IDEaS IDEeS
INNOVATION FOR DEFENCE EXCELLENCE AND SECURITY
INNOVATION POUR LA DÉFENSE, L'EXCELLENCE ET LA SÉCURITÉ

Innovation for Defence Excellence and Security (IDEaS) Program

Request for Information (RFI)

On behalf of Department of National Defence

Solicitation No: W7714-217834/A
GETS Reference No: PW-21-00945859
Closing date: Please refer to the RFI tender notice on BuyandSell.gc.ca.

Issuing Office:

Public Works and Government Services Canada
Services and Technology Acquisition Management Sector
Innovation Procurement Directorate
Les Terrasses de la Chaudière
10 Wellington Street
Gatineau, Quebec K1A 0S5
Email: TPSGC.PAIDEES-APIDEAS.PWGSC@tpsgc-pwgsc.gc.ca

TABLE OF CONTENTS

Part 1 – Introduction to the IDEaS' Classified Stream

1.1 Background

The Innovation for Defence Excellence and Security (IDEaS) program was announced in Canada's defence policy, *Strong, Secure, Engaged* and launched in 2018 to invest $1.6 billion over the next 20 years to access the expertise and solutions from the Canadian innovation ecosystem. The program provides Canadian innovators (from small to large enterprises, academia, non-for profit organisation, Universities, etc.) with a structure and support to encourage solutions for Canada's toughest defence and security challenges.

IDEaS supports the development of solutions from their conceptual stage, through prototype testing and capability development. The program's goal is to access new defence and security solutions from Canadian innovators for the benefit of the Department of National Defence (DND) and the Canadian Armed Forces (CAF). To date, more than $140M have been invested in solutions through the program.

1.2 Purpose of IDEaS' Classified Stream

DND/CAF recognizes that some of the largest and most challenging defence and security issues are classified in nature, and that defence technologies will increasingly be needed from sectors dealing with information and communication, cyber, and other emerging sensory and data processing technologies and software.

DND/CAF are seeking innovative science and technology (S&T) solutions to Canada's classified defence and security Challenges through a classified Call for Proposals. Classified challenges will have a Secret security designation. DND/CAF will support Challenges under the Classified Stream to increase the base of suppliers with classified capabilities to DND, and to address topics specifically linked to the mission of DND/CAF. The Classified Stream will enable the possibility to share secure information about classified Challenges so that tailored solutions may be proposed.

1.2.1 Terminology

This table outlines the terminology employed throughout this document.

Acronym	Definition
CAF	Canadian Armed Forces
CFP	Call for Proposal
CSL	Classified source list
DND	Department of National Defence
DRDC	Defence Research and Development Canada
IDEaS	Innovation for Defence Excellence and Security
ITQ	Invitation to Qualify
PWGSC	Public Works and Government Services Canada
R&D	Research and Development
RFI	Request for Information
S&T	Science and technology

Part 2 – Request for Information (RFI)

2.1 Purpose of this Request for Information (RFI)

Public Works and Government Services Canada (PWGSC) is issuing this Request for Information (RFI) on behalf of the DND IDEaS program, to seek industry feedback on the potential development of a classified stream Call for Proposals (CFP). For the purpose of this RFI, the term "feedback" is defined as any questions, comments, concerns, recommendations etc. submitted to the Contracting Authority.

2.2 Main Objectives of this RFI

The main objectives of this RFI are as follows:

1. Engage industry in order to provide them with an opportunity to review the proposed classified stream procurement strategy and assess which scenario best suits their needs;
2. Determine the current interest and capacity within the supplier community; and
3. Provide industry with an opportunity to respond to questions in an effort to help Canada create an effective path forward in the establishment of a classified stream CFP that meets industry's capability to deliver innovative solutions, and is inclusive of external and departmental objectives.

2.3 Nature of this RFI

Participation in this RFI is encouraged, but is not mandatory. Similarly, participation in this RFI is not required for the participation in any potential subsequent solicitation.

This RFI is neither a call for tender nor a Request for Proposal (RFP). No agreement or contract will be entered into based on this RFI, it is simply intended to solicit feedback from industry. Therefore, potential suppliers of any goods or services described in this RFI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this RFI.

