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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
RFI- ICAM

Solicitation No. - N° de l'invitation	Date
W8474-19AM01/B	2019-07-05
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
W8474-19AM01	PW-$$QE-063-27387
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
063qe.W8474-19AM01	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2021-07-02

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

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

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Norris, Chantale	063qe
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(819) 420-1758 ( )	(819) 956-6907

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

Specified Herein
Précisé dans les présentes

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

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

Signature **Date**

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

Canada

Table of Contents

PART I – INTRODUCTION

Background

The Department of National Defence (DND) has established the Identity, Credential and Access Management (ICAM) project to deliver centralized identity, credential and access management services to the Department.

Currently, DND identity, credential and access controls are heavily compartmentalized, lacking central management, monitoring and control. Complicating the current state are external threats enabled by exposure of DND unclassified networks to the public internet. The existing situation is complex and unsustainable and it exposes Departmental operations to a high level of information security risk.

Purpose of this RFI

Public Services and Procurement Canada (PSPC), on behalf of the DND/CAF, is releasing this Request for Information (RFI) to inform Industry and to seek input on the possible procurement and related costing for the ICAM Project. This RFI will be continually amended to advise industry, on an on-going basis, of industry engagement activities and resulting feedback. To facilitate this process it is Canada's intention to keep the RFI open until such time as a final Request for Proposal (RFP) is released; however, responses to the RFI are requested by the date listed in Table 1 – Procurement / Engagement Activities and Related Dates.

The RFI and engagement process provides Industry with the opportunity to present their capabilities and considerations regarding Canada's requirements for the ICAM Project. Canada may use the information gathered to assist in the development of an RFP. The intent is to actively engage and consult Industry throughout the procurement process to ensure a successful project end-state.

Proposed Engagement and Procurement Process

The proposed engagement and procurement process for this project is explained in greater detail in Part 1 of this RFI and consists of a multi-phased approach as detailed below. Please be advised the proposed procurement activities beyond this initial RFI are for discussion only and may be amended at any time. The decision to conduct any further procurement activities has not been taken.

<u>Phase 1</u>

Letter of Interest: A Letter of Interest (LOI) for this project was issued on 7 November 2018 and closed 17 December 2018, under Buyandsell.gc.ca solicitation number W8474-19AM01/A. A total of thirteen companies responded to the LOI. The results of the LOI indicated the need for a more detailed Request for information (RFI).

Request for Information: An RFI will provide more detailed information to industry and will act as a continuous single point of official project communication. Chiefly it will solicit detailed industry feedback on operational and technical requirements, cost and schedule.

Unclassified Industry Day: To present an overview of the requirements and engagement process.

Unclassified One-on-One Meetings: One-on-one meetings will be held to discuss the RFI.

<u>Phase 2</u>

Request for Information: The RFI issued in Phase 1 will remain open until the draft RFP stage in order to enable suppliers to obtain the necessary security clearances.

Draft Request for Proposal: A draft RFP for the project may be released to suppliers meeting the security requirements for their review and input. The draft RFP may have one or more classified annexes.

Phase 3

Request for Proposal: A formal Request for Proposal for the project may be issued. The RFP will have one or more classified annexes. Only suppliers meeting the security requirements will have access to the classified components of any Draft RFP(s).

Evaluation: Bids will be evaluated in accordance with the terms of the RFP.

Phase 4

Contract Award: A single or multiple contract(s) may be awarded to the winning bidder(s) in accordance with the security requirements and the terms of the RFP.

Procurement Timeline

Canada is at the preliminary stage of a potential procurement process, however it is Canada's intention that the engagement and procurement activities follow the timeline below. Suppliers are advised to note the dates for information requested by Canada and are asked to submit the information requested on or before that date.

Table 1 - Procurement / Engagement Activity and Related Dates

Procurement / Engagement Activity		Date
Security Clearance Sponsorship*		From RFI release to RFP release
Phase 1	LOI	Completed 17 December 2019
	RFI	5 July 2019 to RFP release date
	• Registration deadline to attend Industry Day,	15 July 2019
	• Registration deadline to attend One-on-One Meetings	15 July 2019
	• Unclassified Industry Day	22 July 2019
	• Unclassified One-on-one Meetings	22 – 24 July 2019
	• RFI Response Date	30 August 2019
Phase 2	Draft RFP	Fall 2021
Phase 3	RFP	Summer 2022
	Evaluation	Summer/Fall 2022
Phase 4	Contract Award	Summer/Fall 2023

*The security requirements for the project are described in section 3 of this document.

PART II – REQUEST FOR INFORMATION

1. Instructions for Responding to this Request for Information

1.1. Nature of the Request for Information

Respondents are reminded that this is an RFI and not an RFP. As such, respondents are requested to provide their comments, concerns and recommendations regarding how the requirements or objectives described in this RFI 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 be gained from responses, Canada requests that respondents follow the structure outlined in the Format of Responses.

Whether or not any potential supplier responds to this RFI will not preclude that supplier from participating in any future procurement. Also, the procurement of any of the goods and services described in this RFI will not necessarily follow this RFI.

1.2. Response Costs

Canada will not reimburse any organization for expenses incurred in responding to this RFI, including, but not limited to, expenses incurred for participating in the additional engagement activities or security sponsorship process.

1.3. Treatment of Responses

Use of Responses: Responses will not be evaluated. However, the responses received may be used by Canada to develop or modify the procurement approach. Canada will review all responses received. Canada may, at its discretion, review responses received after the RFI Response Request Date.

Review Team: A review team composed of representatives of DND and 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. Responses will be handled in accordance with the provisions of various legislations including the *Access to Information Act* (R.S. 1985, c. A-1) the *Privacy Act* (R.S., 1985, c. P-21), and the Defence Production Act (R.S. 1985, c. D-1).

Clarifications: Canada may, at its discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response or for one-on-one meetings.

1.4. National Security Exception

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 requirement.

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 NSE.

1.5. Nature and Format of Responses Requested

Respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements described in the RFI could be satisfied. Respondents are also invited to provide comments regarding the content, format and/or organization of any draft documents included in this RFI. Respondents should list and explain any assumptions that they make in their responses.

1.6. Contents of the RFI

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. Nor should respondents assume that none of the requirements will be deleted or revised. Comments regarding any aspect of the requirement are welcome. This RFI also contains specific questions addressed to industry.

1.7. Solicitation Caveat

This RFI 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 RFI.

1.8. Format of Responses

Industry is invited to respond to this RFI and provide the following information no later than the specified response request date. Respondents are asked to consider the following in preparing their response:

- **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 solicitation 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:
  1) the title of the respondent's response and the volume number;
  2) the name and address of the respondent;
  3) the name, address and telephone number of the respondent's contact;
  4) the date, and
  5) the RFI's Solicitation Number.

- **General Layout and File Format:** Respondents may use the written format of their choice, but should use the Product Offerings and Pricing Information Response Template provided at Annex C and keep the same section numbering to facilitate Canada's review and analysis of all responses. Responses should be provided electronically in MS Word, MS Excel, and/or PDF format. The layout of the submission is requested as follows:
  1) Section 1: Executive Summary – 1 to 2 pages, up to a maximum of 2 pages, summarizing the submission in total,
  2) Section 2: Corporate Profile, up to a maximum of 2 pages;
  3) Section 3: Proposed Concept of Solution, up to a maximum of 7 pages (not including costing tables from Annex C); and
  4) Section 4: General Comments and Advice, up to a maximum of 20 pages;

- **Number of Copies:** Canada requests that respondents submit a copy of their response in unprotected (i.e. no password) MS Word, MS Excel, and/or PDF format by email, if the size of the document is less than 5MB, to: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Alternatively, Canada requests that respondents save a copy of their PDF (2003 or later) document onto each of four USB memory drives and mail them to the contracting authority identified herein at section 1.9.

1.9 Enquiries

All enquiries and other communications related to this RFI shall be directed exclusively to the PSPC Contracting Authority. Since this is not a bid solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all respondents; however, respondents with questions regarding this RFI may direct their enquiries to: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

Or if by mail:

Public Services and Procurement Canada
Place du Portage III, 8C2
11 Laurier Street Gatineau, Quebec K1A 0S5
Attn: Chantale Norris or Patrick Scott

The use of email to communicate is preferred. Please ensure the subject line states: **ICAM RFI**

Suppliers are encouraged to submit questions and provide feedback even if they choose not to participate in Industry day and/or one-on-one meetings.

1.10. Language of Response

Responses may be submitted in French or English, at the preference of the respondent.

1.11. Submission of Responses

Time and Place for Submission of Responses: Canada requests suppliers submit responses in accordance with the RFI Response Request Date listed in Table 1 - Procurement / Engagement Activity and Related Dates.

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

Return of Response: Responses to this RFI will not be returned. Comments and input will be accepted any time up to the time when/if a follow-on solicitation is published or if the requirement is cancelled in whole or in part.

2. Objectives of this Request for Information

2.1 Purpose

This RFI is being issued with the key objectives of:

- Establish a continuous single point of official project(s) communication with potential suppliers;
- Solicit detailed feedback from potential suppliers on operational and technical requirements, cost and schedule;
- Advise potential suppliers of the security requirements of the RFP(s) and resulting contract(s) and provide direction and assistance to non-cleared suppliers in obtaining security clearances;
- Solicit advice on industry capabilities to develop the Industrial and Technological Benefits (ITB) Value Proposition (VP) with questions about industrial capacity for performing work related to the future contracts in Canada, strengthening Canadian supply chains, and making long-term investments in the Canadian IT sector.
- Answer questions from potential suppliers via industry day and one on one meetings, ensuring all interested participants receive the same information.
- RFI will remain open until a formal RFP(s) is released in the Definition Phase;
- Provide non-binding indicative project cost and schedule;
- Inform Industry of the proposed procurement approach; and
- Set the conditions for successful follow-on project activities.

3. Security

3.1 Information

One of the key purposes of this RFI is to advise suppliers of the security requirements associated with the various procurement and engagement activities and allow non-cleared suppliers to request security clearance sponsorship by PSPC in order to participate. It is Canada's intention to keep this RFI open until such time as a draft RFP is released to advise suppliers of the security requirements and sponsor suppliers to the Canadian Industrial Security Directorate (CISD). PSPC will cease to sponsor security clearances upon the release of the final RFP. Canada will not delay the release or closing of a RFP while suppliers obtain the required security clearance.

For more information on personnel and organization security screening or security clauses, suppliers should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

3.2 ICAM Security Requirements

It is anticipated that the following security requirements may apply to the Draft RFP, RFP and Contract:

Interested suppliers may be required to hold a valid Facility Security Clearance (FSC) at the level of SECRET, with approved Document Safeguarding at the level of SECRET; Personnel cleared to SECRET and Restricted to citizens of Canada and USA.

It is anticipated that the Draft RFP, RFP and resulting contract may require access to Controlled Goods. Prior to access, the contractor must be registered in the Controlled Goods Program of Public Works and Government Services Canada (Public Works and Government Services Canada (PWGSC).

Security clearance(s) must be issued by PSPC's Canadian Industrial Security Directorate (CISD). The security clearance of foreign suppliers will be confirmed through the International Industrial Security Directorate (IISD) with their own domestic industrial security programs. Please be advised that the proposed procurement activities beyond this initial RFI are for discussion only and may be amended at any time. The decision to conduct any further procurement activities has not been taken.

3.3 Security Sponsorship

As the security requirements for the Draft RFP, RFP and Contract have not been finalized, Canada may at a later date sponsor interested suppliers or potential bidders whose organizations currently do not hold the anticipated clearance(s). Should Canada choose to sponsor suppliers, this RFI will be amended to add the Security Requirements Check List (SRCL) and associated security clauses. Interested suppliers are encouraged to initiate the security clearance process as soon as the security requirements have been finalized. The process for requests for sponsorship is detailed in Annex F. It is the responsibility of the supplier to ensure that the information required concerning the security clearance is provided on time to either the Contracting Authority or the CISD.

