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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Comments - Commentaires

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

Issuing Office - Bureau de distribution

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

Title - Sujet LOI - ICAM	
Solicitation No. - N° de l'invitation W8474-19AM01/A	**Date** 2018-11-06
Client Reference No. - N° de référence du client W8474-19AM01	**GETS Ref. No. - N° de réf. de SEAG** PW-$$QE-063-27048
File No. - N° de dossier 063qe.W8474-19AM01	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à** 02:00 PM **on - le** 2018-12-17	**Time Zone** **Fuseau horaire** Eastern Standard Time EST
F.O.B. - F.A.B. **Plant-Usine:** □ **Destination:** □ **Other-Autre:** □	
Address Enquiries to: - Adresser toutes questions à: Norris, Chantale	**Buyer Id - Id de l'acheteur** 063qe
Telephone No. - N° de téléphone (819) 420-1758 ( )	**FAX No. - N° de FAX** (819) 956-6907
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** Specified Herein Précisé dans les présentes	

Instructions: See Herein

Instructions: Voir aux présentes

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

Canada

Identity Credential and Access Management

Letter of Interest

Table of Contents

PURPOSE AND CONTENTS OF THIS LETTER OF INTEREST

This is the Letter of Interest (LOI) pertaining to the Identity Credential and Access Management (ICAM) Project for the Department of National Defence (DND) and the Canadian Armed Forces (CAF). The purpose of this LOI is to inform and prepare industry for potential procurement opportunities concerning the ICAM Project and seek input and contribution regarding the project’s scope, requirements, schedule and risks. The general contents of this LOI document are:

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

PART II: ICAM Solution

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

ANNEX A: ICAM Project Background

PART I: LETTER OF INTEREST PROCESS

1. INTRODUCTION

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

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

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

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

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

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

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

1.1 Nature of this Letter of Interest

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

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

2. INSTRUCTIONS FOR RESPONDING TO THIS LETTER OF INTEREST

2.1 Nature and Format of Responses Requested

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

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

2.2 Response Costs

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

2.3 Treatment of Responses

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

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

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

2.4 Communication with Industry

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

2.5 Contents of the LOI

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

2.6 Format of Responses

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

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

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

ii. The name and address of the respondent;

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

iv. The date; and

v. The LOI number.

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

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

2.7 Enquiries

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

Contracting Authority: Chantale Norris

Public Services and Procurement Canada
Place du Portage III, 8C2
11 Laurier Street
Gatineau, Quebec K1A 0S5
819-420-1758
Email address: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Please insert “ICAM LOI” in the subject line. Failure to do so may result in delays receiving a response.

The use of email is the preferred method of communication.

2.8 Submission of Responses

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

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

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

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

PART II: ICAM SOLUTION

1. ICAM PROJECT BACKGROUND

Access controls within the Department of National Defence (DND) and between DND and its domestic and international partners are complex and subject to risk from internal and external threats.

The proliferation of identity and credential information across DND needs to be rationalized to reduce information loss, damage and/or compromise.

Rationalized ICAM processes are needed to make users more productive, assets more secure, decisions more transparent and actions more auditable. More specifically, modernizing ICAM will:

- give people visibility of their personal identity information and allow them to update their own profiles;
- mitigate cyber threats; and
- support forensic investigations of access breaches.

In short, DND/CAF needs to modernize and improve the interoperability, promptness, accuracy and privacy of its identity data and credentials and of its access controls to physical facilities, information and information systems. This includes improved interoperability between DND/CAF and partners from OGDA, Allies and the private sector.

2. OBJECTIVE OF THIS LOI

This LOI is being issued with the objective of:

a. consulting industry to better understand available and emerging commercial ICAM infrastructure and service solutions;

b. seeking information to assist the DND/CAF in developing their requirement and assist in the internal planning and approval process that may potentially lead to a solicitation; and

c. seeking information to assist the DND/CAF in potentially grouping some of the deliverables, so that a vendor or team of vendors can provide an integrated solution for a coherent sub-grouping of deliverables.

