreements

Defence Procurement - What Do We Do?

- ➢ The Defence Production Act (1951) provides our Minister exclusive authority to acquire defence supplies/construction/projects
- ➢ Establish and manage contracts to acquire a wide range of technically complex systems for the Army, Navy and Air Force including the acquisition of:
  - Military and Civilian Aircraft & Systems
  - Ships & Marine Systems
  - Armament Systems & Munitions
  - Armoured Vehicles
  - Electronics & Communications Systems
  - Trainers & Simulators
  - Associated Repair & Overhaul Activities
  - Information Security and Electronic Warfare
- ➢ We manage procurements under the Munitions Supply Program to maintain a Canadian industrial capability for high volume ammunition and small arms.

Stakeholders in Canadian Defence Procurement

DND

Finance

Treasury Board

Innovation Science and Economic Dev Canada

Regional Development Agencies

Industry

PSPC

Privy Council Office

Justice

Global Affairs Canada

INDUSTRY ENGAGEMENT PROCESS

Christine Picknell
Contracting Authority
Acquisitions Branch, PSPC

Industry Consultation

- It is Canada’s intent to actively engage and consult Industry throughout the procurement process to ensure a successful project end-state.
- The Letter of Interest (LOI) and engagement process provides Industry with the opportunity to present their feedback regarding the concept described.
- Canada is seeking information on industry capabilities, sustainment, and different solutions.

Industry Engagement Process Overview

- In order to maximize the benefits of the engagement process, Canada may endeavor to solicit comments from participants on various issues raised.

- The engagement process will consist of the LOI, RFI, one-on-one meetings, group follow-up meeting, a possible draft RFP(s), and any other processes deemed necessary by the Procurement Authority.

- Potential respondents are advised that any information submitted to Canada in the engagement process may be used by Canada in the development of a competitive RFP.

- A Fairness Monitor (FM) has been employed to oversee the engagement and procurement process and will remain until contract award.

Engagement Process Guiding Principles

Transparency: ensuring procurement integrity by sharing all procurement outcomes and activities with stakeholders;

Fairness: stakeholders will get an equal opportunity to access engagement activities;

Timeliness: Engagement activities will be planned and conducted early in the procurement process; and

Relevancy: to include tangible, useful, and current outputs that are in alignment with Government of Canada priorities.

Engagement and Procurement Process

- **Phase 1: Summer 2019**
  - Letter of Interest (LOI) – closing June 26
  - Unclassified Industry Day
  - Unclassified One-on-One Meetings

- **Phase 2: January 2020**
  - Request for Information (RFI)
  - Industry Day
  - Possible Classified One-on-One Meetings

- **Phase 3: Request for Proposal (RFP) 2023**

Purpose of Current Letter of Interest

- Solicit feedback from suppliers on proposed solutions to help DND realize their capabilities in the CFLEWM project;
- Solicit advice on how CFLEWM solution can be sustained throughout its life cycle;
- Inform industry of the proposed procurement approach;
- Advise suppliers of the possible security requirements of the potential follow on industry engagement and provide direction and assistance to unscreened suppliers in obtaining security clearances;
- Provide direction and assistance to suppliers in obtaining security clearances and registering with the Controlled Goods Program; and
- Solicit feedback on Industrial and Technological Benefits.

CANADIAN ARMY ARMÉE CANADIENNE

Industry Engagement

Canadian Forces Land Electronic Warfare Modernization

Major Darrell Williams, Project Director

Major Eric McFee, Project Manager

11 June 2019

CANADIAN ARMY ARMÉE CANADIENNE

OUTLINE

- Why do we have the problem?
- What is the problem?
- What is the concept for solution?
- Questions / Comments / Discussion

The content of this presentation is **UNCLASSIFIED** but for **OFFICIAL USE ONLY**.

Canadian Forces Land Electronic Warfare Modernisation

Why?

- Technology has changed rapidly in the last twenty years.

- Use of the EM Spectrum has become critical to most activities in modern military operations.

- New technologies are driving a paradigm shift in EMSO.

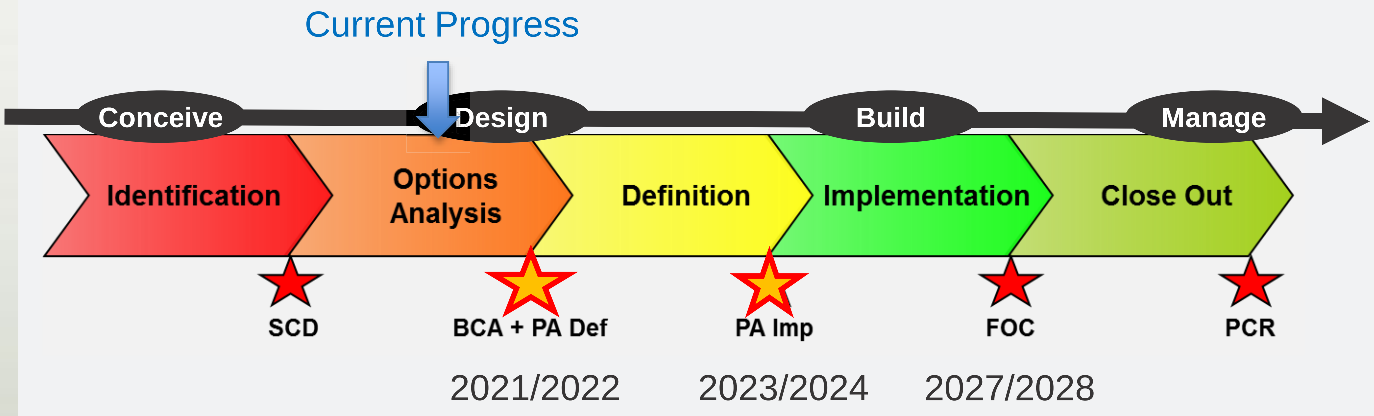
- The ability to effect change in the use of the spectrum has become necessary.