Early submission of all applications for security clearances is strongly encouraged. Suppliers are also strongly encouraged to submit applications for security clearances for key individuals who may be required to have access to sensitive information and/or access to secured sites during any phase of the project starting with the current Industry Engagement up to Contract Award and Delivery.

Similar processes apply, with variances, to all of the countries with which Canada has bilateral security instruments. We encourage foreign suppliers to research the requirements of their own domestic industrial security programs to discover whether they are eligible to meet these requirements, and what the specific procedures that apply to their country might be. As mentioned, early submission is strongly encouraged.

Engagement Activities and any resulting Procurements will not be delayed in order to provide time for suppliers to obtain required security clearances.

4. Industrial and Technological Benefits (ITB) Policy

The ITB Policy, including the Value Proposition, may be applied to the ICAM Project. Engagement with industry through the RFI will help determine the application of the ITB Policy and how Canada could leverage opportunities for economic benefit from this procurement through the Value Proposition. Suppliers will have an opportunity to discuss the ITB Policy, Value Proposition, and how they might be applied to this procurement during one-on-one meetings following the Industry Day.

5. Official Languages

Any future contract for a solution to this project will require the Contractor to provide all documentation in addition to technical and client support in both official languages.

6. Engagement Approach

The industry engagement process began with a Letter of Interest and will conclude when a, or multiple, RFP(s) is/are issued or when Canada otherwise advises suppliers that the engagement process has concluded. As any final solicitation documents may themselves be classified they may not be publically posted. Please be advised that the proposed engagement approach and related procurement activities beyond this initial RFI are for discussion only and may be amended at any time. The decision to conduct any further procurement activities has not been taken.

Suppliers interested in participating in any of the engagement activities are advised to review the Rules of Engagement at Annex D.

Canada intends to undertake the following phased industry engagement approach:

Phase 1 Activities

Letter of Interest (completed)

Request for Information: This RFI aims to provide more detailed information to industry about DND's requirement for ICAM and will act as a continuous single point of official project communications.

Unclassified Industry Day: An unclassified Industry Day will be held at the Rideau Canal Junior Ranks Mess – Palladium Room, 3rd floor, 4 Queen Elizabeth Driveway, Ottawa, ON. The purpose of Industry Day is to present registered industry representatives with an outline of the procurement process, the engagement approach, security requirements and an unclassified overview of the project. The Industry Day is intended to be an open forum allowing Canada to communicate its requirements at a high level, and for industry to ask questions and seek information in order to gain a sound understanding of the requirement. In addition to the live event, Industry Day will be presented on WebEx.

The anticipated agenda for the Industry Day session is:

1. Opening Remarks;
2. Procurement Process – Engagement Approach;
3. Industrial and Technological Benefits Policy;
4. Security;
5. Controlled Goods;
6. Project Overview;
7. Question and Answer Period.

The following Industry Day material will be provided to attendees:

a. Agenda; and
b. Copies of presentation material.

One-on-One Meetings: Canada will make themselves available to registered suppliers for one-on-one meetings. These meetings will be unclassified and will be held at the Rideau Canal Junior Ranks Mess – Athena Room, 3rd floor, 4 Queen Elizabeth Driveway, Ottawa, ON. Suppliers who request a meeting will be provided with additional information and will be asked to identify potential schedule times within the specified window for a meeting with Canada. Canada will either confirm a requested time or will reply with an alternative suggested time. Meeting times will be allocated on a first come, first served basis.

All one-on-one supplier consultations will be concluded prior to the Requested Response Date of the RFI. Canada may request one-on-one consultations with any suppliers at any time during or after the Requested Response Date of the RFI to obtain clarifications on feedback received.

Phase 2 Activities

Request for Information: The RFI issued in Phase 1 will remain open until the draft RFP stage in order to enable suppliers to obtain the necessary security clearances.

Draft Request for Proposal: A draft RFP for the project may be released to suppliers meeting the security requirements for their review and input. The draft RFP may have one or more classified annexes.

Phase 3

Request for Proposal: A formal Request for Proposal for the project may be issued. The RFP may have one or more classified annexes. Only suppliers meeting the security requirements will have access to the classified components of any Draft RFP(s).

Evaluation: Bids will be evaluated in accordance with the terms of the RFP.

Phase 4

Contract Award: A single or multiple contract(s) may be awarded to the winning bidder(s) in accordance with the security requirements and the terms of the RFP.

7. INFORMATION REQUESTED BY CANADA

7.1. Documents of Interest

Attached to this RFI are the following documents for which Canada is seeking comments from industry:

- Annex A – Project Background and Preliminary Statement of Operational Requirements;
- Annex B – System and Architecture Descriptions – Current and Future;
- Annex C – Product Offerings and Pricing Information Response;

The information contained in this document are at a preliminary stage and remain 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. Nor should respondents assume that none of the requirements will be deleted or revised. Comments regarding any aspect of these draft documents are welcome.

7.2 Guidance and Registration

The following annexes provide additional guidance on how to respond to this RFI, Rules of Engagement and the registration process for meetings:

- Annex D – Rules of Engagement;
- Annex E – Registration for Industry Day and One-on-one Meetings; and
- Annex F - Request for Security Sponsorship

7.3 Invitation to Respond

All interested respondents are invited to provide a written submission to include (among others):

a. A description of proposed products and solutions covering each or a set of the notional functional components described in Annex B within the ICAM to-be architecture, operational view (Figure 2) ;
b. Indicative pricing, work breakdown structure, and scheduling of proposed products and solutions, including their integration, installation, configuration, testing, and training tasks;
c. Indicative pricing and scheduling of proposed in-service support and on-going maintenance tasks;
d. Proposed procurement approach with recommendations for competitive procurement, selection criteria, and basis of payment approach; and
e. Additional recommendations or advice concerning the project requirements and plans.

7.4 Information Requested

Using the format identified in section 1.8, Canada requests responses as follows:

Section 1 - Executive Summary:

Respondents are asked to provide:

1) a summary of the respondent's submission in total.

Section 2 - Corporate Profile:

Respondents are asked to provide:

1) Provide a brief introduction and corporate capability description, highlighting products, services, Canadian based capabilities, and experience in delivering ICAM solutions relevant to the project objectives. With respect to delivering ICAM solutions, please specify the following as appropriate:
    a. Whether you have experience in providing ICAM solutions in organizations with greater than 25,000 users distributed across widely geographically separated campuses?
    b. Whether you have experience in delivering ICAM capabilities in a classified environment?
2) Provide a summary of your intended role(s) (e.g., system integrator, component provider, site installer, verification and validation, training provider, in-service support provider, etc.), along with related experience and examples of projects and/or contracts (maximum of three examples for each, if applicable) with the name(s) and type(s) of customer(s) (private industry, government entity).
3) Describe established partnerships with other industries, if any, that would be of benefit to the development of the project capability requirements.
4) Provide security clearance level for your organization (if applicable) including Facility Security Clearance (FSC), Controlled Good Registration and any Document Safeguarding Capability (DSC); and
5) Outline any key assumptions, constraints, concerns, conclusions and recommendations that, in respondent's opinion, Canada should consider as the project evaluates the various options.

Section 3 - Proposed Concept of Solution.

Respondents are asked to provide:

1) Outline Plan of Solution - An outline concept, high-level work breakdown structure, and schedule for any or all deliverables defined in Annex B that the respondent intends to provide, describing key products and components, software, hardware, engineering services, training, and in-service support. Suppliers should, in the context of the information in Annex B:
    i. Provide a description of their vision for a solution(s) in year 2025 that would meet specific or all project requirements and capabilities, as described at in Annex B – ICAM To Be Architecture;
    ii. Provide a description of how their proposed system specifications and capabilities would meet or exceed the requirements outlined in Annex B (note that suppliers may offer solutions that do not necessarily conform to the components described in Annex B within the ICAM To Be Architecture as long as the total solution meets the requirements);
    iii. Provide recommendations and short justifications on the proposed project capability packages;
    iv. Provide recommendations and short justifications for portions of the ICAM capability requiring DND/CAF hardware equipment;
    v. Provide recommendations and short justifications for portions of the ICAM capability that DND/CAF should implement internally as part of the overall solution;
    vi. Provide recommendations and short justifications for portions of the ICAM capability that will require industry-provided In-Service Support (ISS);
    vii. Provide recommendations and short justifications for portions of the ICAM capability requiring industry-provided training;
    viii. Provide their approach to innovation, with a view to maintaining capability relevance throughout the lifecycle; and describe how the proposed solution achieves the desired capability identified in Annex B;
    ix. Indicate the degree of deployable modularity with their solution and its components;
    x. Indicate their solutions' scalability to meet larger enterprise needs of up to 50,000 users with a potential yearly data growth of thirty percent (30%) per year;
    xi. Provide solution deployment details, including phasing approaches, development, testing, implementation, training and upgrades;
    xii. Provide product, sub-system and system-level reliability and availability from historical information;
    xiii. State risks identified for Technical, Management, Training, Security, Support and Schedule. State recommended mitigations (note: if a risk can be mitigated by altering existing policies, CONOPs or architecture, the Supplier should feel free to recommend such a mitigation strategy); and
    xiv. Provide relevant product sheets for proposed products and solutions, if available and not-previously provided.

2) High Level Outline Plan and Sequence of Events - An indicative project plan and schedule (measured in Months after Contract Award) for the delivery of any or all deliverables defined in Annex C that the respondent intends to provide.

3) Estimated Costs for Each Deliverable - An indicative cost estimate, with a per-unit description where applicable, for any or all deliverables defined in Annex C that the respondent intends to provide. The goal is to confidently estimate the Total Cost of Ownership over the life of the capability. To that end, the supplier should present a view so that the development, test, roll-out, support and upgrade costs, including recurring and nonrecurring costs, are clearly identified and broken out for the entire life cycle. In completing the Cost Data Model, provided as Annex C, Respondents are requested to clearly state how each deliverable is costed along with its estimated annual in-service support costs. The in-service support costs should include detailed information, such as quantity of staff required to support the solution. For example, if delivering a capability requires discrete hardware and software units, support personnel or operations centre staff, suppliers should clearly indicate such in the Unit Cost Basis, the Price/Unit and the Number of Units required. At a minimum, the response must indicate the solution as a clearly calculable cost based on a simple model of: *Cost = Price/Unit x Quantity of Units.* The same is applicable for tasks such as engineering solutions, where the response must indicate the cost based on the model: *Cost = Level of Effort (days) x Price/Person (per day) x Number of person required*.

Section 4 - General Comments and Advice.

Respondents are asked to provide comments, remarks, and advice concerning:

1) The performance objectives, operational requirements and/or notional functional components as described in Annex A.
2) The current capabilities as described in Annex B, including operational unit organizational structures.
3) Improvements to project descriptions, objectives, management and procurement approaches to enhance overall implementation efficiencies.
4) Proposed solutions:
   i. Whether the proposed solution(s) fulfill all the relevant requirements?
   ii. List the open source and/or commercially available 3rd party components (suppliers) required to integrate with the proposed solution to make it complete?
   iii. How does/do the proposed solution(s), including selected open source and/or commercially available 3rd party components, integrate and interoperate in a diversified technology environment? Is the proposed solution intended to reuse and integrate existing DND/CAF components?
   iv. Will components of the proposed solution be rendered ineffective in a Disconnected, Intermittent and Low Bandwidth environment and to what extent can interruptions be recovered? What are the proposed alternatives to support in a Disconnected, Intermittent and Low Bandwidth environment and costing associated with that?
   v. Where applicable, could the DND/CAF obtain demonstration licenses of the proposed solution(s) component(s) for its test and evaluation environment?
5) Supply Chain Integrity and Security
   i. References:
      a. https://www.cse-cst.gc.ca/en/page/technology-supply-chain-guidance
      b. https://www.cse-cst.gc.ca/en/node/300/html/25733
      c. https://www.cse-cst.gc.ca/en/node/299/html/25729
   ii. The Communications Security Establishment Canada (CSEC) offers IT Security advice and guidance to the GC on supply chain threats and vulnerabilities, as well as prevention and mitigation guidance.
   iii. The guidelines for Contracting Clauses for Telecommunications Equipment and Services (TSCG-01\G) provides security clauses that can be included in PSPC contracts with the aim of preventing or mitigating supply chain risks to GC communications networks and information technology (IT) infrastructure, often referred to as Supply Chain Integrity.
   iv. The clauses are based on a "managed telecommunications services" scenario, whereby a contractor is given responsibility for selecting, implementing, operating and maintaining the telecommunications infrastructure and services for GC clients. Some of the clauses are also relevant for IT solution or hardware/equipment procurement. The guidelines identify a process to select and tailor specific clauses, including the cost, schedule and requirements considerations.

v. The Contracting Clauses for Telecommunications Equipment and Services Leaflet (TSCG-01\L) describes the purpose and provides an overview of the clause groupings.
vi. Question: How could these contracting clauses potentially affect the cost, schedule and design of your proposed solution? What additional information would your company need to better address cost, schedule and design risks imposed by Supply Chain Integrity related restrictions?