There will be no supplier list created as a result of this RFI. Therefore, whether or not any potential supplier responds to this RFI will not preclude that supplier from participating in any future requirements. Also, the procurement of any of the goods or services described in this RFI will not necessarily follow this RFI. This RFI is simply intended to solicit feedback from industry with respect to its contents.

Nothing in this RFI shall be construed as a commitment from Canada to issue any subsequent solicitation. Canada may use any non-proprietary information obtained as part of this review or while preparing a future official solicitation document. Canada shall not be bound by anything stated in this document. Canada reserves the right to change at any time any or all parts of the requirement, as it deems necessary. Canada also reserves the right to revise its procurement approach, as it considers appropriate, either based on information submitted in response to this RFI or for any other reason it deems appropriate.

2.4 Responses

Because this is not a bid solicitation, Canada reserves the right to contact any respondents to follow up with additional questions or for clarification of any information provided in response to this RFI.

2.4.1 Format of Responses

Interested respondents are invited to review the questions found in Annex "A" and submit their responses using the PDF version of Annex "A" table provided as an attachment to this RFI, to the PWGSC Contracting Authority email address in Part 2.7 of this document, prior to the closing date and time of this RFI. Responses received after the closing date and time may not be reviewed.

Responses may be submitted in either official language of Canada.

Respondents are encouraged to clearly identify, in the information they share with Canada, any information that they feel is proprietary, commercial confidentiality, third party or contains personal information or sensitive information. Please note that Canada may be obligated by law (e.g. in response to a request under the Access to Information and Privacy Act) to consider disclosing proprietary or commercially-sensitive information provided by the respondent if not properly identified.

Canada will not reimburse any respondent for expenses incurred by participating in this RFI.

2.4.2 Use of Responses

Responses received will be reviewed and may be used by Canada to develop, refine, or modify the procurement process.

2.5 Government of Canada Applicable Policies

For the purpose of this R&D program, bidders must meet any program eligibility requirements including but not limited to the following for any follow-on solicitation(s) and/or subsequent contract(s) requirement.

2.5.1 Trade Agreements

Future requirement(s) related to this RFI will be subject to the Canadian Free Trade Agreement (CFTA).

2.5.2 Canadian Content

Future procurement(s) related to this RFI will be conditionally limited to Canadian goods and/or services.

SACC Manual clause A3050T (2020-07-01) Canadian Content Definition is amended as follows:

DELETE: 80 percent
INSERT: 50 percent

2.6 Enquiries

All enquiries related to this RFI must be directed exclusively to the Contracting Authority no later than 5 business days before the RFI closing date and time. Enquiries received after that time may not be answered.

2.7 Contracting Authority

The Contracting Authority for this RFI is:

Defence Sciences Division
Public Works and Government Services Canada
TPSGC.PAIDEES-APIDEAS.PWGSC@tpsgc-pwgsc.gc.ca

2.8 Closing date

Responses to this RFI must be submitted to the PWGSC Contracting Authority identified above, on or before the closing date indicated on buyandsell.gc.ca.

Part 3 – IDEaS Classified Stream Requirement

3.1 Procurement Framework

This section outlines the planned procurement process that Canada is considering in order to launch a classified stream CFP. Although the procurement process remains subject to change in accordance with PWGSC's Standard Instructions, Canada currently anticipates undertaking the multi-phase process described below.

This process would apply to any of the proposed classified stream CFP launch scenarios detailed in Part 3.2.

3.1.1 Invitation to Qualify (ITQ)

The ITQ would be published on Buyandsell.gc.ca (or Canadabuys.canada.ca) with the intent to pre-qualify suppliers to a Classified Source List (CSL) in accordance with the terms and conditions of the ITQ.

Multiple ITQs could be published as PWGSC/DND pre-qualifies suppliers for one or more additional classified domains. An ITQ refresh may also be published to update the list of pre-qualified suppliers on the CSL.