What? Capability Deficiencies

- Limited ability to collect on evolving targets.
- Limited ability to counter the diversity of evolving & emerging threats to Land platforms (i.e. RC-IED, UAS).
- Lack of offensive Electro-Magnetic (EM) non-kinetic, non-lethal fires.
- Insufficient ability to deny the EM spectrum to adversary.
- Lack of tools for command, control, and coordination of EW effects.
- Insufficient ability to develop and maintain an EM spectrum operations common operating picture.

Canadian Army Capability Development

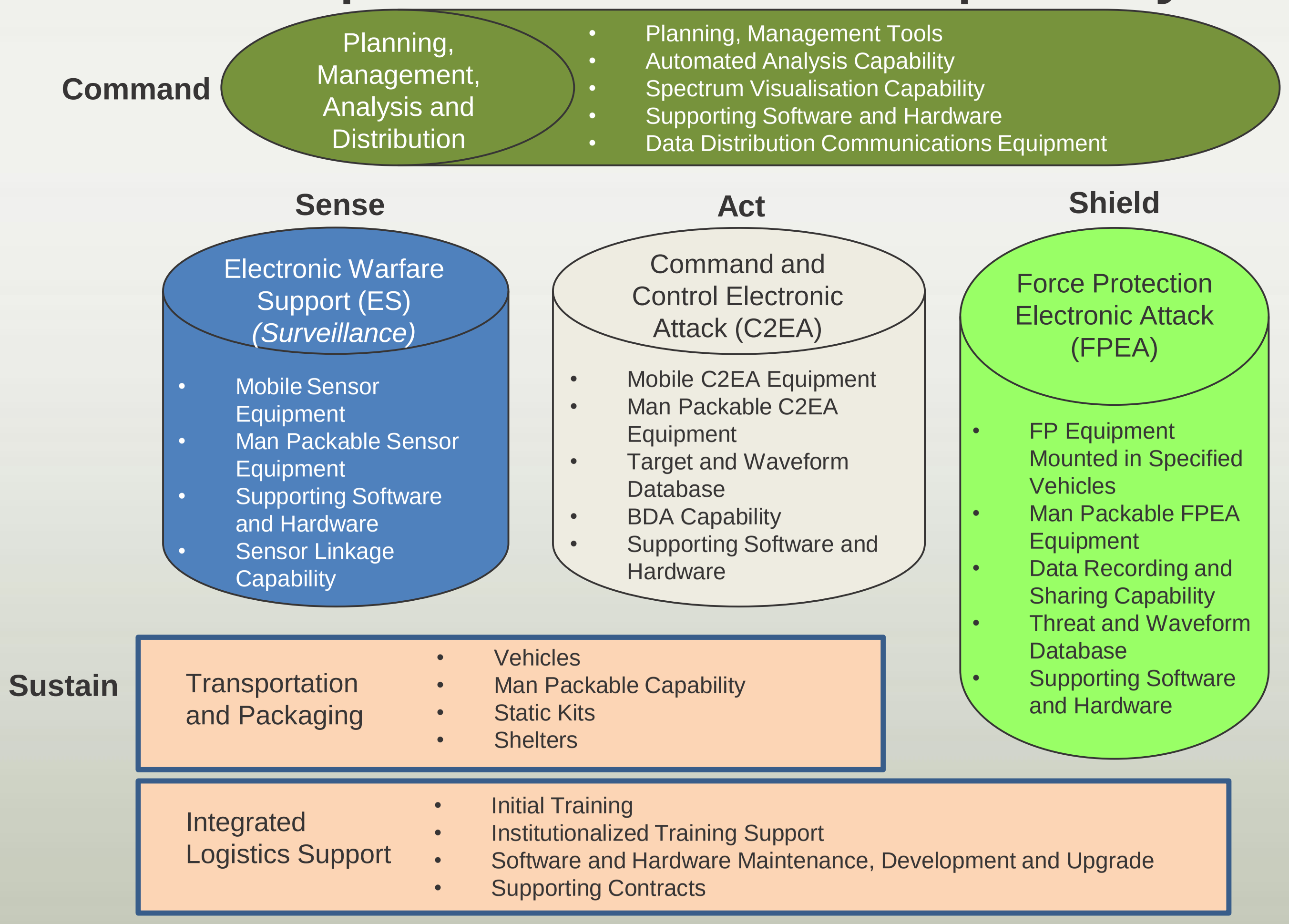
The DND Project Life Cycle



CANADIAN ARMY ARMÉE CANADIENNE

STRONG. PROUD. READY.
FORTS. FIERS. PRÊTS.

A Complete Land EW Capability



Command

Planning, Management, Analysis and Distribution

- Planning, Management Tools
- Automated Analysis Capability
- Spectrum Visualisation Capability
- Supporting Software and Hardware
- Data Distribution Communications Equipment

Sense

Electronic Warfare Support (ES) *(Surveillance)*

- Mobile Sensor Equipment
- Man Packable Sensor Equipment
- Supporting Software and Hardware
- Sensor Linkage Capability

Act

Command and Control Electronic Attack (C2EA)

- Mobile C2EA Equipment
- Man Packable C2EA Equipment
- Target and Waveform Database
- BDA Capability
- Supporting Software and Hardware

Shield

Force Protection Electronic Attack (FPEA)

- FP Equipment Mounted in Specified Vehicles
- Man Packable FPEA Equipment
- Data Recording and Sharing Capability
- Threat and Waveform Database
- Supporting Software and Hardware