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

3. SECURITY REQUIREMENTS

There are no security requirements associated with this LOI.

Any future procurement actions undertaken in support of the ICAM Solution may require suppliers to hold a Level II (Secret) clearance issued by their respective national security agency. Some of the suppliers may also need to meet GC requirements for providing products and services with (classified) Canadian Eyes Only (CEO) restrictions.

3.1 PRIVACY

Canada has an obligation to ensure that Canadian statutes, regulations, and policies on privacy protection are respected. Should personal information be involved in any resulting contract, Canada may request that suppliers are in compliance with the protection of personal information in accordance with the *Privacy Act*, R.S. 1985, c. P-21, the *Personal Information Protection and Electronic Documents Act*,2000, c. 5, and federal privacy policy instruments.

4. NATIONAL SECURITY EXCEPTION

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

5. INDUSTRIAL AND TECHNOLOGICAL BENEFITS (ITB) POLICY

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

The Industrial and Technological Benefits Policy (ITB) may be applied on the Identity Credential and Access Management (ICAM) project. Engagement with industry through the Letter of Interest (LOI) will help determine the application of the ITB Policy and how Canada could leverage opportunities for economic benefit through this procurement.

5.2 The ITB Policy including Value Proposition

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

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

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

5.2.1 Key Industrial Capabilities:

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

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

The definitions for the relevant KICs for this project are:

Cyber Resilience
Cyber resilience spans every element of the domestic commercial, civil and national security sectors and addresses the vulnerabilities created by the expansion of information technology and the knowledge economy. Activities in this segment include design, integration and implementation of solutions that secure information and communications networks. These and

other technologies should focus on achieving effective development of the following cyber capabilities:

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

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

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

6. OFFICIAL LANGUAGES

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

7. ENGAGEMENT APPROACH

7.1 Industry Engagement

The industry engagement process begins with this LOI and will conclude when an official Request for Information, RFP or other competitive process is distributed to suppliers. It is envisaged that a more detailed RFI and an industry day will follow the LOI process, responses to the LOI will assist in developing the RFI.

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

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

PART III: QUESTIONS TO INDUSTRY

1. QUESTIONS TO INDUSTRY

1.1. Areas of Interest

1.1.1 What solutions does your company provide that could help DND realize the capabilities presented in the ICAM conceptual architecture described in Annex A?

1.1.2 Which role would your company potentially look to fill? (e.g. Prime System Integrator, Sub-System Integrator or Product Supplier)

1.2. Governance

What could you offer to DND in the area of establishing or improving ICAM governance, policy, standards, guidelines and processes? What experience does your company have in these areas?

1.3. Experience Supporting Military Requirements

1.3.1 Has your company worked on delivering military requirements before?
1.3.2 What experience does your company have delivering or supporting network capabilities in a military context?
1.3.3 What experience does your company have supporting facility access in a military context?
1.3.4 Has your company had experience with the DND Security Accreditation and Authorization (SA&A) process?

1.4. Experience Delivering ICAM Solutions

1.4.1 What experience does your company have in delivering ICAM solutions? Could you summarize the solutions provided?
1.4.2 What experience does your company have in dealing with “Dirty Data” and could you summarize your recommended approach to data cleansing? [Dirty data, also known as rogue data, are inaccurate, incomplete or inconsistent data, especially in a computer system or database. Dirty data can contain such mistakes as spelling or punctuation errors, incorrect data associated with a field, incomplete or outdated data, or even data that has been duplicated in the database. They can be cleaned through a process known as data cleansing].

1.5. Experience Integrating ICAM Solutions across Large Enterprises

What experience does your company have in integrating ICAM solutions across a large enterprise? Could you summarize the integration provided?