IDEaS may also pursue security clearance sponsorship of respondents that do not meet the security requirement of the ITQ to pre-qualify for participating in the classified CFP. Should IDEaS pursue security sponsorship, the process will be outlined within the ITQ. For more information on the Sponsorship process,respondents should refer to the Contract Security Program (https://www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/parrainage-sponsorship-eng.html)

It is anticipated that an ITQ will result in two groups of suppliers:

Group A: Suppliers who hold a valid security clearances. Group A suppliers will be placed on the CSL and will be invited to a subsequent classified stream CFP.

Group B: Suppliers without a valid security clearance and would require Canada's sponsorship. Canada may pursue security clearance sponsorship of Group B suppliers.

3.1.2 Classified Source List (CSL)

It is anticipated that the CSL will be the primary list of potential suppliers used for the IDEaS classified stream CFP. Once the CSL is established, PWGSC will use the CSL to invite suppliers to propose solutions to classified S&T Challenges.

It is anticipated that the CSL, which will be published on buyandsell.gc.ca (or Canadabuys.canada.ca), will be reviewed, updated and refreshed. PWGSC will be managing the CSL on behalf of DND/CAF.

Canada will notify pre-qualified suppliers on the CSL when the classified CFP is anticipated to launch. The classified stream CFP will be published on buyandsell.gc.ca (or Canadabuys.canada.ca) however individual solicitation processes done under the CSL such as classified Challenge statements and all requisite documents will only be shared with Group A suppliers on the CSL.

Canada will reserve the right to validate at any point in time if suppliers on the CSL are maintaining their security clearance. Any suppliers that fails to maintain their security clearance, will be removed from the CSL.

3.1.3 Classified Stream CFP

It is anticipated that a classified stream CFP will be launched to enable suppliers on the CSL to propose solutions to classified S&T Challenges in one or more of the domains detailed in Part 3.4. Government and departmental priorities, RFI feedback, as well as strategic considerations will assist IDEaS in determining which domains and subsequent Challenges will be further pursued at the CFP stage.

Suppliers will be required to sign agreements (related to non-disclosure) prior to receiving classified documents.Once completed, suppliers on the CSL, for the relevant domain(s) targeted by the challenge(s), will receive all requisite documents such as Challenge statements and solicitation documentation.

It is anticipated that IDEaS will use the feedback received in response to this RFI to determine which CFP launch scenario detailed in Part 3.2 to pursue.

The classified stream CFP is anticipated to largely mirror the continuum structure of the current unclassified IDEaS CFP. Please refer to the unclassified IDEaS Call for proposals 004 for additional information or visit the IDEaS website for additional information on the program.

3.1.4 Contract Award

It is anticipated that for the Classified Stream CFP the individual maximum contract funding for component 1a will be up to $400,000 CAD (excluding applicable taxes) for a maximum performance period of 8 months and individual maximum contract funding for component 1b will be up to $1.6M CAD (excluding applicable taxes) for a maximum performance period of 16 months

Multiple contracts may be awarded under each classified CFP, and one or more CFP may be issued each year.

3.2 CFP Launch Scenarios for Considerations

Based on the Procurement Framework identified in Part 3.1, the IDEaS Program has identified two potential scenarios for the CFP launch.