Sustain

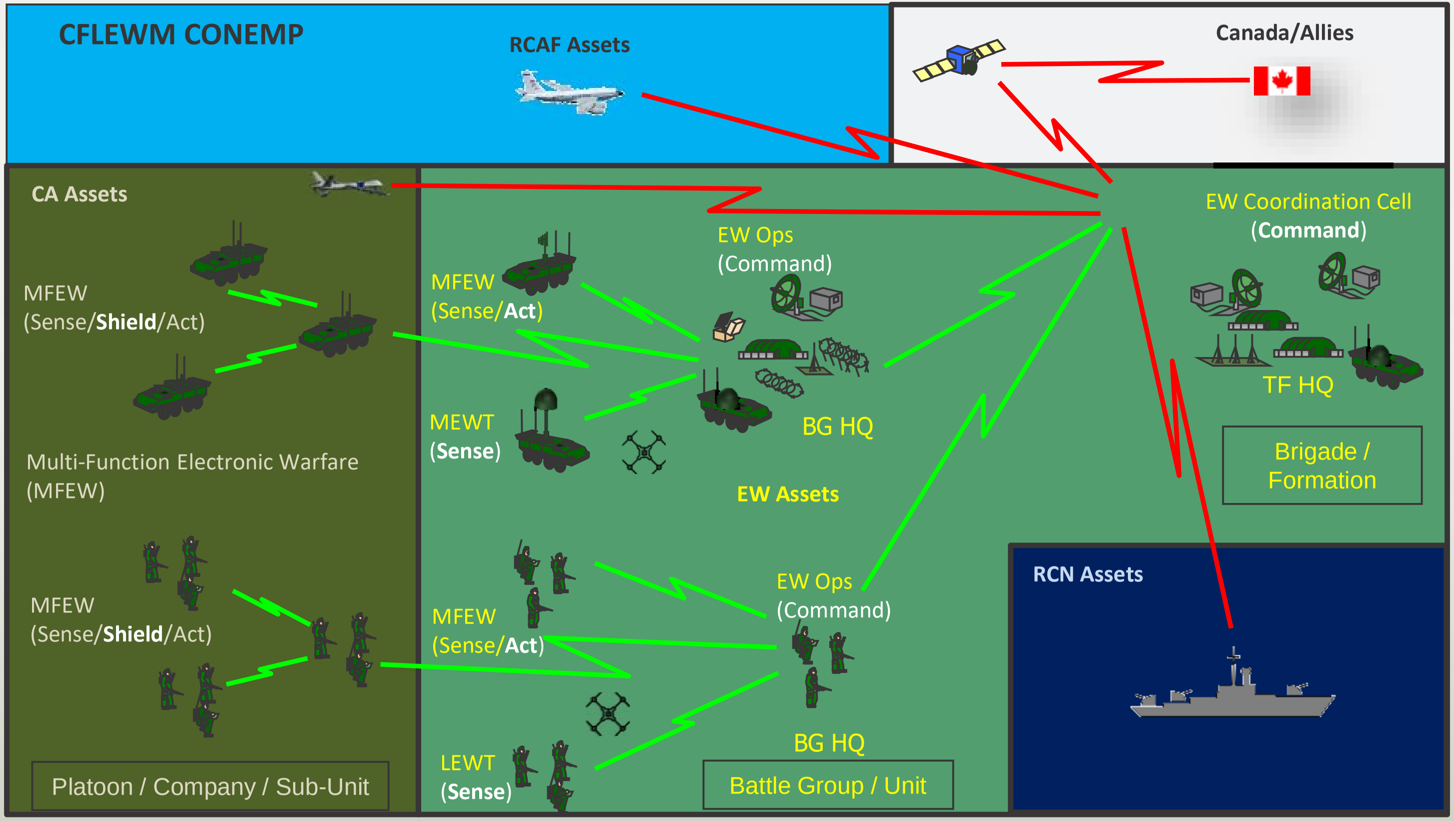
Transportation and Packaging

- Vehicles
- Man Packable Capability
- Static Kits
- Shelters

Integrated Logistics Support

- Initial Training
- Institutionalized Training Support
- Software and Hardware Maintenance, Development and Upgrade
- Supporting Contracts

Proposed CFLEWM CONOP



Abbreviations:

- MFEW - Multi-Function EW
- MEWT – Mobile Electronic Warfare Team
- LEWT – Light Electronic Warfare Team

This is the proposed CFLEWM OV-1

STRONG. PROUD. READY.
FORTS. FIERS. PRÊTS.

High Level Mandatory Requirements Summary

Requirement	HLMR	Includes
1.3.2.1	EW Command	Understanding the Electromagnetic Environment (EME), Exporting Data, Planning EW Operations, Execute and Control EW Operations, Analyse Friendly Force Interference
1.3.2.2	EW Sense	Detect Signal of Interest (SoI),Classify the SoI, Analyse the SoI, Exploit the SoI, Geographically locate SoI, Survey the EME, Record the SoI
1.3.2.3	EW Act	Execute Non-Kinetic Actions, Target Adversarial use of the EME, System Interoperability, Control of Act System, Act Configuration
1.3.2.4	EW Shield	Control of Shield System, Detect RC Threats, Target RC Threats, Geographically Locate, Suppress EME Threats, Record EME, Shield System Interoperability, Shield Configuration
1.3.2.5	EW Sustain	Training, Support to Operations
1.3.2.6	Common	Compatibility, Flexibility

Key Issue: CFLEWM is currently scoped/funded to provide ECM capability for 1 BG. SSE ‘Concurrent Operations’ may require additional capability, potentially an additional BGs worth of equipment and personnel resources including Brigade enablers.

Programmatic Update

- Capital Investment Fund 2018 for this project publicly released $250-400M CAD.

- First engagement to seek feedback on concept.

- Request for Information (RFI) will build on responses from LOI and is planned to be released in early 2020.

- Request for Proposal (RFP) is planned for release in 2023.

Options

- **Option 1 (Prime Contractor)**: The contractor would be responsible for all aspects of integration, sub contracting, and delivery of a complete capability. Competitive process.

- **Option 2 (DND as Integrator)**: DND would act as the integrator to develop a complete capability. Multiple contracts to provide sub-components. Could be a combination of Competitive, FMS, sole source (for allied interoperability).

- **Option 3 (DND as Design Authority)**: Multiple contracts including an integration contract that is responsible to integrate the sub-components contracts into a complete capability under direction of DND. Could be a combination of Competitive, FMS, sole source (for allied interoperability).