1.6. Experience Delivering Automated ICAM Solutions

What experience does your company have in developing and deploying solutions to support the automation of ICAM functions? Could you summarize your experience in the following processes:

1.6.1. Automated:
- 1.6.1.1. provisioning;
- 1.6.1.2. de-provisioning;
- 1.6.1.3. self-service user profile management;
- 1.6.1.4. automated detection of anomalies;
- 1.6.1.5. automated authorization workflows; and
- 1.6.1.6. any other relevant examples.

1.7. Experience Delivering ICAM Solutions across Domains and Network Security Levels

The CAF and DND currently have numerous information and security domains spanning multiple organizational levels (strategic, operational and tactical) as well as security classifications (Top Secret, Secret, Confidential, Protected). Summarize your experience providing ICAM solutions in multi-domain/security environments?

1.8. ICAM Intelligence

What ICAM intelligence solutions can your company provide that could help the department mitigate cyber security threats? Areas of intelligence which DND is interested includes:

1.8.1. Real-time monitoring of user access permissions;
1.8.2. Real-time monitoring of requirement for a user to have access;
1.8.3. Identification of orphaned accounts including how many are active, how many are inactive, when were they used and what did they access; and
1.8.4. Identification of what access is normal vs suspicious.

1.9. Risk

1.9.1. In your experience, what risks were considered when implementing your solution?

1.9.2 What was your solution for mitigating these risks?

1.10. Security & Privacy

1.10.1 Security of information and privacy by design are a priority for DND/CAF. What approach or design has your company taken to ensure the security of information processed by your solution and how does it enable privacy of an individual’s information?

1.10.2 Key to the implementation of a DND ICAM solution is the ability to support varying levels of identity and credential assurance. What experience does your company have implementing business processes and services that support enterprise identity and credential assurance up to and including level four?

1.11. Interoperability

1.11.1 DND/CAF have numerous systems, services, domains, applications and partners, some of whom have differing interoperability requirements. What approach would you take to ensuring ICAM solutions work between DND/CAF and Other Government Departments and Agencies (OGDA) and multinational partners, including requirements for interoperability between current and future ICAM solutions?

1.11.2 Is federation of ICAM services between partners a viable solution?

1.11.3 With which ICAM related interoperability standards (if any) is your solution compliant?

1.12. Recommended Delivery Approach

1.12.1 Based on previous experience implementing ICAM solutions, what approach would you take to delivering ICAM solutions to the DND/CAF environment (e.g. greenfielding, COTS vs. custom build on top of existing systems, delivery of all or some ICAM functions “as a service,” another approach or combination of approaches)?

1.12.2 Why do you propose such an approach?

1.13 Recommended questions to ask in an RFI

While taking into account your ICAM experience, what types of questions would you suggest are asked in the RFI and what additional information would you expect to see in order to better articulate your responses on possible solutions and associated costs?

1.14 ICAM ITB and VP Industry Engagement Questions

Defence Sector

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

1.14.1 Based on the high level mandatory requirements proposed by the Department of National Defence, describe what Direct Work activities your company would foresee undertaking in Canada for the production and the maintenance of the ICAM. As part of your response, please highlight what Direct Work activities your company would foresee performing in Canada in the KIC Cyber Resilience.

Supplier Development

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

1.14.2 As a result of the ICAM project, please indicate what new supply chain opportunities could be made available to Canadian suppliers and what opportunities you foresee that could be specifically targeted at Canadian SMBs (less than 250 employees in Canada). Please include in your response information on:

a. Which activities should be perceived as providing the highest value to Canada and how these activities could impact Canadian suppliers.
b. Supplier development opportunities that could be performed in the KIC Cyber Resilience, directly or indirectly related to the ICAM project.

1.14.3 The ITB Policy requires at least 15 percent of the value of the contract to be work with Canadian SMBs. Please describe the challenges and opportunities that you foresee if Canada motivates higher levels of SMB participation through a rated requirement.