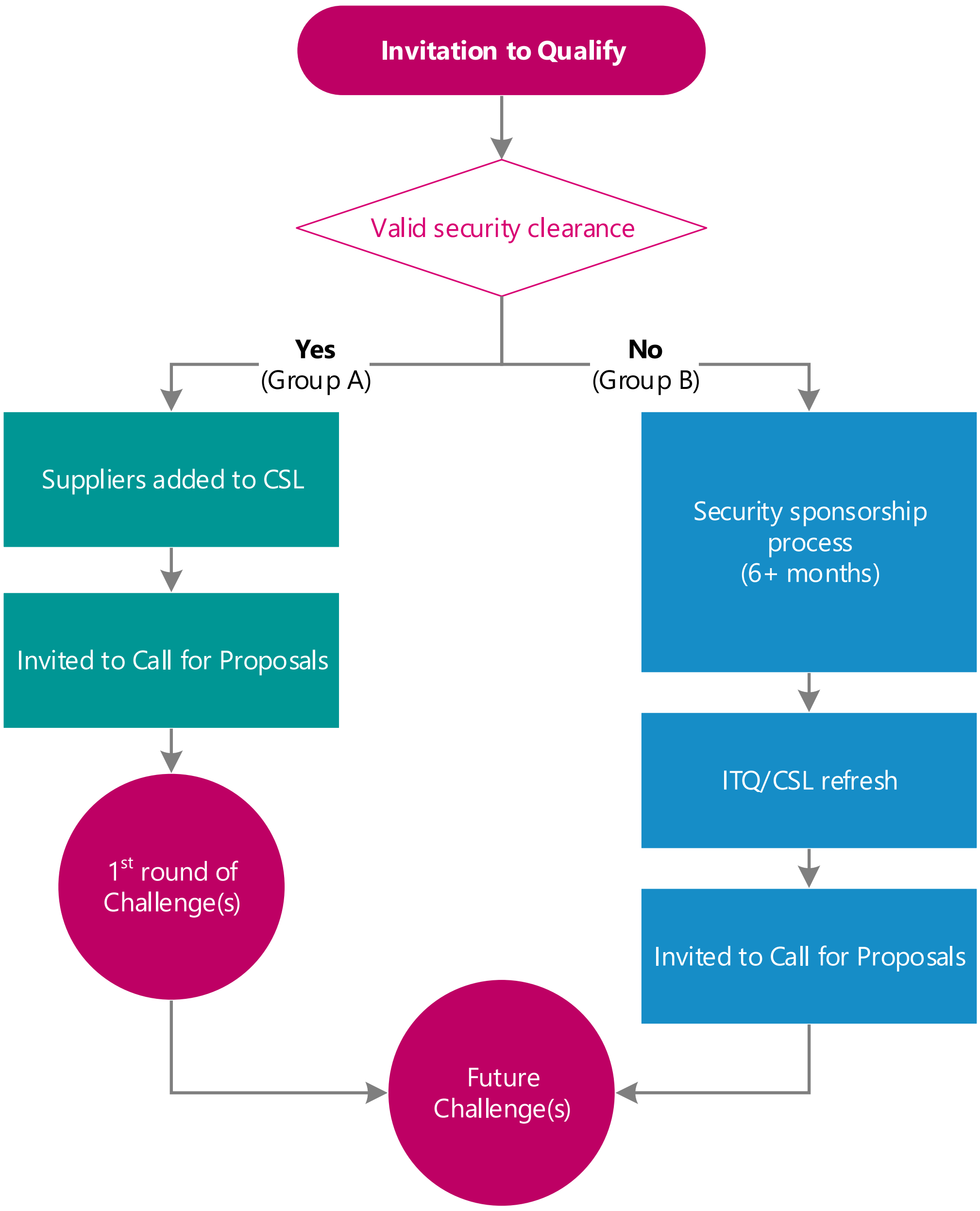
3.2.1 Scenario 1 - Rapid Launch

In this scenario, the ITQ would be published and used to establish one Group of pre-qualified suppliers for the CSL.

Group A, would be the pre-qualified suppliers on the CSL, and would be invited to participate in all future classified CFP and Challenges.

Group B, would be for suppliers who are seeking sponsorship to meet the ITQ requirement. Suppliers would get the opportunity to obtain the appropriate security clearance and be ready to apply to the next ITQ once Canada performs a CSL refresh.

The diagram below has been included for illustrative purposes of Scenario 1.