Innovation, Science and
Economic Development Canada

Innovation, Sciences et
Développement économique Canada

Industry Engagement for Canadian Forces Land Electronic Warfare Modernization (CFLEWM)

Industrial and Technological Benefits/ Value Proposition

June 11, 2019

Building a prosperous and innovative Canada

Canada

Outline

- Objective
- Defence Procurement Strategy
- Industrial and Technological Benefits including Value Proposition
- Skills Development and Training Pillar
- Key Industrial Capabilities (KICs)
- Industry Consultation
- Next Steps

Objective

- The Government of Canada is consulting with industry to support the development of an approach for leveraging economic benefit for the Canadian Forces Land Electronic Warfare Modernization (CFLEWM) Project.

- Feedback from industry will be used to:

    - Validate the Government of Canada’s analysis of the Canadian information technology industry sector and related capabilities; and,

    - Develop an economic leveraging approach in support of the CFLEWM project.

Canada’s Defence Procurement Strategy

- **Announced in February 2014, by the Ministers of:**
  - Public Works and Government Services (now Public Services and Procurement Canada)
  - National Defence
  - Industry Canada (now Innovation, Science and Economic Development Canada)
- **Goals:**
  - Deliver the right equipment to the Canadian Armed Forces and the Canadian Coast Guard in a timely manner
  - Leverage purchases of defence equipment and services to create jobs and economic growth in Canada
  - Streamline the defence procurement process

Industrial and Technological Benefits (ITB) Policy

- The Industrial and Technological Benefits (ITB) Policy has been in place since 1986. In 2014, it was transformed to include the Value Proposition (VP).

  - Winning bidders are selected on the basis of price, technical merit and their Value Proposition
  - The VP includes bidder’s commitment to undertake work in Canada and will generally account for 10 percent of the overall score
  - Companies awarded procurement contracts must undertake business activity in Canada equal to the value of the contract

Value Proposition

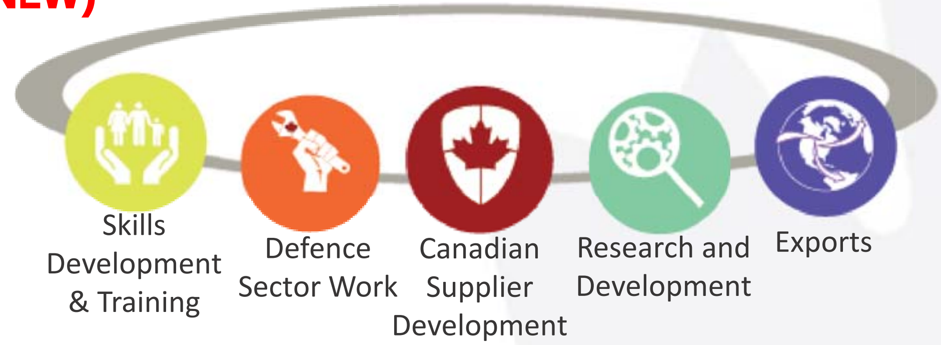
- Commitments/activities proposed at bid time
- Rated and weighted during bid evaluation

Outstanding Obligation

- Activities identified after contract award
- Brings identified activities up to 100 percent of contract value

Value Proposition Pillars

- Supports the long-term sustainability and growth of Canada's **defence industry**;
- Supports the growth of bidders' Canadian operations as well as their **suppliers in Canada**, including SMBs in all regions of the country;
- Enhances innovation through **research and development (R&D) in Canada**;
- Increases the **export** potential of Canadian-based firms; and
- Promotes **skills development and training** to advance employment opportunities for Canadians. **(NEW)**



Skills Development & Training Pillar (NEW)

- The Skills Development & Training Pillar was created to address current or anticipated skills gaps and training opportunities

- Bidders will be encouraged to identify initiatives to develop skills and training through:
  - ✓ Work integrated learning programs (e.g., co-operative education; work placements)
  - ✓ Apprenticeship programs
  - ✓ A new or existing skill development program at or through a post-secondary institution
  - ✓ Other activities that align with the ITB objectives for skills development and training

The VP is a flexible framework

On a procurement-by-procurement basis, there is flexibility to:

- Increase/decrease the weight of the VP
- Weigh individual evaluation criteria differently
- Apply all or some of the evaluation criteria
- Add additional evaluation criteria
- Apply mandatory requirements
- Develop different rating grids

Informed by:

Industry engagement

Research and analysis

3rd party experts

Key Industrial Capabilities (KICs)

- Key Industrial Capabilities (KICs) were introduced in April 2018 to ensure that defence procurements can better drive innovation, exports and the growth of firms through the ITB Policy.

- KICs represent areas of emerging technology with the potential for rapid growth, established capabilities where Canada is globally competitive, and areas where domestic capacity is essential to national security.

- KICs are defined as the skills, technologies, and supply chains required to support the growth of these capabilities. They are broader than the companies associated with the end solution; they include the post-secondary institutions that develop skills and research, the SMEs that form part of the value chain, and intellectual property that is developed in Canada.

Key Industrial Capabilities

EMERGING TECHNOLOGIES

- Advanced Materials
- **Cyber Resilience**
- Remotely-piloted Systems and Autonomous Technologies
- **Artificial Intelligence**
- Space Systems

LEADING COMPETENCIES & CRITICAL INDUSTRIAL SERVICES

- Aerospace Systems & Components
- **Defence Systems Integration**
- Ground Vehicle Solutions
- Marine Ship-Borne Mission and Platform Systems
- Shipbuilding, Design and Engineering Services
- Training & Simulation
- Armour
- Electro Optical / Infrared Systems
- In-Service Support
- Munitions
- Sonar & Acoustic Systems

Industry Consultation

- The Government of Canada is seeking industry feedback to support the development of the economic leveraging approach for the CFLEWM project

- Industry engagement questions were published on Buyandsell in advance of the CFLEWM Industry Day.

- We encourage all potential bidders and suppliers to provide comments.