6) Any other areas of concern or advice that would aid in providing a recommendation for improvement for the definition of the projects and their implementation.

Appendix 1 to RFI

ABAC	Attribute Based Access Control
AC	Access Control
ACL	Access Control Lists
ACS	Access Control System
ADM (IM)	Assistant Deputy Minister (Information Management)
API	Application Programming Interface
BPMN	Business Process Model and Notation
CA	Comprehensive Approach
CAF	Canadian Armed Forces
CISD	Canadian Industrial Security Directorate
CIV	Civilian
CONOPS	Concept of Operations
COTS	Commercial-Off-The-Shelf
CSEC	Communications Security Establishment Canada
CSNI	Consolidated Secret Network Infrastructure
CSV	Comma Separated Values
DIMEI	Director of Information Management Engineering and Integration
DMN	Decision Model and Notation
DND	Department of National Defence
D-PKI	DWAN – Private Key Infrastructure
DWAN	Defence Wide Area Network
DWAN-PKI	DWAN Public Key Infrastructure
EAGS	Enterprise Access Governance Service
EFAS	Enterprise Federated Authentication Service
EGAS	Enterprise Governance Access Service
EIDS	Enterprise Identity Data Service
GBA+	Gender Based Analysis-Plus
GC	Government of Canada
GOTS	Government-Off-The-Shelf
HRMS	Human Resource Management System
HTTP	Hypertext Transmission Protocol
ICAM	Identity, Credential and Access Management

ID	Identity
idms	Identity Management System
IISD	International Industrial Security Directorate
ISS	In Service Support
IT	Information Technology
ITB	Industrial and Technological Benefits
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOA	Level of Assurance
LOI	Letter of Interest
MOTS	Military-Off-The-Shelf
MS	Microsoft
NATO	North Atlantic Treaty Organization
NSE	National Security Exception
NTLM	NT LAN Manager
OAUTH	Open Authentication
OGDA	Other Government Departments and Agencies
OIDC	OpenID Connect
OT&E	Operational Test and Evaluation
PACS	Physical Access Control System
PDF	Portable Document Format
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
PKI	Public Key Infrastructure
PSPC	Public Services and Procurement Canada
RBAC	Role Based Access Control
RDBMS	Relational Database Management System
REST	Representational State Transfer

RFP	Request for Proposal
RFI	Request for Information
SA&A	Security Assessment and Authorization
SAAG	Security Assessment and Authorization Guideline
SAML	Security Assertion Markup Language
SCIM	System for Cross Domain Identity Management
SDS	System Design Specification
SEP	System Engineering Plan
SIR	System Interface Requirements
SoDs	Segregation of Duties
S-PKI	Secret – Public Key Infrastructure
SOP	Standard Operating Procedures
SQL	Structured Query Language
SRD	System Requirements Document
STANAG	Standing NATO Agreement
TRA	Threat Risk Assessment
USB	Universal Serial Bus
VP	Value Proposition
VPN	Virtual Private Network
V&V	Verification and Validation
WS-Fed	Web Services Federation
XACML	eXtensible Access Control Markup Language

ANNEX A

PRELIMINARY STATEMENT OF OPERATIONAL REQUIREMENTS

ICAM Capability Background

Between 2018 and 2027 the Department of National Defence (DND) ICAM project will design and deliver interoperable and federated ICAM capabilities to centrally manage, monitor and control identities, user accounts and credentials. These ICAM capabilities will improve the productivity and security of Departmental resources and enable the Department to meet government policies related to privacy.

Continuing the current approach to ICAM, which is distributed, disconnected and lacking in automation will limit the protection of assets, slow the ability of users to access resources, hamper decision making related to the granting and revoking of access-entitlements, and increase the risk of loss, damage or compromise to Departmental assets.

DND has determined that it must modernize and improve interoperability, accuracy and privacy of its identity data and credentials and of its access controls to physical facilities, information and information systems. Currently, the Department is dealing with multiple uncoordinated identity and credential information sources that get duplicated multiple times.

The ICAM project will enable asset owners to quickly and safely generate user credentials and resolve access decisions by using a single digital identity provided by a centrally managed identity service. Rationalized ICAM processes will be created to make users more productive, assets more secure, decisions more transparent and actions more auditable. In addition, ICAM will:

- Mitigate cyber threats;
- Support rapid forensic investigations of access breaches;
- Give people visibility of their personal identity information,
- Allow people to enter and update their own profiles; and
- Allow for GBA+ in the design of identity, credential and access systems.

As of July 2019, DND was in the process of establishing an ICAM Governance framework that will coordinate ICAM activities across the Department. Concurrently, the ICAM Project was in the Options Analysis phase, during which the project team produced 15 ICAM use cases that describe required functionality of the capability. These use cases can be found in the Operability Requirements section below.

System Operations

Mission and Scenarios.

The Department of National Defence (DND) will deliver an Identity, Credential and Access Management (ICAM) capability to centralize identity, credential and access services in the Department.

Currently, DND identity, credential and access controls are compartmentalized, lacking central management, monitoring and control. Complicating the current state are external threats enabled by exposure of DND unclassified networks to the public internet. The existing situation is complex and unsustainable and it exposes Departmental operations to information security risk.

When delivered, the future ICAM capability will be based on the principle that every entity in the Department, both person and non-person, will have a single digital identity. Between 2018 and 2027 the Department of National Defence (DND) ICAM project will design and deliver interoperable and federated ICAM capabilities to centrally manage, monitor and control identities, user accounts and credentials. These ICAM capabilities will improve the productivity and security of Departmental resources and enable the Department to meet government policies related to privacy.

Continuing the current approach to ICAM, which is distributed, disconnected and lacking in automation will limit the protection of assets, slow the ability of users to access resources, hamper decision making related to the granting and revoking of access-entitlements, and increase the risk of loss, damage or compromise to Departmental assets.

The ICAM project will enable asset owners to quickly and safely generate user credentials and resolve access decisions by using the single digital identity provided by a centrally managed identity service. Rationalized ICAM processes will be created to make users more productive, assets more secure, decisions more transparent and actions more auditable. In addition, ICAM will:

- Give people visibility of their personal identity information;
- Allow people to enter and update their own profiles;
- Allow for Gender Based Analysis-Plus (GBA+) in the design of identity, credential and access systems;
- Mitigate cyber threats; and
- Support rapid forensic investigations of access breaches.

The diagram below at Figure 1 provides an overview of ICAM business processes and shows navigation through the high level ICAM use cases. Figure 1 splits ICAM into two main processes – those for users whose information is stored within DND, such as for its employees and contractors, and those whose information is managed externally and is leveraged through a federated process. DND managed users and federated users fall within the following three categories:

- Federal Entities – Any individual that is an employee or contractor to the Federal Government. Can be DND managed or federated depending on the user and system;
- Business Partners – Individuals from state and local governments, or commercial organizations are usually federated however in some cases may be DND managed; and
- Customers – Individuals that are DND customers. They are usually federated, but may in some cases be DND managed.

While each use case describes a particular ICAM business process, all are highly interrelated. The dotted lines within the diagram depict relationships between use cases.

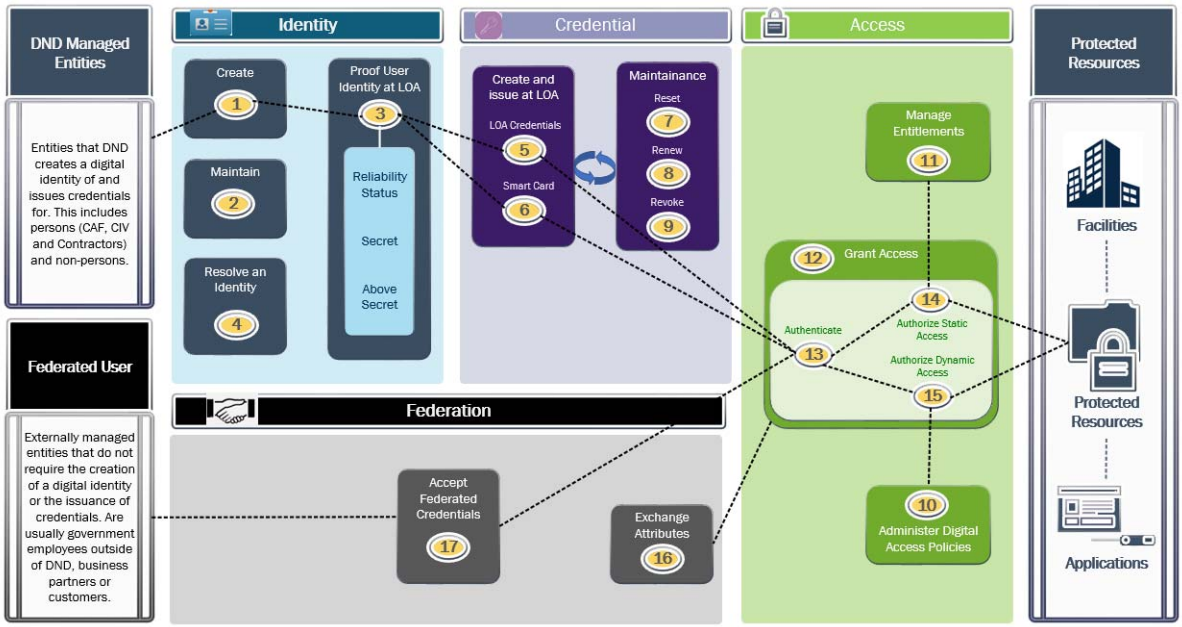

Figure 1: ICAM operational view. Numbers 1-17 refer to the ICAM tasks listed in Section ***Error! Reference source not found.****.*

<u>Operating Environment</u>

The ICAM capability will operate across the CAF/DND environments at all security levels: Unclassified, Secret, and Above Secret. The capability will act as the central authority for digital identity supporting the highest levels of identity and credential assurance in order to support the requirements of the different environments and security levels.

Through standardization, governance and delivery of a common service, ICAM will be able to integrate with strategic through to tactical level logical and physical access control points.

The operational authority of logical resources (networks, applications, etc.) will be able to integrate with the ICAM capability to support their own specific requirements for identity information, authentication and access and credentials.

The operational authority for facilities and bases will similarly be able to integrate with the ICAM capability to support their own specific requirements for identity information, authentication and access and credentials.

While the project itself will target integration with a subset of logical and physical resources, the intention is to provide a modern service with standardized interfaces, high identity and credential assurance and governance to support the eventual integration of all systems/services with a single ICAM capability.

The operating environment for the capability needs to consider both current and potential future requirements of systems requiring access control across the CAF/DND.

Threat Environment

Historically, the Department contained threats to information assets by securing them inside physically controlled spaces. With the information age, 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 DND's electronic information and control systems. The current situation has not come about due to a failure of any single element within the organizational framework or due to a sudden unanticipated change to the environment. Rather, it has arisen slowly through the proliferation of computers and networked services into every operation and corporate business practice.