Invitation to Quality

3.2.2 Scenario 2 - Deferred Launch

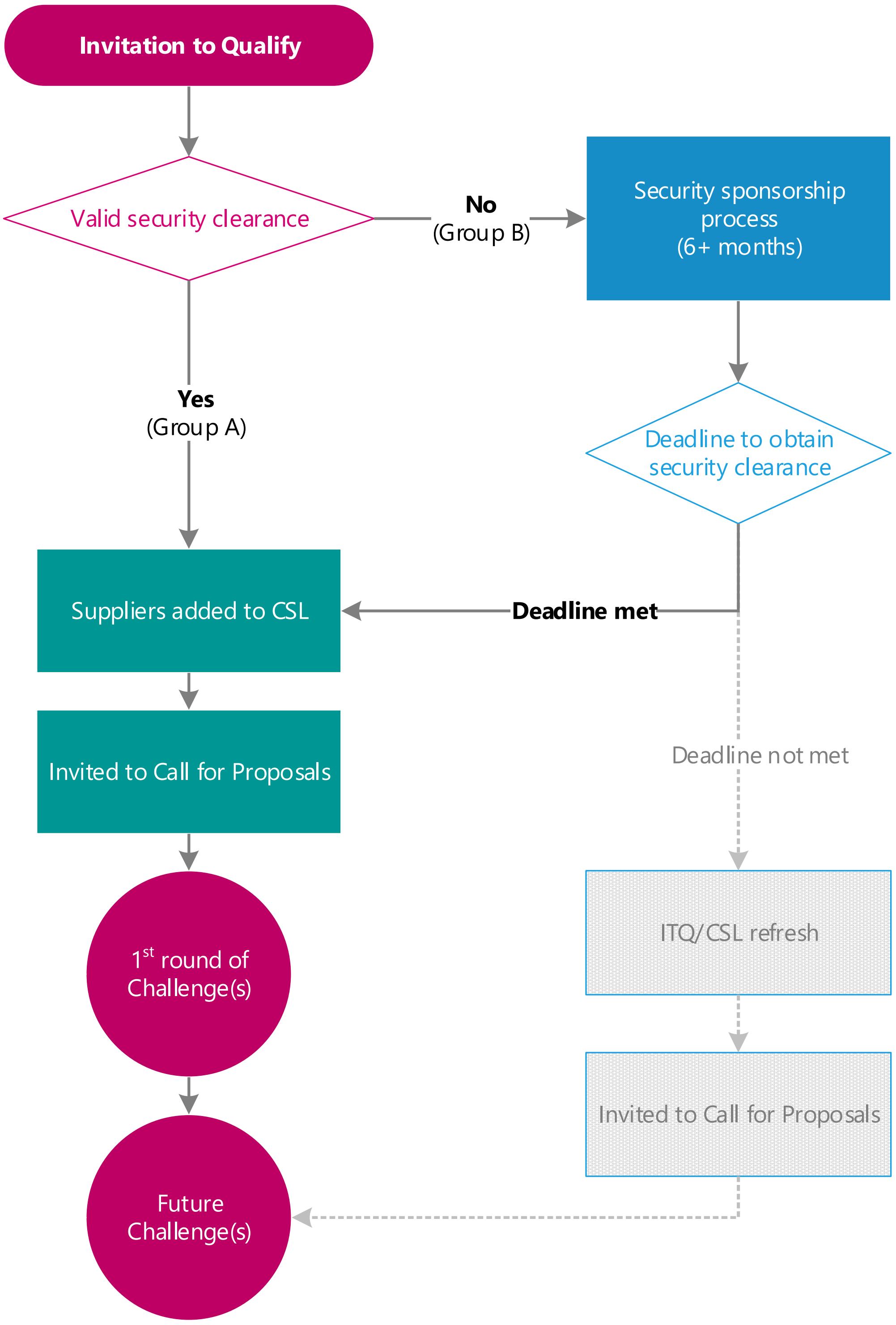
In this scenario, the ITQ would be published and used to establish two Groups of suppliers.

Group A, would be the pre-qualified suppliers on the CSL.

Group B, would be suppliers selected by DND/CAF to be sponsored. Suppliers would only be added to Group A of the CSL after appropriate security clearance has been received and validated by PSPC.

Note that Group B suppliers will be given a set deadline, identified in the ITQ, in which to meet the identified security requirement. When the deadline has expired, all suppliers listed on Group A of the CSL will be invited to participate in the pursuant classified CFP at the same time.

The diagram below has been included for illustrative purposes of Scenario 2.



3.3 Potential Security Requirements

The following security clearance level will be required in order to respond to the classified stream CFP:

- Secret

The estimated timeline for Group B bidders to receive a security clearance via the sponsorship process is approximately 6 months or more.