Next Steps

- Written feedback regarding the ITB/VP questions is to be submitted to the PSPC Contracting Authority.
- Information provided to the Government of Canada will be considered in the development of the economic leveraging approach for the CFLEWM project.
- For more information on Canada’s Industrial and Technological Benefits Policy, please visit: http://www.canada.ca/itb

For any ITB related questions, contact:

Mr. Mathieu Belanger

Project Manager

Industrial and Technological Benefits Branch

Innovation, Science and Economic Development Canada

Tel: (613) 410 2344

Email: mathieu.belanger@canada.ca

Website: http://www.canada.ca/itb

Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Canadä

Controlled Goods Program

General program overview and how to register

Dominic Dubé
Education Program Officer
Controlled Goods Program
Program Management and Learning Division

Serving GOVERNMENT, serving CANADIANS.

The Controlled Goods Program’s Raison d’être

“To ensure that controlled goods are safeguarded while in the custody of private sector companies and protected against unauthorized access.”

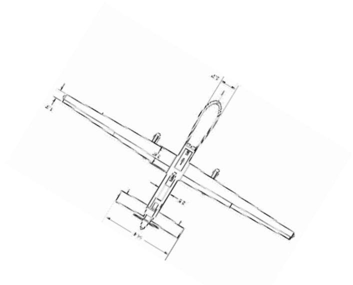
The Controlled Goods Program

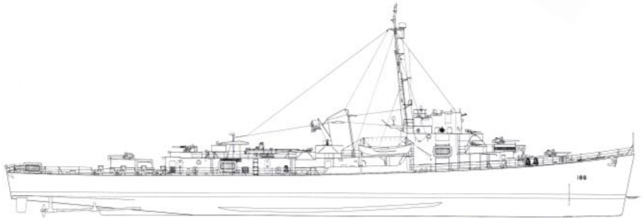
- Established in 2001 to support the provision of the Canadian exemption under the U.S. *International Traffic in Arms Regulations* (ITAR)

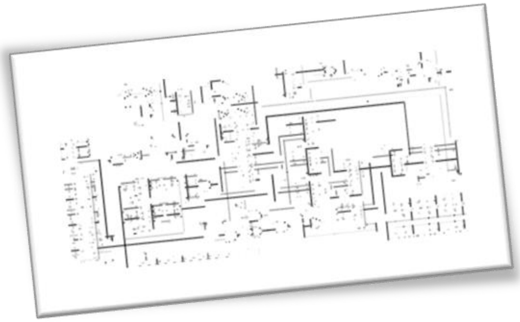
- Legislated by the *Defence Production Act* (DPA) and *Controlled Goods Regulations* (CGR)

Definition of controlled goods

- Controlled goods are primarily goods, including components and technical data that have military or national security significance, which are controlled domestically by the Government of Canada and defined in the *Defence Production Act*







Summary, controlled goods are

- goods, including components and technology (for example, blueprints and technical specifications in paper or electronic format), with strategic significance or national security implications, regardless of where they are manufactured

- defense articles originating from the United States that are controlled by the United States Munitions List—part 121 of the United States International Traffic in Arms Regulations, as amended from time to time

- goods, regardless of where they are manufactured, that are manufactured from technical data originating from the United States and are controlled by the International Traffic in Arms Regulations

Controlled Goods List

- Controlled Goods List contained in the schedule (section 35) of the *Defence Production Act*

- Guide to the schedule to the *Defence Production Act*
  - provides a simplified listing of the items that are identified as controlled goods in the *Defence Production Act*.
  - helps identify whether or not an item is included on the Controlled Goods List
  - schedule takes precedence over the guide

Why register

- It is the law. Individuals and organizations must register in the Controlled Goods Program if they need to **examine**, **possess** or **transfer** controlled goods. During registration, applicants must demonstrate this need

- Failure to register may be considered an offence under federal laws, and could lead to prosecution and sanctions

Any person who fails to comply with the *Defence Production Act* may:

- have their registration with the Controlled Goods Program suspended or revoked

- face prosecution for failing to comply and be subject to a fine not exceeding $2,000,000, and/or imprisonment not exceeding 10 years

As an individual or an organization, you must register before you:

- examine, possess or transfer controlled goods in Canada

- transfer controlled goods outside of Canada
  - registration is required before getting an export permit from Global Affairs Canada

- receive bid solicitation documents containing controlled goods or controlled technology

Understand if you are examining, possessing or transferring controlled goods

- **Examine** means to consider in detail or subject to analysis in order to discover essential features or meaning

- **Possess** means either actual possession, where the person has direct physical control over a controlled good at a given time, or constructive possession, where the person has the power and the intention at a given time to exercise control over a controlled good either directly or through another person or persons

- **Transfer** means, with respect to a controlled good, to dispose of it or disclose its content in any manner

Roles in the Controlled Goods Program

Owner

- owns 20% or more of the outstanding voting shares or interests of the business

Authorized Individual

- usually the owner or another senior official of the organization with signing authority

Designated Official

- completes mandatory training for designated officials
- conducts security assessments of employees, officers and directors
- determines the risk of transferring controlled goods to anyone who is not registered or is not exempt from registration and authorizes the extent to which they may examine, possess or transfer controlled goods
- verifies the information provided to them by temporary workers, international students and visitors for the purpose of applications for exemption and submit the exemption requests to the CGP

How to register

To register in the Controlled Goods Program, you must complete the following steps:

1. Appoint an authorized individual
2. Appoint a designated official
3. Complete the application for registration form
4. Complete a security assessment application form for each required individual
5. Review your applications and supplementary documentation
6. Submit your application

Application for Registration

- submit a completed & signed Application for Registration
  - Section H (Certification and consent), is signed by the Authorized Individual
- provide evidence of the legal status of the company (e.g. copy of Certificate of Incorporation, Master Business Licence, etc.)
- clearly provide a description of your business activities in relation to controlled goods on the application form as well as any companies with whom you have / will have a business relationship involving controlled goods. If you have supporting documentation regarding justification for registration, such as a contract, an RFP, a Third Party E-mail / Letter, please submit those as well
- controlled goods to be listed in section D.10
  - when bidding on contracts with controlled goods, check with the bid authority to obtain the CGL item numbers and descriptions