Furthermore, the threat to information assets will exponentially increase as a result of DND continuing to implement the Comprehensive Approach (CA) to operations, since CA requires increased internal, interdepartmental and multinational accessibility and information sharing. Along with the expectation that accessibility and information sharing will increase, DND senior leadership expects that the safeguarding of information also will increase to support privacy requirements and the confidentiality of information assets.

Threat Risk Assessments

ICAM systems will be at unclassified, secret and above-secret domains. Threat Risk Assessment (TRA) requirements will be different depending on which domain is implicated.

Concept of Operations

The ICAM capability will create a single digital identity for each person and non-person entity in the Department. A central identity management function will be used by the managers of physical and logical assets, including bases, stations, other facilities, networks, applications and other IT services to create and manage credentials needed to authenticate and authorize a person or non-person entity's access to an asset.

The central identity service will act as a broker between organizations that need to produce and/or consume identity information. The broker will permit asset managers to use both role based and attribute based identity information to make access decisions.

ICAM will not be embedded in existing or new access management systems, rather it will be provided as an available service to which the operational authorities for networks, applications and physical access systems will subscribe. A set of standard processes and protocols will be put in place to mediate the exchange of identity and credential information.

DND and the CAF have many relationships with external organizations including Other Government Departments and Agencies, allied militaries and private sector partners. These relationships will require DND to provide federated ICAM capabilities that enable the exchange of identity and credential information with these external organizations. Examples of federated uses of ICAM are:

- Automatically authorize the sharing of an information object with an external partner;
- Automatically authorize the access of an external person to a DND physical space;

- Automatically deliver identity information to an external partner to enable access by a DND entity to an external organization's physical or logical asset.

ICAM includes a governance function that will coordinate the implementation of ICAM capabilities across Level 1 organizations in the Department, to make decisions about adopting standards, to optimize a program of initiatives and projects to maximize the net benefit of investments in ICAM and to maintain the architecture views of the ICAM enterprise as it is implemented and develops over time.

Key Roles

Table 1: ICAM Key Roles

Roles/Actors	Definition
Access Control System (ACS)	In the fields of physical security and information security, access control (AC) is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication, which requires two or more authentication factors, is often an important part of layered defense to protect access control systems.
Application	Application software is computer software designed to perform a group of coordinated functions, tasks, or activities for the benefit of the user.
Approval authority	The Designated Approving Authority is the official with the authority to formally assume responsibility for operating a system or business function at an acceptable level of risk.
Authoritative source	A recognized or official data-production source, which publishes reliable and accurate data for subsequent use by clients. An Authoritative source may be the functional combination of multiple, separate data sources.
Business Partners	Individuals from Other Government Departments and Agencies or private sector organizations.
Contractor	The Contractor is the person, entity or entities named in the Contract to supply goods, services or both to DND.
Credential manager	Credential manager is an individual or system that issues, resets, renews or revokes credentials.
Credential service provider/Issuer	A Credential Service Provider is a trusted entity that issues security tokens or electronic credentials to subscribers and could be commercially provided, an agency service, or a shared service.
Customers	Individuals that are DND customers. They are usually federated, but may in some cases be DND managed.
Data administrator	Data administrator is an individual that works closely with the administration body to administer and implement additions and adjustments to digital access policies.
Data repository	The repository itself is an infrastructure of databases that collect, manage and store varying data sets.

Roles/Actors	Definition
Data Source	The primary location from where the authoritative data comes.
Digital policy administration body	Policy administration body that creates and updates the rules that govern logical and physical access for an organization and translates those rules into the digital policies that govern access decisions. Policymaking bodies often draw on federal regulations, executive orders, legislation, organization-specific rules, and past precedent when crafting or updating digital access policy.
Employee	A generic term that encompasses DND civilian employees and military members.
Entitlements manager	Entitlements manager oversees and adjusts the access privileges granted to individuals, roles, and groups within an organization.
Federated Entities	Any individual that is an employee or contractor to DND. Can be DND managed or federated depending on the user and system.
Identity manager	The identity manager identifies relevant sources of data on the individual and aggregate identity data to create a complete identity profile.
Personnel administrator	HR administrator responsible for populating new hire's or contractor's information into the appropriate authoritative data source.
Protected resource	All DND resources that can only be accessed by authorized users or systems.
Remote system	A system to which a user does not have physical access, but which he or she can access or manipulate via some kind of computer network.
Requestor	Requester is defined as the person or a system who initiates a request.
Sponsor	Sponsor is an official who can verify an individual's need for items like credentials. For example a sponsor could request LOA3 credential for an individual.

Key Tasks

Table 2: ICAM Key Tasks

#	Task
1	Creation (on-boarding) of an entity's digital identity.
2	Maintenance of an entity's digital identity.
3	Identity proofing at the required level of Assurance, e.g. currently in DND, identity proofing is done at the levels of: 1. Reliability; 2. Secret; and/or 3. Above secret.

#	Task
4	Resolution of an Identity Internal to DND.
5	Creation and issuance of Level of Assurance Credential.
6	Creation and issuance of smart card.
7	Resetting credentials for an entity.
8	Renewing credentials for an entity.
9	Revoking credentials of an entity.
10	Administering digital access policies.
11	Managing entitlements by overseeing and adjusting the access privileges granted to an entity.
12	Granting access to protected resources.
13	Authenticating an entity.
14	Authorizing access using static methodology.
15	Authorizing access using dynamic methodology.
16	Exchanging attributes in a federation.
17	Accepting Credentials in a Federation.

Concept of support

Support to the ICAM capability will follow industry best practices. These are currently captured under the Information Technology Infrastructure Library (ITIL) framework, which focuses alignment of IT services to business needs. ITIL practices will be adapted to suit the unique environment and organizational structure of the DND/CAF

As the ICAM capability will become a key service extending throughout the DND/CAF, high level support for the service will be provided by Assistant Deputy Minister (Information Management) (ADM(IM)), specifically the Director of Information Management Engineering and Integration (DIMEI). Their role will be to maintain the ICAM Reference Architecture for the Department and provide oversight of engineering and integration of resources with the ICAM capability.

Essential to the success of the capability will be the establishment of a permanent ICAM governance body within DND. The governance body will have multiple levels from an Executive Steering committee down to working groups which can support the continual integration, support, management and evolution of the ICAM service.

Within the different domains, the ICAM capability will be incorporated into the existing support systems available.

<u>Lines of Support</u>

The Concept of Support will outline, in the future, how the five ITIL components, listed above, will be enhanced and implemented by ADM(IM) to support the capabilities delivered by the project. The detailed Concept of Support will be developed during the Definition Phase of the project as system design, key performance measures and functional specifications are defined.

Levels of Support

ICAM systems and infrastructure support will be aligned with the three level approach currently used by the DND/CAF, specifically:

- First level support – involves the registration and classification of received incidents, and immediate response to attempt to restore a failed service as quickly as possible. If an immediate solution cannot be achieved, first line support will refer the issue to second line support. First line support also processes service requests and keeps users informed about the status of resolution;

- Second level support – takes over incidents that cannot be resolved immediately by first line support. Second line support will coordinate with service providers as required to resolve incidents. Problems that cannot be resolved at this level will be passed to third line support; and

- Third level support – is provided by engineering services. Engineering services will liaise with manufacturers and third party suppliers as required to resolve incidents. Typically, incidents that are raised to the third level of support require a change request to modify the system in order to solve the incident.

For ICAM systems and infrastructure, the levels of support will be determined for each service and system provided. Support organizations will be tasked to provide specific levels of support based on their available knowledge, skills, technical data, special tools, test equipment and/or time.

Applications.

The ICAM capability will be integrated into both the Defence Wide Area Network (DWAN) and Consolidated Secret Network Infrastructure (CSNI) as a core service. Major applications (e.g. Directory Services, PKI, Human Resource Management System (HRMS)) residing within these networks will be integrated to allow management and control through the new service. Physical access systems will be connected to the service. Additional applications, networks and services will be considered for integration based on a case by case basis during both the definition phase and implementation phase of the ICAM project.

Design and Concept Guidance

ICAM design guidance is:

- At the centre of ICAM design is the concept of a single digital identity for each person and non-person entity;

- Design of the ICAM system must be based on the principle that identity and credential information is authoritative, created and controlled by authoritative sources;

- Automation is a central concept to the ICAM capability design;

- The ICAM services must be modular to the maximum extent possible;

- Interoperability between organizations and interoperability between DND and external partners is key to a successful ICAM design;

- Information privacy, in particular the privacy of personal information, is central to the ICAM capability design concept;

- ICAM information exchanges, formats and protocols are, whenever possible, based on industry and/or government common and agreed standards. The ICAM capability design must maximize the use of Commercial-Off-The-Shelf (COTS), Government-Off-The-Shelf (GOTS) or Military-Off-The-Shelf (MOTS) components and minimize the custom design of systems;

- The ICAM capability must consider maximum reuse of existing systems, components, processes and organizational structures, must be designed with expandability and extensibility in mind and must facilitate upgrades with emerging technology;

- The ICAM capability design must minimize the requirement for new infrastructure;
- The ICAM capability design must maximize the use of available state-of-the-art IT technologies (this guidance does not remove the requirement for reuse (subparagraph h); and
- The ICAM capability design must be able to support up to 30% yearly data growth. This must be considered for both the design of the infrastructure and In-Service Support.

The following ICAM services are in scope:

- Enterprise Identity Data Service (EIDS) – Described in Annex B of this RFI.
- Enterprise Federated Authentication Service (EFAS) – Described in Annex B of this RFI.
- Enterprise Governance Access Service (EGAS) – Described in Annex B of this RFI.
- ICAM Cross Domain Information Exchange Gateway

EIDS and EFAS may be developed by DND prior to the ICAM implementation phase. These services would then need to be integrated into the ICAM solution.

Creating the following services are not in scope:

- DWAN Public Key Infrastructure (D-PKI)
- Secret Public Key Infrastructure (S-PKI)

Security Assessment and Authorization

A complete SA&A will be conducted in accordance with the Security Assessment and Authorization Guideline (SAAG), resulting in the promulgation of appropriate direction regarding the implementation of the hardware, software, personnel and procedures necessary to meet the capability security requirements.

System Effectiveness Requirements

Level of Requirement / Performance Criteria

All ICAM requirements are mandatory. Requirements will be prioritized by: value, negotiation, time boxing and level of effort.

General Requirements

The establishment and maintenance of a permanent governance structure that:

- Provides ICAM policy direction;
- Optimizes the ICAM program against DND strategic objectives;
- Directs and manages identity and credential data standards; and
- Creates and maintains the ICAM enterprise architecture.

The ability to create an authoritative identity and associated credentials that can be used to mediate access within DND/CAF and externally between DND/CAF and OGDA and multinational partners.

The ability to securely update, store and retire the unique identities and associated credentials of CAF members, DND employees, foreign partners, internal contractors, visitors and non-person entities.

The ability to control in near real-time, i.e. minutes to hours, the access entitlement to a building, site or space that has an access control point, supporting protection from unauthorized access.

The ability to control access entitlements to electronic information, networks, Information Technology services, applications and systems supporting protection against unauthorized access.

The ability to on-board and off-board people and non-person entities for access to physical and electronic information assets within a matter of minutes or hours, while minimizing human errors through automation of identity information sharing between systems, networks and organizations.

The ability to isolate damaged or destabilized segments of ICAM and maintain identity, credential and access management functions across the unaffected segments of the enterprise.