For more information on the personnel and organization security screening or security clauses, respondents should refer to the Contract Security Program of PWGSC (https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html)

3.4 Domains

The following S&T domains will be considered for the ITQ and classified CFP processes:

1. Underwater Warfare

This domain seeks to ensure that friendly forces establish and maintain control of the underwater environment by denying an opposing force the effective use of underwater systems and weapons. A primary focus is underwater situational awareness through the long range detection, classification, localization, tracking, and neutralization of underwater threats (submarines, torpedoes, and naval mines). This ensures the free movement of Royal Canadian Navy and civilian platforms underwater, the protection of sovereign water space, the approaches to Canada, and sea lines of communication.

2. Cloud-based Data Fusion and Automation

This is a broad category that involves innovative and modern digital technologies that will support the Defence Team, including: cognitive computing capabilities; cloud computing and mobile technologies; augmented and virtual reality systems; enhanced data analytics; data fusion automation, anomalous activity pattern detection, cybersecurity and Digital Twin technologies.

3. Space Sensor Payloads

These space based surveillance assets–significantly expand the Canadian Armed Forces' Joint Intelligence, Surveillance, and Reconnaissance (ISR) capacity. These assets may be used for sensing of the Earth (including ground, air, marine, and sub-marine environments) or Earth's orbital environment (including the immediate area around the spacecraft and/or areas thousands of km distant). Sensors are needed that can operate in various regions of the electromagnetic spectrum, may be passive or active in nature, used for real-time tracking of inbound threats and imaging or non-imaging applications, able to sense broad-band, narrow-band, or spectral signals, and provide data with high or low time resolution. These new platforms will be integrated with existing assets into a networked, joint system-of-systems that will enable the real-time flow of information that is so essential to operational success.

4. Counter Explosive Threat (CET)

This domain incorporates the collective efforts at all operational levels to defeat the explosive threat system by attacking the networks, defeating the device, and preparing the force to reduce or eliminate the effects of all forms of explosive threat for use against friendly forces and non-combatants. The intent of capability development in this challenge area is to maintain freedom of maneuver at the operational level in the presence of explosive threats in order to enable mission objectives, while increasing solider safety through improved abilities to predict, detect, neutralize, and exploit explosive threats. While improvements to current capabilities would be welcomed, the vision is to improve mounted and dismounted CET through the exploitation of anticipated future uninhabited ground vehicle (UGV) and uninhabited aerial vehicle (UAV) platforms, fusing inputs from a heterogeneous suite of stand-off or remote sensors in order to provide high-level decision support to the commander, as well to provide options for subsequent rapid, stand-off or remote neutralization. Classified aspects of this challenge area pertain to current capability deficiencies, and/or the specific design and operational descriptions of extant and emergent threats.

5. Defeating Radio Controlled Improvised Explosive Devices (RC-IED)

Technologies and algorithms that provide transformational enhancements to the ability of Force Protection Electronic Countermeasures (FPECM) to defeat Radio Controlled Improvised Explosive Devices (RCIED). This could include methodologies, including autonomous approaches, for rapid development and deployment of countermeasures for new and emerging threats, new technologies enabling practical simultaneous countermeasures and sensing, and other enhancements that would support a new generation of improved and effective FPECM systems.

6. Counter-Uninhabited Aerial Systems (C-UAS)

Approaches and systems for countering UAS that are capable of detecting, tracking, identifying, and/or neutralizing the UAS from as far away from the device as possible, and able to perform these functions from either fixed installations or in a moving vehicle. The Canadian Armed Forces needs systems which can deploy easily and readily, and automate these tasks to the extent possible (to minimize training, user input and level of effort in performing these functions).