Authorized Individual and all Owners of 20% or more

- submit a completed & signed Security assessment application
- two pieces of government-issued identification (at minimum one must be photo identification)
  - – proof of citizenship (for example, birth certificate, passport, permanent resident card)
  - – proof of residence (for example, driver's license, government-issued document with address)
- certified criminal record check based on fingerprints **or** a name-based criminal record check verified against the RCMP's Canadian Police Information Centre (CPIC) system . When completing the form, please use “**private sector**” for employment and ensure the results are sent to the applicant’s home address, so they can then be submitted with the application and other documentation
  - – for foreign individuals or those who have lived outside of Canada for 6 consecutive months or more within the last 5 years, we require a Criminal History check from a recognized police agency – Example: Certificate of Good Conduct; FBI Check, Police certificate

Designated Official(s)

- submit a completed & signed Security assessment application
- two pieces of government-issued identification (at minimum one must be photo identification)
  - proof of citizenship (for example, birth certificate, passport, permanent resident card)
  - proof of residence (for example, driver's license, government-issued document with address)
- certified criminal record check based on fingerprints - have electronic fingerprints taken. When completing the form, use “**private sector**” for employment and ensure the results are sent to the applicant’s home address, so they can then be submitted with the application and other documentation

Processing times

- an application for registration, along with all supporting documentation, can take 32 business days to process

- you may inquire about the status of your registration after a four week waiting period

- we accept only complete applications with all supporting documents

- if incomplete (missing signatures, missing supporting documents, missing fingerprint results, etc.), the application will be returned

Submitting applications

Mail / Courier

Controlled Goods Program
Public Services and Procurement Canada
PSPC Central Mail Room
Portage III, 0B3
11 Laurier St
Gatineau QC K1A 0S5

E-mail
dmc-cgd@tpsgc-pwgsc.gc.ca

Facsimile
(613) 948-1722

Registration checklist

- ❑ Company
  - ❑ Application for registration
  - ❑ Evidence of the legal status of the company in Canada
- ❑ Authorized Individual
  - ❑ Security assessment application
  - ❑ two pieces of government-issued identification
  - ❑ Certified criminal record check or a name-based criminal record check
- ❑ all Owners of 20% or more
  - ❑ Security assessment application
  - ❑ two pieces of government-issued identification
  - ❑ Certified criminal record check or a name-based criminal record check
- ❑ Designated Official(s)
  - ❑ Security assessment application
  - ❑ two pieces of government-issued identification
  - ❑ Certified criminal record check

Questions?

Website: http://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html

Email: DMC-CGD@tpsgc-pwgsc.gc.ca

Toll-free number: 1-866-368-4646

National Capital Region: 613-948-4176

Call us Monday to Friday, 8:00 am to 5:00 pm Eastern time. Services are available in English and French.

Public Services and Procurement Canada’s Contract Security Program

June 11, 2019

Laura Haddad
Senior Client Relations Officer
Public Services and Procurement Canada
Industrial Security Sector, Outreach Division

Jonathan Joubert
Outreach Officer
Public Services and Procurement Canada
Industrial Security Sector, Outreach Division

Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Canada

Overview

- PSPC’s Contract Security Program
- Types of organization security screenings
- Organization security screenings and subsets
- Sponsoring process
- Registration roadmap
- Personnel security screening
- Aftercare
- Subcontracting process
- Your roles and responsibilities
- Request for visit procedure
- Webinars
- Questions
- Contact us
- Useful links

PSPC’s Contract Security Program

- enables industry to participate in sensitive government contracts in Canada and abroad

- provides security screening services for organizations and their employees

- ensures the necessary contract security clauses are included as part of contracting vehicles

- ensures industry complies with contracting security requirements

Types of organization security screenings

	Organization screening	**Personnel security screening**	**Information and assets**
Classified National interest	Facility security clearance	Top Secret	Top Secret
		Secret	Secret
			Confidential
Protected Non-national interest	Designated organization screening	Enhanced reliability	Protected C
		Reliability status	Protected B
			Protected A

Organization security screenings and subsets

Document safeguarding capability

If the contract requires the **safeguarding of sensitive information and/or assets at a contractor's site(s)**, your organization will also need to obtain a <u>document safeguarding capability (DSC)</u> at the level specified in the contract.

PSPC's Contract Security Program will conduct physical security inspections:

- **before contract award** for the following contract security requirement:
  - DSC
  - production capability
  - authority to process information technology (IT)

Your organization must be willing to **make the required changes** to your facilities as well as **incur the cost(s)** in order to be approved for DSC.

Organization security screenings and subsets (cont'd)

Authority to process information technology (IT)

If your organization is required to **use its own IT system(s) to produce, process or store sensitive information electronically**, your organization will also need to obtain the authority to process IT.

- IT requirements are defined by the client department in a **technical document** attached to the contract

- PSPC's Contract Security Program will conduct an IT security inspection typically **after contract award**

Renewal timelines

Document safeguarding capability

Production capability

Shredding capability

Bulk storage capability

Security level	Renewal timelines
Protected A	4 years
Protected B	3 years
Protected C	1 year
Confidential	2 years
Secret	2 years
Top secret	1 year
NATO Confidential	2 years
NATO Secret	2 years
NATO Top secret	1 year
production	contract specific
shredding	2 years

Sponsoring process

To register in PSPC’s Contract Security Program (CSP), organizations must be sponsored by a Government of Canada **approved sources.**

Who can be an approved source?

- a government of Canada procurement officer
- a Government of Canada security officer or project manager
- a prime contractor registered in PSPC’s CSP
- national and designated security authorities on behalf of a foreign company or government that is contracting to the organization

Registration roadmap

To clear personnel, your organization must first be security cleared!