Operability requirements

Table 3: ICAM operability requirements

ID	Title	Description Entity = 1) Person Entity and 2) Non-Person Entity
1	Create an Identity	When an entity is on-boarded to a DND unit, information is collected and stored to act as their digital proxy in IT systems. This information is stored within an identity record, which is then modified or deleted as needed. Once a digital identity record is established, it is pushed to other systems from an authoritative source and provisioned access permissions (see Manage Entitlements). **Note:** There are different path ways for Persons (member, an employee, contractor or temporary visitor) and non-persons.
2	Maintain an Identity	Once an entity's identity has been created at DND, the identity data can be updated only within the authoritative source to ensure the accuracy of the data. The ICAM system shares the updated identity with resources which have access to that entity's identity data.
3	Proof an Identity at Level of Assurance Reliability Secret Above secret	Before an individual is on-boarded a proofing process is completed. This process establishes their proof of Identity after which the individual receives credentials at an appropriate Level of Assurance. The level of assurance required for an individual is role dependent and can be Reliability, Secret or above Secret. Proofing provides a level of assurance that further defines and allows an individual to receive credentials. **Reliability**: Requires an individual to submit basic documents to prove their claimed identity. **Secret**: Requires the completion of a strong verification process and additional documents than required for reliability. **Above Secret:** Requires the most robust process for verifying the individual's claimed identity.
4	Resolve an Identity Internal to DND	DND has multiple source systems that contain data relevant to an entity's identity. A request for identity data will be initiated to the identity manager. The identity manager must be able to identify the relevant sources of data for obtaining identity attributes from their originating, authoritative systems and aggregate it into a single record for presentation or evaluation.
5	Create and Issue Level of Assurance Credential	When a request for assurance level credentials is initiated, a credential service provider must be able to validate the request and assign credentials to the requestor. A credential token meets the required assurance level when it uses a single or multiple factor for authentication (See Authentication use case),

ID	Title	Description Entity = 1) Person Entity and 2) Non-Person Entity
		mandates a strong PIN or password, and only transmits credential information using cryptographic protection.
6	Create and Issue smart card	When an individual is on-boarded a smart card must be created and issued. A smart card will contain the necessary data for the cardholder to be granted access to DND facilities and information systems and assure appropriate levels of security for all applicable DND applications. A smart card must be secure and reliable.
7	Maintain Credential - Reset	When an individual forgets the shared secret associated with their credential, usually a password or PIN, they can request a reset. This prevents them from having to request a new credential.
8	Maintain Credential - Renew	When an entity's credential expires and they have the necessary approvals in place, they must have an option to automatically renew the credentials rather than go through the issuance process again.
9	Maintain Credential - Revoke	When an entity separates from DND or is no longer eligible for their credential, their credential should be revoked. Once the credential manager receives the request for revocation, the credential manager invalidates the credential and disables its access provisions.
10	Administer Digital Access Policies	Policy administration describes the process of creating and updating the rules that govern logical and physical access for an organization and translating those rules into the digital policies that govern access decisions. Creation and implementation of policy process will happen during design time, before persons and non-persons attempt to access protected resources. Once a policy is created, it will be referenced during run time to dynamically make access decisions at the time access is attempted based on an entity's roles and attributes. Policymaking bodies will draw on federal regulations, executive orders, legislation, organization-specific rules, and past precedent when crafting or updating digital access policy.

ID	Title	Description Entity = 1) Person Entity and 2) Non-Person Entity
11	Manage Entitlements	Entitlements management is the process of overseeing and adjusting the access privileges granted to an entity within an organization. This process is known as 'provisioning' and applies to static access management. Managing entitlements will occur during design time, before an entity attempts to access protected resources, and entity's entitlements will be provisioned before they access protected resources. Request to create entitlements for an entity will be submitted, reviewed and if the requested change is in accordance with policy and the entity has a mission need for access, the request will be approved. The entity is provisioned with updated access entitlements. Those entitlements are updated and maintained whenever their roles change.
12	Grant Access to a Protected Resource	Only an eligible entity is granted access to the protect resources. In this process the entity is authenticated, authorized or denied user access to protected logical and physical resources including systems, files and physical facilities. A person entity has the ability to view and authorize the sharing of their identity information with resource owners.
13	Authenticate an Entity	During this process certain steps are followed for authenticating an entity who has requested access to a protected resource. During authentication a system will verify the entity's claimed identity to a certain level of assurance (LOA). There are three types of authentication factors: something you know (such as a password or PIN), something you have (such as a smartcard), and something you are (such as your fingerprint). The system will then prompt the entity to provide authentication, entity provides single or multiple factor authentication (depends on LOA). The Access Control System then verifies the entity's input against information about the entity's claimed identity. If the factors are verified, authentication is successful.
14	Authorize Access - Static	A static method of authorizing access to a protected resource is followed for authorizing access. Under the static model, DND will provision entities to a set of access entitlements. When the entities attempt to access a protected resource, the access control system (ACS) checks their permissions against the resource's access rules. This model is typical of Access Control Lists (ACL) and RBAC (role-based access control) systems.
15	Authorize Access - Dynamic	A dynamic method of authorizing access to a protected resource is followed for authorizing access. Under the dynamic model, DND establishes a set of access policies. When the entities attempts to access a protected resource, the access control system (ACS) evaluates their attributes against those policies. When an entity's attributes change, their access entitlements

ID	Title	Description Entity = 1) Person Entity and 2) Non-Person Entity
		change dynamically. This model is typical of ABAC (attribute-based access control) systems.

Interoperability Requirements

Interoperability requires that the ICAM capability has the ability to meet the following interoperability standards:

- EIDS Standards
  - Front end: System for Cross-domain Identity Management (SCIM), Lightweight Directory Access Protocol (LDAP),
  - Back end: LDAP, Relational Database Management System (RDBMS), Comma Separated Values (CSV) Feed, LDAP Data Interchange Format (LDIF), Custom Representational State Transfer (REST);

- EFAS Standards –
  - Authenticator support: Client Certificate Auth, Password, One Time Password based auth (Out of Band & Device),
  - Federation: Security Assertion Markup Language (SAML), OpenID Connect (OIDC), OAuth, WS-Fed,
  - SSO: Kerberos, NT LAN Manager (NTLM), HTTP-Header, Federation token; and

- EAGS Standards –
  - Front end: EFAS protected (Browser based web app, Mobile app),
  - Back end (Provisioning / Access mgmt): SCIM, LDAP, RDBMS, CSV Feed, Custom REST, RACF/Top-Secret, Powershell, SSH, MS-Exchange, SharePoint, CRM-Dynamics,
  - Workflow: Business Process Model and Notation (BPMN) / Decision Model and Notation (DMN) modeling tools, custom activities and automation scripts,
  - Access Modeling: Role Based Access Control (RBAC) / Attribute Based Access Control (ABAC), and
  - Notifications: e-mail, mobile alerts.

The infrastructure must provide the capability to exchange attributes in a federation. The term ‘federation’ describes an environment where an agency has established the tools and policies to accept identity and credential information from entities at another organization, thus expanding secure access to entities outside the organization. When an entity from a partner's organization requests access to a DND resource, DND uses entity's attributes to make an access decision. Rather than creating a new identity record, DND query’s a metadata service to determine where a record of that entity's attributes already exists. This is also used to support design time identity maintenance. The approach is both a brokered and non-brokered approach for obtaining attributes. It also applies to situations where attributes are being sought from another division within DND.

The infrastructure must provide the capability to accept credentials in a federation. DND will federate with external (government and private sector) organizations in order to conduct operations, expand services, reduce costs, and improve overall efficiency.

Survivability

The ICAM capability, as a core service to DND/CAF, will operate within the target environment (e.g. Low – DWAN, High – CSNI) on infrastructure with the highest level of survivability available. The ICAM capability end-state will be to support multiple security domain ICAM requirements. Interfacing with the Enterprise Identity Data Services (EIDS) will be the authoritative identity attribute sources. Once these sources are consolidated (on the Low side), they will be transferred up to higher security domains. ICAM will leverage current and future cross domain solutions to move

instances into higher security domains. Survivability will be designed within each security domain to the degree necessary to support operations.

Availability

Availability is a measure of the % of time ICAM computer-related hardware or software is in an operable state. Availability level for ICAM is expected to be 99.99%. This level may be revised in any RFP may be issued.

Availability also may be considered based on ICAM consuming systems and be designed, configured and deployed in a manner relevant with the end-usage. For example, the availability of the system to issue new credentials may be lower than the availability of the verification during authentication. The end state will be a highly available ICAM solution capable of supporting DND operational requirements.

Reliability

Reliability refers to the ability of a computer-related hardware or software to consistently perform according to its specifications. Reliability level for ICAM is expected to be 99.99%. This level may be revised in any RFP that may be issued.

The ICAM capability, as a core service to DND/CAF, will operate within the target environment (e.g. Low – DWAN, High – CSNI) on infrastructure with the highest level of reliability.

Supportability

ICAM shall meet the following supportability requirements:

- The ability to be delivered with all required In-Service Support resources to operate and support the capability;
- The ability to provide centralized operations and service management of the ICAM capability the low side (DWAN) and the high side (CSNI);
- The ability to monitor the status of services, detect when a service is not functioning correctly, and generate event notifications automatically to the appropriate network operations centre;
- The ability to align/re-align services in a timely manner without impacting the rest of the capability, using automated tools to the maximum extent possible;
- The ability to track, record and manage the details, dependencies and interfaces for all its services, using automated tools to the maximum extent possible;
- The ability to provide a user self-service portal;
- The ability to monitor and generate automated reports on service metrics;
- The ability to manage user and entity identities using automated tools to the maximum extent possible;
- The ability to manage user and entity credentials using automated tools to the maximum extent possible;
- The ability to grant access to the infrastructure using automated tools to the maximum extent possible; and
- The ability to support the allocation of administrative privileges.

Security and Privacy

- The following are ICAM security and privacy requirements:
- The ability to enable, and in some cases enforce, access control using multi-factor authentication;
- The ability to control user credentials across all ICAM enabled systems;
- The ability to immediately terminate an entity's access to one or all ICAM enabled systems;
- The ability to limit privileged users to ICAM administration functions and information;
- The ability to use security marking metadata labeling compliant with STANAG 4774 – Confidentiality Metadata Label Syntax;
- The ability to use binding of security marking metadata to information in accordance with NATO STANAG 4778 - Metadata Binding Mechanism and DND/CAF Policy;
- The ability to support access decisions based on an entity's role(s);
- The ability to support access decision based on an entity's attributes;
- The ability to audit ICAM workflows including –
    - On boarding,
    - Off boarding,

    - Identity proofing,
    - Credential issuance,
    - Credential revocation,
    - Authentication, and
    - Access authorization;
- The ability to audit access decisions, including –
    - Manual,
    - Automated,
    - Authorized, and
    - Unauthorized;
- The ability to support forensic investigation of security breaches;
- The ability to guarantee and protect privacy of information for Personally Identifiable Information (PII);
- The ability to track the provenance of all identity data processed by the ICAM capability from creation to destruction; and
- The ability to provide tamper proof auditing of all policy and access decisions processed by the ICAM capability.

Environmental Sustainability

The ICAM capability shall meet Government of Canada Green Procurement policies.

Safety and Health

The following are ICAM safety and health requirements:

- The ability to meet Government of Canada and DND/CAF safety and health policies.
- Continuous Evolution;
- The ability to support insertion of new capabilities without impacting other sub-systems; and
- The ability to continually upgrade and replace ICAM services within the ICAM architecture.

Delivery Requirements. ICAM delivery requirements will be promulgated during the Definition phase of the project.

Sub-System Effectiveness Requirements

Enterprise Federated Authentication Service (EFAS)

The ICAM capability shall have the ability to federate identity with existing networks (DND/CAF, Five Eyes (FVEY), OGD, NATO, Others). Note that an EFAS (minor project) is being developed in parallel with the ICAM major project using industry standard protocols and interfaces. The ICAM major project solution will need to integrate EFAS through standard communications interfaces.

Enterprise Access Governance Service (EAGS)

The following are ICAM EAGS requirements:

- The ability to store & manage enterprise policy;
- The ability to manage logical access to networks;
- The ability to manage and integrate with physical access control systems;
- The ability to support self-service access requests;
- The ability to manage and report on compliance with policy and standards;
- The ability to provide connectors to databases, directories & service Application Programing Interfaces (APIs);
- The ability to integrate with Information Technology Service Management system in target environments;
- The ability to store & manage entitlements for the target environments;
- The ability to provide workflow and automation of requests for creation, updating and deleting of access;
- The ability to audit all transactions completed by the EAGS system in a tamperproof repository;
- The ability to track and view the provenance of identity data from creation to deletion; and
- The ability to ensure the privacy of identity data.

Enterprise Identity Data Service (EIDS)

EIDS is being developed by DND as a minor project. This service will support EFAS and the ICAM capability by collecting identity attributes, which will be used in federated authentication and access solutions. The following are ICAM EIDS requirements:

- The ability to manage access to identity data based on policy;
- The ability to ensure the integrity of identity data;
- The ability to ensure the protection of identity data;
- ICAM Cross Domain Data Transfer Services; and
- The ability to transfer all required identity information from the low side (DWAN) to high side (CSNI) in accordance with the prescribed standards and DND/CAF identity data model.

ICAM Physical Access Requirements

The DND ICAM solution will integrate with DND base/garrison physical access systems. Standards and protocols will meet industry standards to maximize the adoption of ICAM to support physical access requirements.

Training Requirements

Initial and transition training will be provided by the ICAM project to personnel who operate, administer, maintain and support ICAM services. Steady state ICAM training will be developed within the ICAM project and will be provided to new ICAM system administrators. Training frequency will be based on the rate of rotation of ICAM system administrators.

ANNEX B

ICAM SYSTEM AND ARCHITECTURE DESCRIPTIONS

ICAM As-Is Architecture

The as-is DND ICAM architecture is depicted in Figure 1. This operational view shows a siloed approach to ICAM, identities, credentials and access controls are disconnected across different enclaves and domains that exist within DND. Some inroads have been made to reduce these silos and the ICAM project will leverage current technologies and standards to provide a single digital identity and associated identity service which can be used by applications across DND networks and physical access systems.

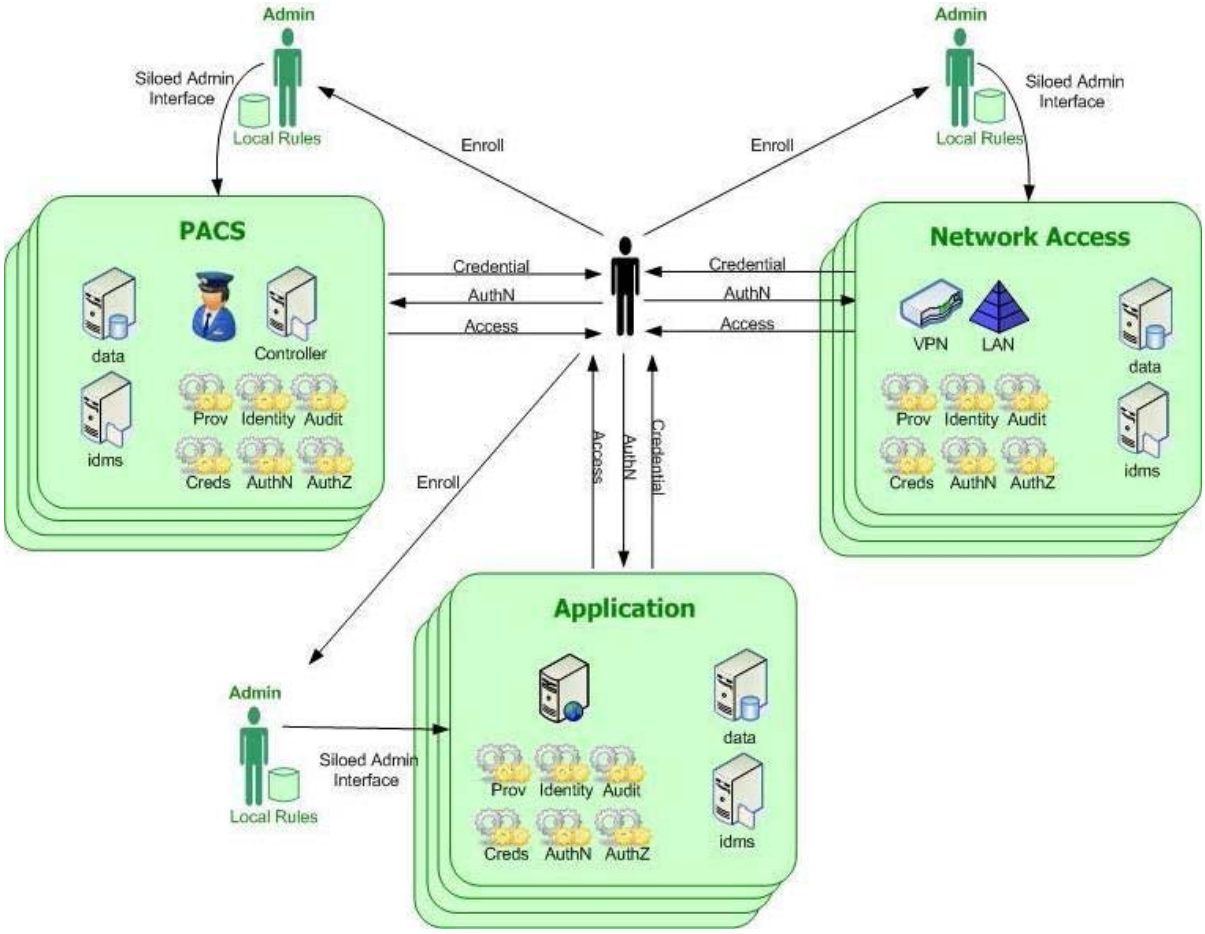

Figure 1: DND as-is ICAM *architecture, operational view*

ICAM To-Be Architecture

In the future ICAM architecture (Figure 2), each entity in the Department (person and non-person) will have a single digital identity. The ICAM capability will be centred on an identity service that uses the single digital identity for authentication and authorization decisions across the Department and to external partners. This operational architecture shows ICAM services supporting applications within the designated domain while the same service supports applications across the designated domain boundary into classified environments and federated to partner networks and applications.

Figure 2 depicts the following services:

- S-PKI (Secret-PKI) and D-PKI (DWAN PKI);
- EFAS – Enterprise Federated Authentication Service;
- EIDS – Enterprise Identity Data Service; and
- EAGS – Enterprise Access Governance Service.

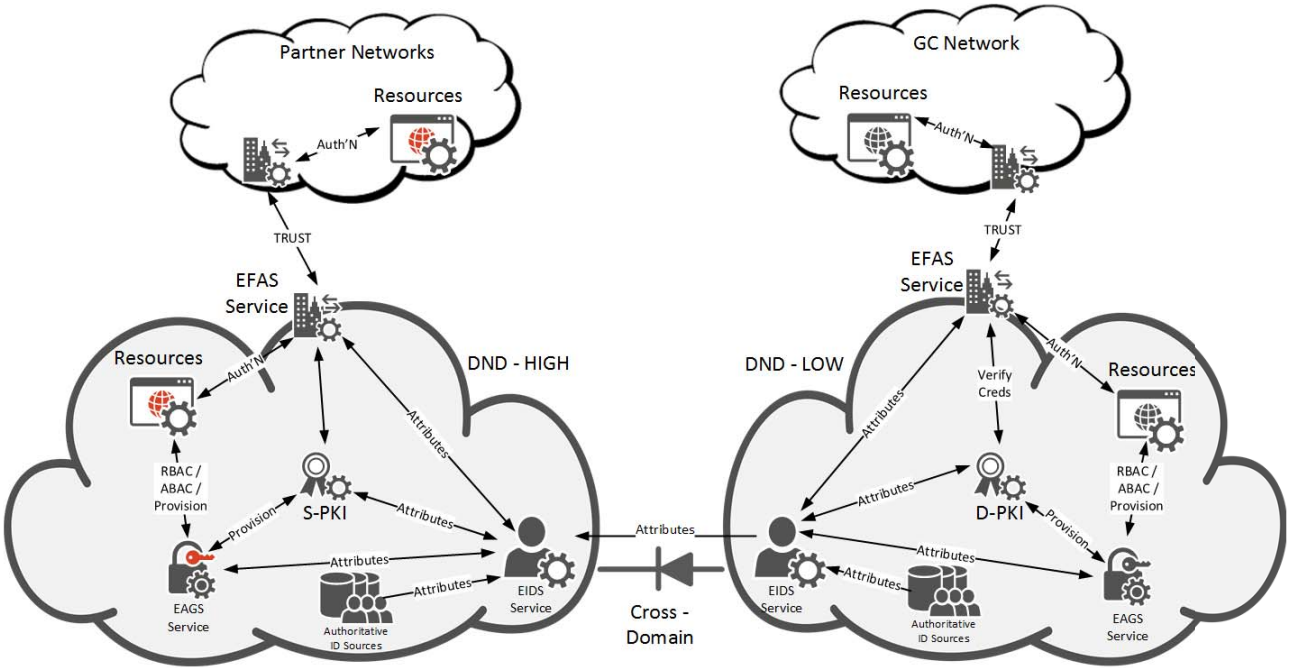

Figure 2: ICAM to-be ICAM architecture, operational view

S-PKI and D-PKI are existing services that the ICAM project will leverage and not replace. Other depicted services in Figure 2 are within scope of the ICAM project.

Enterprise Identity Data Service

The EIDS is depicted in Figure 3.

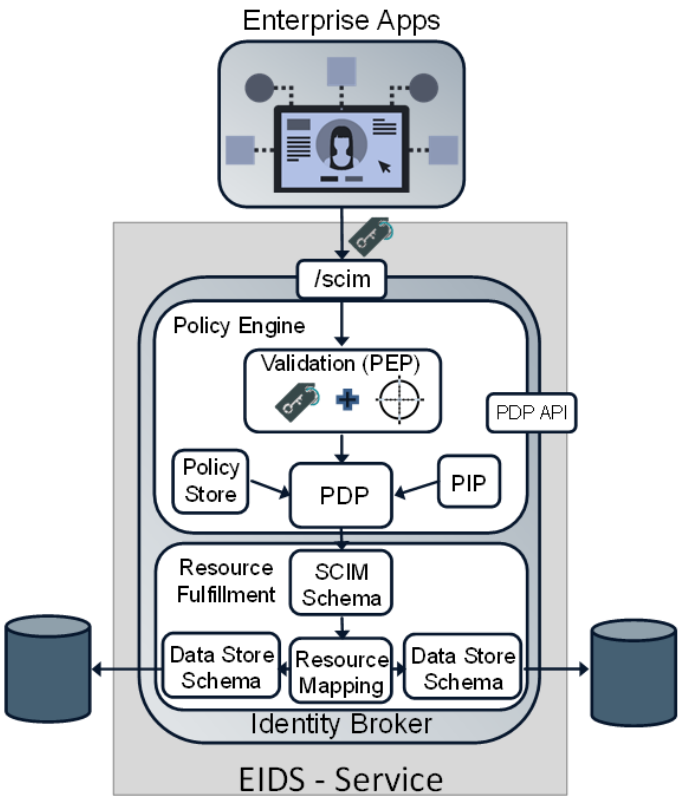

Figure 3: ICAM to-be architecture – EIDS

The EIDS is the Policy Enforcement Point (PEP)[1] that ties into the authoritative identity data. Essential to the success of implementing the EIDS service will be:

- Creation of a standardized DND Identity Data Model that includes
  - Enterprise Attributes
  - Community of Interest Attributes
  - Local Attributes;
- Identification of the authoritative sources for identity attributes
- Leveraging the System for Cross Domain Identity Management (SCIM) standard to support identity interoperability;
- Developing the policy to enable the exchange of identity data; and
- Establishment of governance to enforce defined policy.

[1] Definitions for the PEP, Policy Decision Point (PDP) and Policy Information Point (PIP) are found in the XACML open standard available from OASIS

Enterprise Federated Authentication Service

The EFAS is depicted in Figure 4.

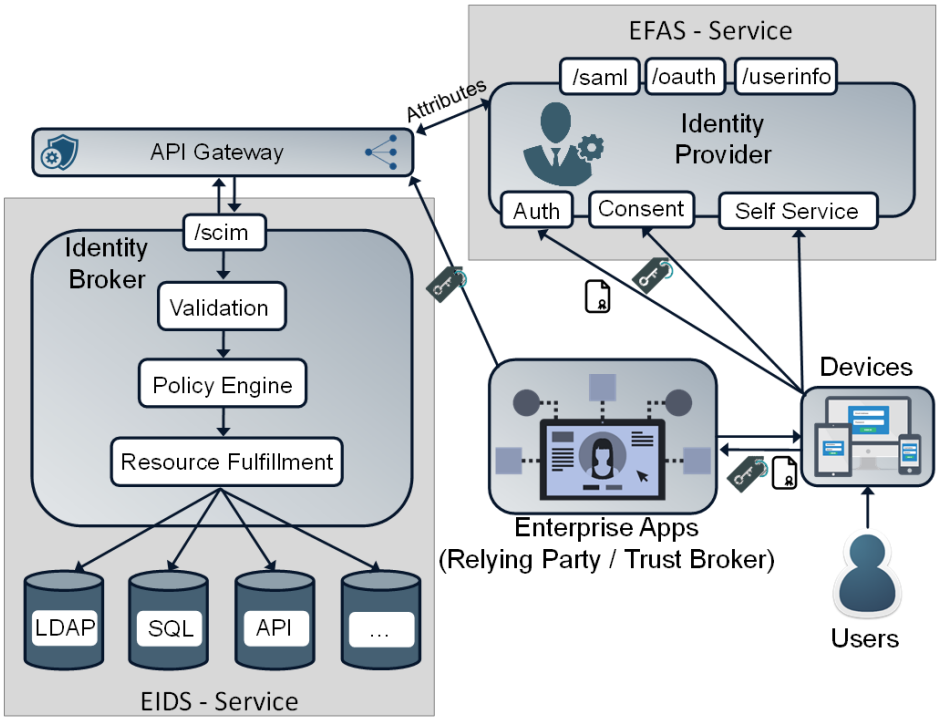

Figure 4: ICAM to-be architecture, EFAS

The EFAS acts as the identity provider. EFAS enables the use of current open standards such as SAML, OIDC, OAUTH and WS-Fed. EFAS will be adaptable to evolving standards. EFAS is the trust broker between DND, Other Government Departments and Agencies (OGDAs) and other external partners.

Enterprise Access Governance Service

The EAGS is depicted in Figure 5.

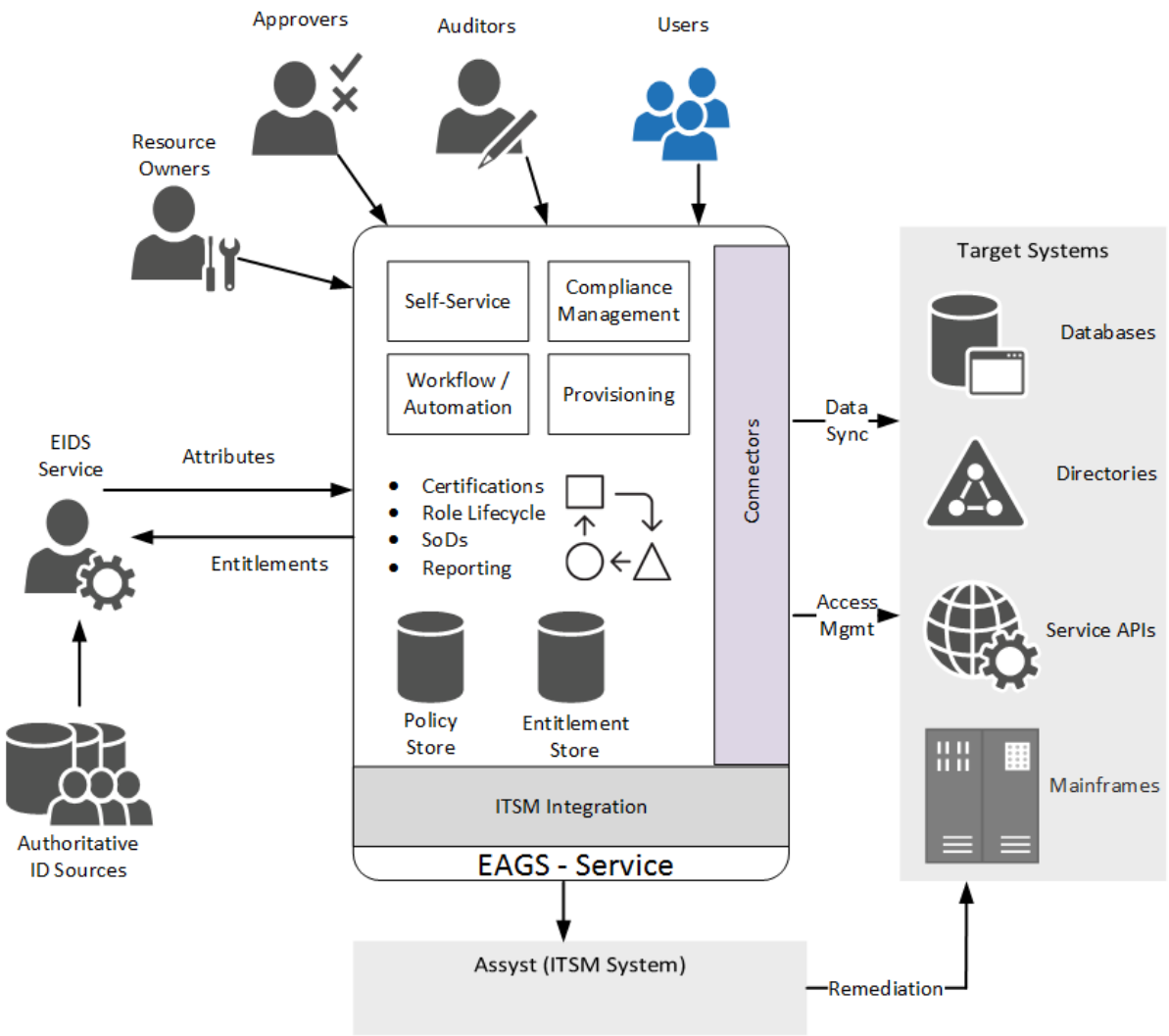

Figure 5: ICAM to-be architecture - EAGS

The EAGS will be the primary access management system for DND. As part of the ICAM capability, the EAGS will integrate with databases, directories and services requiring authentication and authorization.

ANNEX C

PRODUCT OFFERINGS AND PRICING INFORMATION RESPONSE

Supported Information

RFI participants are invited to provide non-binding confidential cost estimates for the project deliverables listed in this Annex that you have interest and experience in delivering. Partial responses are welcome.

As mentioned in Annex B, the procurement strategy is not mature yet. The level of details provided by the industry will help the Project Team finalize the Business Case Analysis.

Pricing Tables Details Information

The tables in this annex should be used by RFI respondents to provide pricing for the project deliverables, with RFI participants encouraged to include additional information on separate pages. For the purpose of this project, two (2) software products are identified, as listed immediately below and depicted in Figure 1.

<u>The ICAM software product requirements:</u>

- An identity broker that is comprised of :
    - Enterprise Identity Data Service (EIDS). A standardized policy based identity service that manages the exchange of identity data between identity information provider services and the credential and access management services that need identity information;
    - Enterprise Access Governance Service (EAGS). A standardized governance service for the management of entitlements, policies and workflows as detailed in Annex B; and
    - Enterprise Federated Authentication Service (EFAS). A standardized federated identity service for extending CAF/DND identity to GoC and Partner networks. Further described in Annex B.

<u>Integration requirements</u>

- EIDS, EAGS, EFAS and ICAM Cross Domain Data Transfer Service will need to be integrated with each other and with existing DND networks, identity repositories, credential systems and physical access control systems. The costing for integration should be broken up into a number of scenarios –
    - Integration of Authoritative Data Source with EIDS;
    - Integration of Physical resource with EAGS & EFAS – Authentication managed by ICAM capability, authorization managed by resource;
    - Integration of Physical resource with EAGS & EFAS – Authentication and authorization managed by ICAM capability;
    - Integration of Logical resource with EAGS & EFAS – Authentication managed by ICAM capability, authorization managed by resource; and
    - Integration of Logical resource with EAGS & EFAS – Authentication and authorization managed by ICAM capability.

Figure 1 shows the interaction between components of the ICAM system. The EIDS provides identity attributes, which originate in authoritative identity sources, to other ICAM services for the issuance of credentials, the control of access to local resources and control of access to external sources through federation. Figure 1 shows the requirement for ICAM services to operate synchronously in the “DND Low” (low classified) and the “DND High” (high classified) environments.

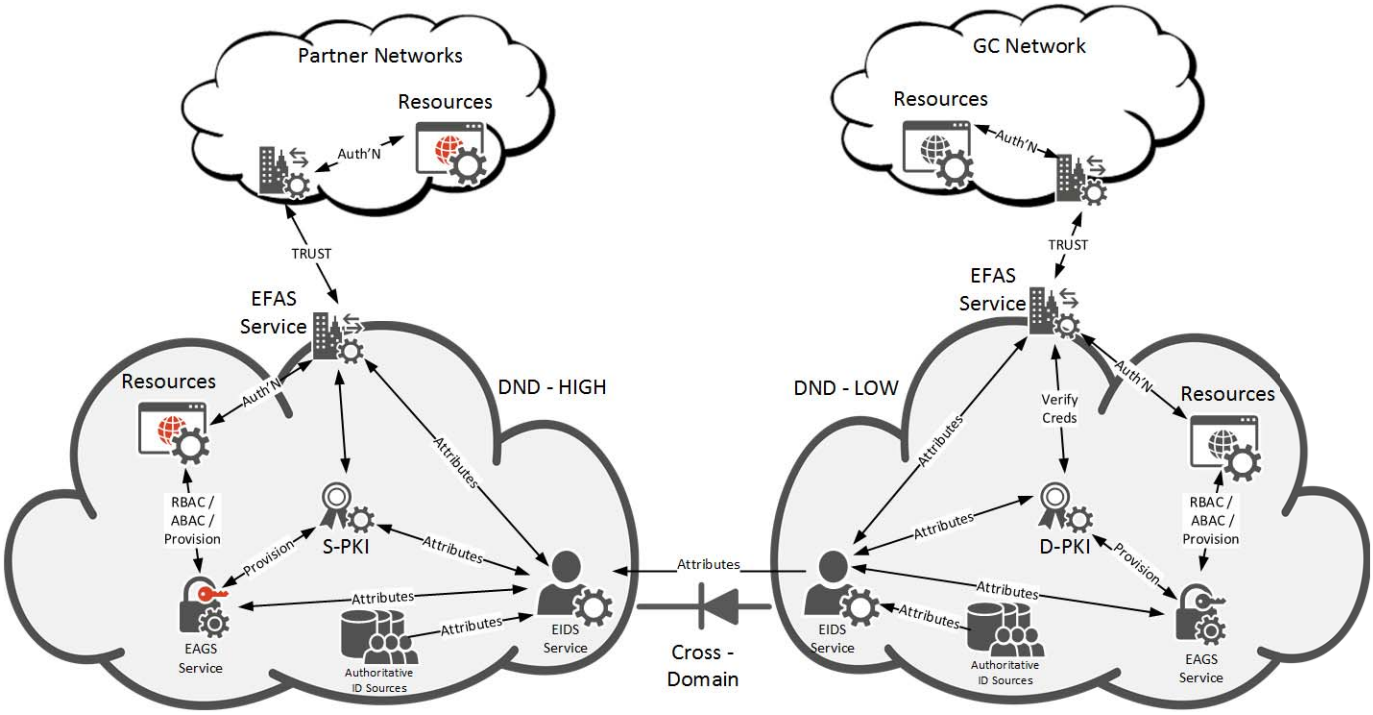

Figure 1: ICAM deliverable components shown in high level architecture

For costing purposes, the project has identified the following additional and supporting deliverables that DND believes will be needed. Deliverable supporting and sub-element pricing should consider the following:

- Hardware. Hardware required to run the ICAM software;
- Process Improvement. Required documentation of new business processes needed to enable the operation of ICAM services, including business rules, procedures and new or changed positions in the organization;
- Project Management. Project management team requirements during the project cycle for the specific deliverable elements;
- Engineering Design. Engineering design of the deliverable element. In addition to the design, this also includes configuration and testing;
- Operational Test and Evaluation (OT&E). On-site acceptance testing to ensure the deliverable element capability objectives are met in the actual production environment (large scale);
- Installation. Installation and configuration at DND sites; and
- Documentation as follows:
    - Project Work Breakdown Structure (WBS) and WBS dictionary
    - Project schedule
    - Project quality plan
    - Project risk plan
    - System Requirements Document (SRD),
    - System Engineering Plan (SEP),
    - Concept of Operations (CONOPS),
    - Service Interface Requirements (SIR),
    - System Design Specification (SDS),
    - Verification and Validation (V&V) Plan,
    - System Implementation Plan,
    - System Lifecycle Support Plan,
    - Build and configuration Documents,
    - Test reports, and

    - Troubleshooting documentation for In Service Support (ISS) (e.g., Playbook, Standing Operating Procedures SOPs).
- Training. Following training to meet DND/CAF user and support requirements for the deliverable element (note that only required training is listed in individual pricing tables) –
    - General User. Common user training for DND/CAF personnel who will use new capabilities,
    - Advanced User. Advanced user training required for “power” users (i.e., to provide local support to the executive and general user communities that would not warrant helpdesk-type support), and
    - Technical User. Technical training required for personnel who will operate, administer, maintain and support the system, both prior to activation of any new/modified Secret IT infrastructure capability and thereafter upon new personnel rotation into these functions; and
- Support. Estimated price per year to support the deliverable element after deployment.

The Description column should be used to include details on the deliverable sub-element, as applicable. For example, for data centre capabilities, specify the hardware devices (server, storage, switch, etc.) that are used for pricing. Provide multiple lines as required to account for different hardware devices.

The Total Price should list the cost for the deliverable sub-element.

All pricing is to be submitted in original currency denomination, which is to be indicated in the Currency column.

Add any additional information in the remarks section to help the project team better understand the estimated total price.

Table 1 – Identity Broker (including EIDS and EAGS)

Deliverable Sub-Elements	Description	Total Price ($)	Currency	Remarks
Hardware				
Software				

Table 2 – Enterprise Federated Authentication Service (EFAS)

Deliverable Sub-Elements	Description	Total Price ($)	Currency	Remarks
Hardware				
Software				

Table 3 – Integration

Deliverable Sub-Elements	Description	Total Price ($)	Currency	Remarks
Hardware				
Software				

Table 4 – Supporting Deliverables

Deliverable Sub-Elements	Description	Total Price ($)	Currency	Remarks
Project Management				
Process Improvement				
Engineering Design				
System Integration				
OT&E				
Installation				
Documentation				

Deliverable Sub-Elements	Description	Total Price ($)	Currency	Remarks
General and Advanced User Training				
Technical User Training				
Annual Support				

ANNEX D

RULES OF ENGAGEMENT

Introduction

These rules of engagement apply to the entire engagement process and in particular the one-on-one meetings.

General Rules and Principles

1. An overriding principle of the industry early engagement is that it be conducted with the utmost of fairness and equity between all parties. No one person or organization shall receive or be perceived to have received any unusual or unfair advantage over the others.
2. These rules of early engagement will apply beginning with the release of this RFI document and conclude with the release of the Request for Proposal (RFP).
3. The engagement process will consist of the RFI, one-on-one meetings, and a possible draft RFP(s) and any other processes deemed necessary by the Procurement Authority.
4. In order to maximize the benefits of the engagement process, Canada may endeavor to solicit comments from participants on various issues raised.
5. Any solutions, ideas or issues raised during the one-on-one sessions will be analyzed for further consideration by Canada.
6. A draft of the RFP(s), for a final review before the official RFP(s) is/are issued, may be made available to participants meeting the security requirements.
7. Canada will not disclose proprietary or commercially sensitive information concerning a participant to other participants or third parties except and only to the extent required by law.
8. 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.

Terms and Conditions

The following terms and conditions apply to the engagement process. In order to encourage open dialogue, participants agree to the following:

1. Participants are expected to discuss their views concerning the procurement, and to provide positive resolutions to the issues in question.
2. No electronic recordings, audio or visual, will be permitted during the one-on-one meetings.
3. Participants must provide to Canada advance notification if they plan to have legal representation at the one-on-one meeting. Canada reserves the right to decline any meetings which include legal representation.
4. **Participants are to direct inquiries and comments only to the PWGSC Contracting Authority or authorized representatives of Canada**, as directed in notices given by the Contracting Authority. Any communication to unauthorized representatives of Canada may be subject to full disclosure by Canada on Buy and Sell.
5. Registration is required to participate in the Industry Day(s) and is limited to potential suppliers. Industry Days are not open to the public.
6. Canada is not obligated to issue any RFP(s), or to negotiate any contract for the projects.
7. If Canada does release one or multiple RFP(s), the terms and conditions of the RFP(s) shall be subject to Canada's absolute discretion.
8. Canada will not reimburse any person or entity for any cost incurred in participating in this industry engagement process.

9. Participation is not a mandatory requirement. Not participating in this RFI engagement process will not preclude a bidder from submitting a proposal when the final RFP(s) is/are released.

10. Draft documentation (RFP(s), Evaluation Plan(s), SOW(s)) will be released to participants who meet the security requirements for comments.

11. By informal discussion and good faith negotiation, PWGSC and the participant shall make all reasonable efforts to resolve any dispute, controversy or claim, arising out of or in any way connected with this industry engagement.

ANNEX E

INDUSTRY DAY and ONE-ON-ONE MEETING DETAILS AND REGISTRATION

Industry Day

All interested industry respondents are invited to attend an Unclassified group presentation to industry that will be conducted in Ottawa, ON. This industry day will allow DND project staff to present an overview of the project and to obtain industry input, and allow industry to ask questions to PSCP, CISD, DND and ISED. The industry day will be conducted at the Unclassified level. Suppliers who do not attend the industry day are still welcome to submit a response to this RFI.

Industry Day Details:

Date: Monday, 22 July 2019

Time: 9:30 – 12:00

Location: The Rideau Canal Junior Ranks Mess - Palladium Room,
4 Queen Elizabeth Drive, 3rd floor Ottawa, ON

Registration Deadline: 15 July 2019. Suppliers are requested to register by the Registration deadline.

Please arrive thirty minutes prior to industry day start time in order to facilitate sign-in. Attendees are responsible for their own transportation, accommodation, meals, parking and all other expenses.

WebEx: This event will also be available via WebEx at the date and time listed above. Suppliers who would like to register to attend via WebEx are requested to send an email to: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca to register.

One-On-One Meetings

The intention of the one-on-one meetings is to hold discussions with Industry.

Suppliers are advised that although discussions at the one-on-one meetings will provide more granularity of DND requirements, they are not required to provide a fulsome response to the RFI. Suppliers are not required to attend a one-on-one meeting. Suppliers who do not attend are still welcome to submit a response to this RFI.

One-on-one meeting details:

Format: One hour time slots allocated per Supplier

Period: 22 – 24 July 2019

Available timing:

- 22 July 2019, 1300 - 1630 hrs
- 23 July 2019, 0800 - 1600 hrs
- 24 July 2019, 0800 - 1600 hrs

Location: The Rideau Canal Junior Ranks Mess – Athena Room,
4 Queen Elizabeth Drive, 3rd floor Ottawa, Ontario

Registration Deadline: 15 July 2019. Suppliers are requested to register by the Registration deadline. Should suppliers not register by the deadline, a meeting will not be guaranteed. Registration for one-on-one meetings will be conducted on a first come first serve basis, however, DND and supplier availability, will affect the scheduling of the meeting dates.

Suppliers are requested to arrive fifteen minutes prior to their meeting time in order to facilitate sign-in. Attendees are responsible for their own transportation, accommodation, meals parking and all other expenses.

One-On-One Meeting and Industry Day Registration Process

To register, suppliers **must submit** to the PWGSC Contracting Authority identified below the following:

- Number of people to attend the Industry Day and/or one-on-one meeting
- Point of contact email and phone number
- Language of preference: English or French (for one-on-one meetings)

Please note that:

- due to the space constraints of the location each interested supplier may only register **up to four (4) representatives** to attend the Industry Day and one-on-one meeting; and

- the names of all attendees may be published;

Contracting Authority for the Industry Day and One-on-One Meetings:

Attn: Chantale Norris or Patrick Scott
Public Works and Government Services Canada
Place du Portage III, 8C2
11 Laurier, Gatineau, Canada K1A 0S5

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

The use of email to communicate is preferred.

Information Prior to Industry Day and the One-On-One Meetings

Suppliers may provide comments or questions in writing in either official language to the Contracting Authority identified above.

By participating in the Industry Day and one-on-one meeting, attendees agree to the rules of engagement detailed in Annex D.

Communication with Industry

Canada will document all industry day concerns/issues, questions, suggestions, together with their responses. During the engagement process, the PWGSC Contracting Authority may choose to communicate with registered suppliers through direct email rather than posting additional notices on Government Electronic Tendering Service. To ensure the fairness, transparency and integrity of the Process, PWGSC will share information resulting from the process (excluding proprietary and/or confidential information) with Industry.

The presentation made by Canada, responses to questions raised during the industry day, and the list of attendees will be published on the Government Electronic Tendering Service after the event.

Language

Documents will be available in both official languages.

ANNEX F

REQUEST FOR SECURITY SPONSORSHIP

INTRODUCTION

As the draft RFP(s), final RFP(s) and resulting contract may contain Classified information, one of the key purposes of this RFI is to provide direction and assistance to interested suppliers who do not meet the security requirements in obtaining required security clearances.

SPONSORSHIP REQUEST FOR SECURITY CLEARANCE

Suppliers whose organizations will require valid clearances issued by the Canadian Industrial Security Directorate (CISD) are encouraged to initiate the security clearance process as soon as the Security Clauses are finalized via an RFI Amendment posted on Buy and Sell. Requests for sponsorship can be sent to the PWGSC Contacting Authority below via e-mail.

Prime Contracting Authority for Security Sponsorship:

Chantale Norris or Patrick Scott
Public Services and Procurement Canada (PSPC)
Place du Portage III, 8C2
11 Laurier, Gatineau, Canada K1A 0S5

TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

The use of email to communicate is preferred.

It is the responsibility of the Supplier to ensure that the information required concerning the security clearance is provided on time to either the requesting authority or CISD. The request should include the following information:

a. legal name of the company;
b. business name, if different from legal name;
c. mailing address;
d. civic address, if different from mailing address;
e. company telephone number;
f. surname and given name of the contact person (Canadian official);
g. title of the contact person;
h. telephone number of the contact person;
i. e-mail address of the contact person; and
j. language preference (English or French).

Upon receipt of a request for sponsorship, CISD will contact the supplier to complete the gathering of required information.

For any inquiries concerning any security requirements, the supplier should contact CISD at 866-368-4646, or (613) 948-4176 in the National Capital Region. CISD Website: http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html

There are no direct costs charged to suppliers wishing to obtain a Facility Security Clearance (FSC). However, the suppliers may incur indirect costs from being required to meet the minimum standards such as installing mechanisms for document safeguarding, if applicable.