7. Soldier Systems Integration

The Canadian Armed Forces' dismounted soldiers must be able to operate in a complex and dynamic environment and in the face of an opposing force that is employing state-of-the art technology. They require high performance, lighter weight protection systems to mitigate current and emerging battlefield threats with increased mobility and reduced physiological burden. They must employ signature management solutions that reduce detectability and allow freedom of maneuver in the face of new sensor technologies and platforms. CAF dismounted soldiers also require advanced sensing technologies and network enabled systems that enhance situational awareness, leverage multiple data sources and inform and accelerate decision making while mitigating cognitive workload. And they require advanced weapon systems that deliver lethal and non-lethal effects while increasing speed and accuracy of target engagement at longer ranges and with a lighter system weight. In all cases, soldier borne systems must minimize soldier born cognitive and physical load, be robust and adapted to the realities of the battlefield and operational employment, address current and emerging threats, and be easy to use to minimize training requirements and maximize effectiveness.

Annex "A" – Request for Information (RFI) Questions for Industry

Interested respondents are invited to review the questions below and submit their responses by using the fillable PDF version of Annex A provided as an attachment to this RFI on BuyandSell.

Questions	
RFI and Procurement Framework	
Q1	Is the information described in Part 3 of the RFI clear and reasonable? *Factors to consider: understanding the key steps of the process, the procurement framework, the difference in the proposed CFP launch scenarios, understanding how to participate, etc.*
A1	
Q2	Would you consider applying to the Invitation to Qualify (ITQ) as described in the RFI? Please explain what would make your organization want to apply (or not) and why?
A2	
Q3	Is there information you feel should be brought to Canada's attention that hasn't been mentioned in the proposed framework? Are there any show stoppers, for you as an organization, which you would like to identify to Canada?
A3	
Scenario 1 – Rapid Launch (refer to Part 3.2)	
Q4	Is this scenario feasible for your organization?
A4	
Q5	What would make this scenario desirable?
A5	
Q6	What are any issues, if applicable, that you foresee with this scenario?
A6	
Q7	Are there modifications you would like to propose to make this scenario align with your business operations?
A7	
Q8	In your opinion, would this scenario fit the purpose of the classified stream listed in Part 1.2 of the RFI?
A8	
Scenario 2 – Deferred Launch (refer to Part 3.2)	
Q9	Is this scenario feasible for your organization?
A9	
Q10	What would make this scenario desirable?
A10	
Q11	What are any issues, if applicable, that you foresee with this scenario?
A11	
Q12	Are there modifications you would like to propose to make this scenario align with your business operations?
A12	

Q13	In your opinion, would this scenario fit the purpose of the classified stream listed in Part 1.2 of the RFI?
A13	
Other	
Q14	If the IDEaS program pursues any of the proposed CFP launch scenarios, are there concerns around favoring one set of innovators over others? If so, are there modifications you would like to propose to mitigate this?
A14	
Q15	Do you have another potential CFP launch scenario to propose to resolve the issues you identified to the question above?
A15	
Organization and Security	
Q16	Please identify the size of your organization from the following :
A16	1. Small Business (1 to 99 employees) 2. Medium Business (100 to 499 employees) 3. Large Business (500 employees or more) 4. Other *(please describe)*
Q17	Please identify your type of organization from the following:
A17	1. Academia 2. For profit 3. Not-for-Profit organization 4. Association 5. Other *(please describe)*
Q18	Please identify which of the following PWGSC security clearances are already held by your organization:
A18	1. Personnel 2. Organization 3. Facility (document safeguarding) 4. None of the above
Q19	Has your organization worked for the public sector where your organization was required to meet security requirements under contracts of a classified nature? If so, please specify which Canadian federal safety or security department(s) or any other federal department(s).
A19	
Domains (refer to Part 3.4)	
Q20	Which domain(s) could your organization provide solutions for? Please identify all domains where your organization has capacity to develop solutions.
A20	1. Under water warfare 2. Cloud-based data fusion and automation 3. Space sensor payloads 4. Counter Explosive Threat (CET) 5. Defeating Radio Controlled Improvised Explosive Devices (RC-IED)

	6. Counter-Uninhabited Aerial Systems (C-UAS) 7. Soldier Systems Integration
Q21	From the domains identified in Question 20, please identify and rank your top 5 domains, in order of preference, from 1 to 5 (1 being most preferred).
A21	1. 2. 3. 4. 5.
Q22	Under the domain(s) for which your organization could provide solutions, how would you qualify your level of expertise, and experience (e.g., examples of experience, projects, number of years).
A22	