PSPC's Contract Security Program will request the following:

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
The approved source submits private sector organization screening (PSOS) & security requirement checklist (SRCL) to PSPC's Contract Security Program (CSP), to sponsor your organization into the program.	Your organization is contacted by PSPC's CSP. You will receive an establishing letter, asked to **complete** screening forms, a series of registration forms and appoint a company security officer (CSO). **If required:** your organization will also appoint an alternate company security officer (ACSO) and identify key senior officials (KSO).	Your organization **submits** the completed registration forms to PSPC's CSP (within 30 days). Incomplete forms may result in rejection of registration application.	PSPC's CSP **reviews** your organization's registration forms, analyzes security requirements, your organization structure, its ownership and required signatures.	Your organization **replies promptly** to PSPC's CSP if any information or signatures are missing, forms are incomplete or if further details are required.	PSPC's CSP **processes** personnel security screening/ clearance for CSO/ ACSO and KSOs (where required) and grants screening/ clearances.	Your organization is officially **registered** in PSPC's CSP. You can now submit *personnel security screening requests* for your employees and register to use the **Online industrial security services (OLISS).**

Most common errors:

- Missing signatures where required
- Missing copies of CSO photo ID
- Missing proof of business ownership
- Missing Annex 1B if appointing an ACSO

Processing timelines

Organization security clearances	Estimated processing timelines
Designated organizational screening	up to 4 months
Facility security clearance (Secret)	6 months or more
Facility security clearance (Top Secret)	12 months or more
Document safeguarding capability	varies
Authority to process IT	varies

Personnel security screening

Electronic fingerprint requirement

- criminal record name check process (CRNC) replaced with a criminal record check process that uses **electronic fingerprinting**
- **mandatory** for **new, update and upgrade** clearance requests **(as of February 1st 2017)**

Credit check

- soft check completed by a credit bureau
- **mandatory** for all **new, update and upgrade** clearance requests **(as of January 29, 2018)**

- these requirements **do not** affect the **validity** of existing clearances
- personnel must provide **consent**

Service standards

Personnel security screening	Service standards
Reliability status (simple)	7 business days
Reliability status (complex*)	up to 120 business days
Secret (simple)	up to 4 months
Secret (complex*)	up to 12 months
Top Secret	12 months or more

* additional information and/or verifications required

Aftercare

- new provision in the Treasury Board of Canada Secretariat ***Standard on Security Screening*** (Appendix F): https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115&section=html

- assurance that the supplier will remain compliant

- minimizes risk in working with sensitive information

- reduces potential delays that could affect contract timelines and costs

- helps prevent security breaches

Aftercare (cont’d)

security briefing

ongoing assessment of eligibility

reporting changes in behaviour

reporting changes of circumstance

reporting unusual contact or incidents

Subcontracting process

The prime contractor’s **company security officer (CSO)** or **alternate company security officer (ACSO)** is responsible for: :

1. completing an security requirement checklist (SRCL) identifying the security requirements of the subcontract
2. requesting a private sector organization screening (PSOS) on behalf of the subcontractor
3. submitting the SRCL and PSOS form to PSPC’s Contract Security Program (CSP) for approval
4. obtaining and inserting the security clauses and SRCL into the subcontract
5. validating the subcontractor’s organization and personnel are cleared
6. submitting a copy of the awarded subcontract containing the SRCL to PSPC’s CSP

Work cannot start until the subcontractor obtains the appropriate security screening

Identifying subcontractors

- Subcontracts are used when a **prime contractor** wishes to subcontract a portion of the prime contract to another organization or self-employed individual.
  - example:

subcontractor: a building contractor who subcontracts electrical wiring work to an electrician

VS.

employee: a building contractor who hires a permanent electrician to work on various projects

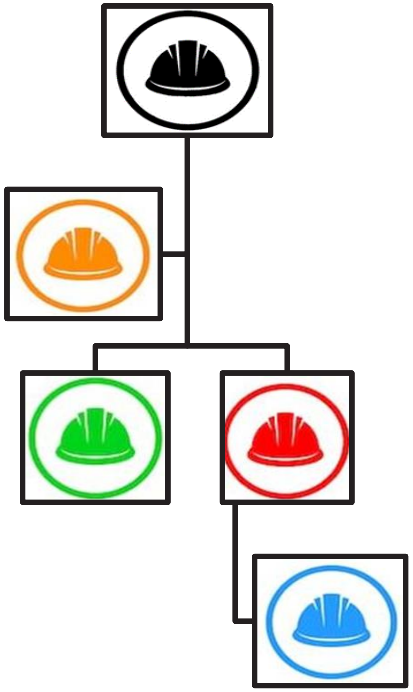
- Security needs to be considered in subcontracts when the prime contract has security requirements.

A contractor cannot request personnel screenings for employees of a subcontracting organization.

Identifying subcontractors (cont'd)

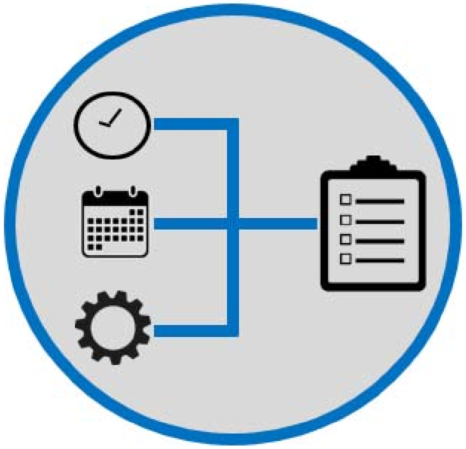
Before initiating a subcontract with security requirements, the **prime contractor** must seek prior approval from PSPC's Contract Security Program (CSP) to ensure that:

- the subcontract has the **same security requirements** as the prime contract (or lower)
- the subcontractor has the **appropriate security clearance**



Your roles and responsibilities

- find an **approved source**
- **comply** with PSPC’s Contract Security Program registration process
- **obtain and maintain** your organization security clearance
- **screen personnel** involved in government sensitive contract
- meet **physical security requirements** if necessary
- **identify subcontractors** and ensure security of subcontracts if necessary