Skills Development and Training:

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

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

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

1.14.5 Please describe the Skills Development and Training activities your company currently undertakes, and how your company could extend these activities to Canadians. As part of your response, please highlight any Skills Development and Training activities that are currently linked or could be linked in future to the KIC Cyber Resilience.

Research and Development (R&D)

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

1.14.6 Please describe your company's priority areas for R&D investment and how they relate to the ICAM project. As part of your response, please explain to what extent these priority areas align with the KIC Cyber Resilience.

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

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

Export:

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

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

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

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

Other Questions:

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

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

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

Please provide your written feedback to these questions and any other comments regarding Industrial and Technological Benefits/Value Proposition to the PSPC Contracting Authority by the LOI deadline.

ANNEX A: ICAM CAPABILITY AND PROJECT

1. INTRODUCTION

1.2. The ICAM project will deliver a capability to increase accessibility across and between organizations, mitigate security risks to facilities, information and Information Technologies and alleviate constraints on productivity caused by problems with access controls within the Department of National Defence (DND), with Other Government Departments and Agencies and with multinational partners, including the United States, NATO and Five Eyes.

1.3. The new approach to ICAM in the Department will protect assets, streamline users' ability to access resources, improve decision making related to the granting and revoking of access-entitlements and decrease the risk of loss, damage and compromise to Departmental assets.

2. ICAM BUSINESS DRIVERS

2.1. Government Drivers. The features of the DND ICAM capability are guided by Canadian legislative directions, which require (1) Government of Canada information and Information Technology assets to be secure and (2) privacy of Personally Identifiable Information to be protected and controlled.[1] To align the ICAM capability with legislation, DND will use the Defence Information Technology Security Strategy[2], which outlines elements of an integrated security environment, including enforcement of security policy, authentication, access control, reporting, and auditing.

2.2. Technology. Technological advances have made ICAM capabilities more effective. ICAM will be able to leverage technologies such as biometrics, block-chain technology, multi factor authentication, tokenization and modern cryptography to strengthen authentication and authorization, and enable Attribute Based Access Control of both physical and electronic information assets.

2.3. Cyber threat. Emerging technologies have enabled broader and easier access to information. Coupled with increasingly persistent and sophisticated criminal, intelligence, and military threats, these new technologies have increased the risk of unauthorized access to electronic information and physical assets.

2.4. Efficiency. Over time DND has increasingly leveraged Information Technology as a business enabler. Initially, systems, networks, applications and associated user repositories were deployed independently primarily due to security or technical constraints at the time the system was implemented. The Information Technology Infrastructure has evolved to where convergence and interoperability of systems and environments is needed for the CAF/DND to be operationally effective. Existing siloed systems can leverage a common ICAM capability to enable this Information Technology Infrastructure convergence strategy.

The Department is looking at ICAM to improve efficiency in the following ways:

2.4..1. Adopting standards for identity data;

2.4..2. Leveraging emerging technologies such as biometrics;

2.4..3. Streamlining current manual business processes through automation; and

2.4..4. Improve user experience and minimize number of access accounts.

[1] Privacy Regulations SOR/83-508 http://laws-lois.justice.gc.ca/eng/regulations/SOR-83-508/page-1.html#h-3

[2] Defence Information Technology Security Strategy, 8 June 2010 http://admim-smagi.mil.ca/en/about/governance/key-documents.page

2.5. Privacy. ICAM will support privacy and confidentiality of information.

3. CAPABILITY DESCRIPTION

3.1. The ICAM project will look at Department-wide solutions for provisioning, management, and de-provisioning of accounts and access entitlements on networks, applications, Information Technology services and facility control systems.

3.2. The Department is considering a conceptual ICAM architecture as shown in Figure 1. Note that this architecture includes; identity management, credential management, access management, reporting, auditing and federation[3].

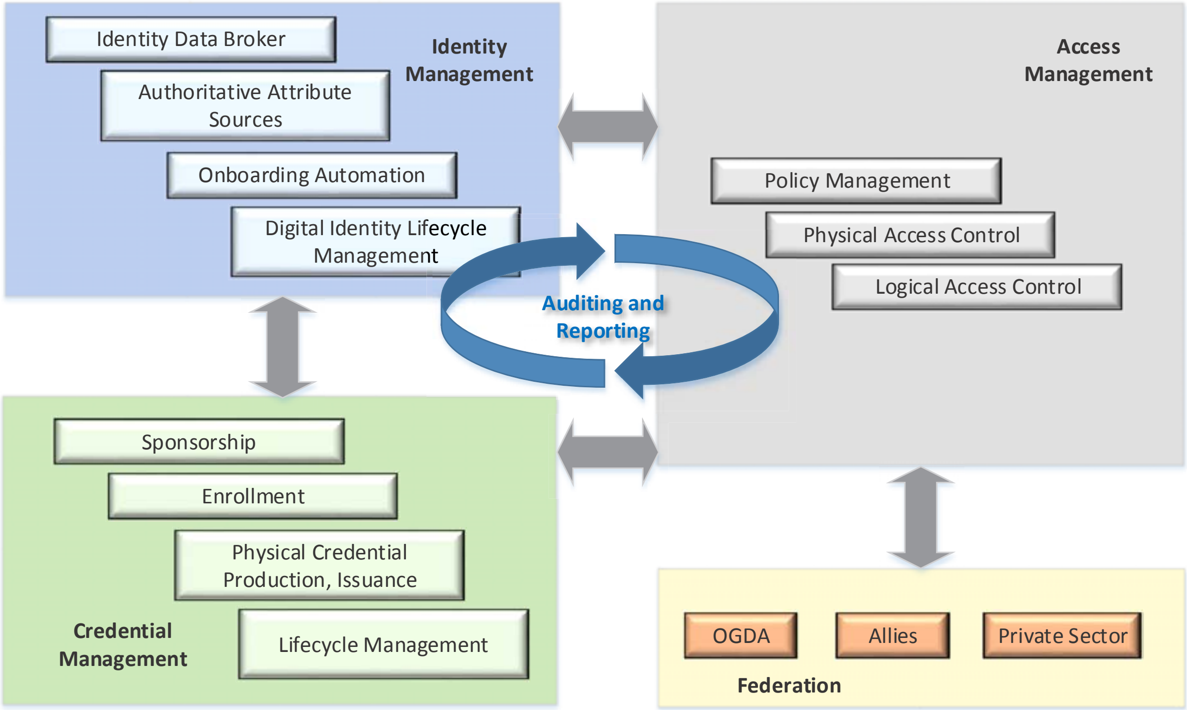

Figure 1: DND conceptual ICAM architecture

4. Project Description

4.1. A DND ICAM project has been established and approved. The project will deliver ICAM capabilities, including organizational structure, governance, material, infrastructure and training required to increase the Department's ability to manage identities, credentials and access controls in a coordinated manner.

4.2. The project currently is in the Options Analysis phase within which capability delivery options will be considered. Options analysis will consider effectiveness, cost, timeliness and technical feasibility. At

[3] In information technology, federated identity management amounts to having a common set of policies, practices and protocols in place to manage the identity and trust into Information Technology users and devices across organizations.

the end of this phase the project team will prepare a detailed Business Case, which will be submitted to the Defence Capability Board to help them make a decision whether to continue the project and proceed to the Project Definition phase. The project is expected to deliver in the 2022 to 2027 timeframe.

5. IMPLEMENTATION OPTIONS BEING CONSIDERED

5.1. The following options are currently being considered and the feedback to these options would be useful.

- Enhancing existing ICAM systems, by layering on governance, business processes and some technical integration to existing systems;

- Deliver new centralized ICAM services, featuring an identity repository that contains or connects to authoritative sources of identity information used in the Department; and

- Building on option 2, create an Identity Services Broker (ISB) that mediates the exchange of identity information between distributed identity repositories, credential issuing systems, access control systems and individual users.