Request for visit procedure

- a request for visit is required for a security-cleared individual to:
  - visit a government/commercial organization in **Canada or abroad**
  - access protected/classified information or assets while visiting a restricted government installation
- must include a justification, the contract number or the project/program name
- must be approved by PSPC’s Contract Security Program

Types of visit requests

Types of visit requests	Description
Canada to Canada	Canadian visit to a Canadian organization or government facility
Canada to foreign	Canadian visit to a foreign organization or government facility
Canada to United States (US)	Canadian visit to an American organization or American government facility
US to Canada	American visit to a Canadian organization or Government of Canada facility
Foreign to Canada	A foreign visit to a Canadian organization or government (from a country other than the United States) facility

Types of visit requests (cont'd)

- a **one-time visit** is a single, not amendable, event over a specified period of time (less than a month) i.e., a meeting, conference or a symposium

- a **recurring visit** is a series of separate visits, amendable, for the length of the contract (maximum of one year) i.e., a frequent check point verification

- an **emergency visit** is reserved for visits of an **urgent nature**

- **amendments** are for renewing a recurring visit, adding or removing individuals from the visitor listing or adding locations

Request for visit timelines

Australia	35
Belgium	28
Denmark	22
Finland	29
France	30
Germany	35
Israel	35
Italy	35
Netherlands	25
New Zealand	25

Norway	25
Spain	35
Sweden	30
Switzerland	35
United Kingdom	35
United States of America	36
North American Treaty Organization (NATO) agencies	25

Request for visit process

For visits **Canada to Canada**

1. The **company security officer (CSO)** or **alternate company security officer (ACSO)** of the **Canadian visiting organization** must get approval from PSPC's Contract Security Program (CSP) by completing and submitting the **request for visit (RFV)** form.

2. PSPC's CSP verifies the facility security clearances, personal security clearances, the contract, project or program and all related security requirements.

3. If applicable, PSPC's CSP reviews documentary proof.

4. The visit is stamped, sent to the **authorized official of the visited site** for concurrence.

5. The **authorized official of the visited site** provides concurrence, signs and dates the **RFV** form, and forwards it back to PSPC's CSP.

6. PSPC's CSP updates, re-verifies and provides final approval stamp and returns **RFV** form to the **CSO/ACSO** or authorized official.

Request for visit process (cont’d)

For visits **Canada to foreign** and **Canada to United States (CUS)**

1. The **company security officer (CSO)** or **alternate company security officer (ACSO)** of the **Canadian visiting organization** must get approval from the **foreign government** through PSPC’s Contract Security Program (CSP) by completing and submitting the **request for visit (RFV)** form.
2. All **RFV** requests going from Canada to foreign or CUS **MUST** include valid contact information for the MILITARY point(s) of contact related to the project. Failure to include this information can cause significant delays, and may jeopardize the approval of the visit altogether.
3. PSPC’s CSP verifies the information provided on the **RFV** form and sends a validation to the foreign country for concurrence.
4. The **foreign authority** validates the request, may provide concurrence, and their response is routed back through the **International Industrial Security Directorate (IISD)**, who provide final confirmation to **CSO/ACSO** or authorized official.

Request for visit process (cont'd)

For visits **United States (US) to Canada** or **foreign to Canada**

1. The **security officer** of the **visiting organization** must get approval from their own country's **designated security authority (DSA)** by completing and submitting the **request for visit (RFV)** form.

2. The **visiting organization's** own **DSA** verifies the facility security clearances, personal security clearances, the contract, project or program and all related security requirements.

3. All **RFV** requests going from the US to Canada or foreign to Canada **MUST** include valid contact information for the MILITARY point(s) of contact related to the project. Failure to include this information can cause significant delays, and may jeopardize the approval of the visit altogether.

4. Once the **visiting organization's** own **DSA** validates the **RFV** form, a copy is sent to PSPC's Contract Security Program (CSP).

5. PSPC's CSP verifies the information provided on the **RFV** form and sends it to the visiting location for their site specific approval.

Webinars

- How to obtain a clearance with the Contract Security Program
- Completing a designated organization screening (DOS) application
- Completing a facility security clearance (FSC) application
- Handling and safeguarding
- Document safeguarding capability (DSC)
- Subcontracting
- Contracting outside of Canada
- Aftercare and security awareness

Request a copy of the recording:
SSIDSICSensibilisation.ISSCISDOutreach@tpsgc-pwgsc.gc.ca

Contact us

General inquiries

Phone

Toll-free: 1-866-368-4646

National capital region: 613-948-4176

Email

ssi-iss@tpsgc-pwgsc.gc.ca

Website

http://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html

Useful links

Contract security resources

http://www.tpsgc-pwgsc.gc.ca/esc-src/ressources-resources-eng.html

Organization and personnel security screening

http://www.tpsgc-pwgsc.gc.ca/esc-src/enquete-screening-eng.html

Subcontracting security requirements

https://www.tpsgc-pwgsc.gc.ca/esc-src/soustraitance-subcontracting-eng.html

Reporting security incidents and changes in circumstances and behaviors

https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/signalement-reporting-eng.html

Approval for visits to secure sites

https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/visite-visit-eng.html

News and updates about contract security

http://www.tpsgc-pwgsc.gc.ca/esc-src/nouvelles-news/index-eng.html

Contract Security Program roadmaps for Government of Canada suppliers

https://www.tpsgc-pwgsc.gc.ca/esc-src/ressources-resources/feuillederoute-roadmap-eng.html

Contract security training

https://www.tpsgc-pwgsc.gc.ca/esc-src/formation-training-eng.html

©Copyright

CLOSING REMARKS

Major Darrell Williams

Christine Picknell

Director Land Requirement, DND
Acquisitions Branch, PSPC

Transcript not available

Questions?

You may also forward your inquiries to the generic inbox at: **TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca**