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
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.\11, rue Laurier
Gatineau
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Comments - Commentaires

Issuing Office - Bureau de distribution
Business Transformation and Systems Integration
Service/Division de transformation des opérations et d'intégrat
Special Procurement Initiative Dir
Dir. des initiatives speciales d'approvisionnement
Terrasses de la Chaudière 4th Floo
10 Wellington Street
Gatineau
Québec
K1A 0S5

Title - Sujet Request for Information (RFI) Identity Services and Access Management Solution (iSAMS)	
Solicitation No. - N° de l'invitation G9292-227767/A	**Date** 2021-05-16
Client Reference No. - N° de référence du client G9292-227767	**GETS Ref. No. - N° de réf. de SEAG** PW-$$XE-677-39483
File No. - N° de dossier 677xe.G9292-227767	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-06-23 Heure Avancée de l'Est HAE

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

Address Enquiries to: - Adresser toutes questions à: Heather Wilson	**Buyer Id - Id de l'acheteur** 677xe
Telephone No. - N° de téléphone (819) 639-0671 ( )	**FAX No. - N° de FAX** ( ) -

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

Specified Herein
Précisé dans les présentes

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée See Herein – Voir ci-inclus	**Delivery Offered - Livraison proposée**

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

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

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

Signature **Date**

Canada

Destination Code - Code destinataire	Destination Address - Adresse de la destination	Invoice Code - Code bur.-comptable	Invoice Address - Adresse de facturation
D - 1	NCR - Gatineau RCN - Gatineau 140 Promenade du Portage GATINEAU QC J8X 4B6 CANADA	I - 1	ESDC Comptes Payable Montreal 200 Rene-Levesque Blvd. West Guy Favreau Complex, West Tower Montreal QC H2Z 1X

Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM Destination	Plant/Usine	Delivery Req. Livraison Req.	Del. Offered Liv. offerte
1	iSAMS 9200 Initiation	D - 1	I - 1	1	Each	$	$	See Herein – Voir ci-inclus	

Identity Services and Access Management Solution (iSAMS)

Request for Information No. G9292-227767/A

Introduction

The purpose of this Request for Information (RFI) is to solicit comments and feedback from industry and potential respondents concerning the draft Identity Services and Access Management Solution (iSAMS) Statement of Work and its appendices, including the iSAMS Requirements Workbook; the iSAMS Conformance Criteria Workbook; and the Client Identity and Access Management Legacy at ESDC and Characteristics of Target Solution for iSAMS. This RFI also includes a series of questions to industry. Comments and feedback received from industry as a result of this RFI will help Canada refine and finalize the draft documents for the iSAMS procurement. Suppliers are encouraged to provide information that they feel would improve the documents and the procurement process as a whole.

Background

Employment and Social Development Canada (ESDC) is seeking an Enterprise Identity Services and Access Management Solution (iSAMS) that delivers a single secure access point to ESDC programs and services for identity registration and authentication in real-time. The Enterprise Cyber-Authentication Solution (ECAS) system that is currently being used to register and authenticate identity for external clients is unable to meet the medium and long-term requirements for ESDC's Benefits Delivery Modernization (BDM) transformation objectives. The iSAMS will replace ECAS and provide a single secure access point to ESDC programs and services. The iSAMS will also provide increased functionality to onboard additional programs and add new capabilities to respond to emerging business requirements. The BDM Programme will depend on iSAMS to successfully deliver on current and future authentication requirements, both in terms of increased volume and additional functionality.

With the iSAMS, ESDC is looking to expand their Identity, Credential and Access Management ("ICAM") capabilities. The strategic purpose of ISAMS is to establish a modern and secure digital identity ecosystem as a key enabler of seamless and frictionless service delivery to BDM clients.

The iSAMS must be compliant with the Public Sector Profile of the Pan-Canadian Trust Framework (PCTF) and the Standard on Identity and Credential Assurance.

- Public Sector Profile of the PCTF Version 1.1 (dated 2020-06-02): https://canada-ca.github.io/PCTF-CCP/PCTF.html
- In addition, the iSAMS must comply with the conformance criteria of the Public Sector Profile of the PCTF, at Level of Assurance 2 (LOA 2) or higher. These conformance criteria can be found in *Appendix 4 to Annex A – Conformance Criteria of the Public Sector Profile of the Pan-Canadian Trust Framework (PCTF).*
- While compliance with the Public Sector Profile of the PCTF Version 1.1 (dated 2020-06-02) is mandatory for the iSAMS, there are specific conformance criteria that may be optional (e.g., are designated "should"). The designations defined in the conformance criteria will take precedence in these cases.
- Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32612

iSAMS Benefits and Goals

Anticipated benefits associated with the iSAMS are:

- Modernized registration and authentication process resulting in increased client satisfaction (both citizens and agents)
- Potential increased scalability with the potential to expand beyond ESDC
- Enhanced security
- Alignment with new functionalities delivered by the BDM Programme
- Conversion of approximately 200,000 plus paper bound transactions to the digital channel for delegates
- Reduced number of clients that are pushed to offline channels via adaptive authentication

iSAMS Value Proposition

Users	Integrity	Programs and Services	Client Service Benefits	Internal
• User centric - empower Users with control over their digital assets • Let Users choose their sign-in option • Reduce Users' response burden upon consent • Leverage mobile devices • Privacy sensitive design • Enables immediate service delivery - removal of the need for snail mail-based PAC / AC through simplified registration process	• Enable up-front process controls • Reduce costs of Identity Proofing • Accelerate e-services and their adoption • Full audit capabilities • Enable electronically verifiable claims to streamline the provision and verification of proof documentation	• Reduce agent-facing work items and adjudication costs • Increase e-services and their adoption • Align with Government of Canada policies, guidance, and initiatives • Enable service transformation • Privacy and security sensitive design • More risk management options	• Streamline Client experience • Channel differentiation • Cross channel support • Mobile device enabled • Enable service bundles • Respect Users' privacy and time	• Align with modern IT architecture and practices • Standards based • Enable development and maintenance of controls and processes across multiple program domains • Streamline integration requirements through standardization of interfaces and processes • Reduce complexity and co sts • Reduce risks associated with "honey pots" of client data

The iSAMS will modernize ESDC's security posture and introduce new functionality designed to:

- Introduce alternatives that would enable Clients to gain real time access to their accounts without needing to wait for physical mail-based access codes. This is expected to increase adoption of the eservices channel.
- Reduce Agent facing work items by enabling Clients to electronically manage their delegates (who can act on their behalf with ESDC). This functionality has the capacity to migrate over 200,000 currently paper bound work items from agents to online self-service.
- Introduce adaptive authentication that moves the department away from the current one size fits all authentication process and instead makes the Client facing authentication process a function of the risks presented by the transaction. This functionality has the potential to keep many Clients that are currently directed to offline channels to stay in the eservices channel by more effectively managing risks through step up authentication requests.
- Introduce a globally unique identifier that will be assigned to all and can be used to return the Social Insurance Number to its rightful place as a program identifier.

Appendix 3 to Annex A – Client Identity and Access Management Legacy at ESDC and Characteristics of Target Solution for iSAMS intends to provide the suppliers with the insights required to understand ESDC's context and to recommend a deployment model for the iSAMS in context of ESDC's:

- Legacy systems at ECAS, My Service Canada Account (MSCA) , My Service Canada Business Account (MSCBA);
- Desired characteristics of the target state iSAMS; and
- Anticipated release schedule and the anticipated iSAMS deployment timeline governing what feature functionality will be introduced and when.

Security Requirements Associated with the RFI

There are no security requirements associated with this RFI.

Anticipated Security Requirements Associated with the proposed RFP

Canada anticipates that the Security Requirements included at Attachment 2 will apply to the proposed RFP.

Supply Chain Integrity Process

Canada anticipates that the Supply Chain Integrity Process described in Attachment 4 will apply to this requirement.

Accessible Procurement

Public Services and Procurement Canada (PSPC)'s goal is to ensure that the goods and services the Government of Canada (GC) buys are inclusive by design and accessible by default. Considering accessibility in public procurements is now an obligation in the Treasury Board Contracting Policy and, accessibility criteria must be included in the requirements for goods and services, where appropriate.

Reply to the Request for Information

Comments, suggestions and any other feedback are requested to be provided via e-mail to the PSPC Contracting Authority at TPSGC.DGAMVP-ABBDM.PWGSC@TPSGC-PWGSC.GC.CA, **on or before 2:00 PM (Eastern Daylight Time) on Monday, May 31, 2021.**

Each supplier should ensure that its name and return address are provided and that the RFI number appears in the subject line of the email. Each supplier is solely responsible for ensuring its feedback is delivered on time via email to the Contracting Authority.

Suppliers are not required to provide formal proposals in response to this RFI. Suppliers should explain any assumptions they make in their replies. Any marketing or promotional information submitted as part of any reply may not be reviewed. Responses will not be used for competitive or comparative evaluation purposes; thus, the reply format is not as rigorously defined as would normally be for an RFP.

Canada does not intend to have in-person meetings as a result of this RFI nor does Canada commit to providing a response to any of the feedback or questions posed to Canada as part of this feedback. However, Canada will consider all feedback received in reply to this RFI. Feedback received after the close of this RFI may still be considered during the development of draft solicitation documents.

Canada will not reimburse any supplier for expenses incurred in responding to this RFI.

Questions Associated with the Requirement

1. **Company Information:**
   a. Provide an overview of your Identity, Credential and Access Management product and services portfolio.

2. **Solution Information:**
   a. Canada is interested in understanding the Vendor's capabilities and offerings as they relate to deployment models, specifically: Cloud (implementing a Protected B, Medium integrity, Medium availability (PBMM) profile - see reference link below for more details), Hybrid and On-Premise deployment models. Please describe the recommended deployment model for your Identity, Credential, and Access Management Solution and explain why.

      Cloud Model: Solution deployment in the cloud hosted on a Protected B Platform.

      - Reference link:
        - https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html

      Hybrid Model: Solution deployment is a combination of On-Premise and Cloud with capabilities to meet specific, modular needs.

      On-Premise Model: Solution is hosted on the customer's premise with customer control of deployment and maintenance.

   b. The intent of the *Appendix 3 to Annex A – Client Identity and Access Management Legacy at ESDC and Characteristics of Target Solution for iSAMS* is to provide additional context for the suppliers that might help them to propose a deployment model that best fits Canada's needs. Does this document include the required information to recommend a deployment model (on premise vs. Cloud vs. hybrid model)? If "No", please explain what information can be clarified or added.

   c. What infrastructure (if any), services or additional support is required to support your Identity, Credential, and Access Management Solution over the contract periods, including if Canada chooses to scale the solution within ESDC or to other Government of Canada organizations?

   d. Please specify whether the proposed solution will be hosted on physical or virtual servers.

3. **What is the pricing model for your Identity, Credential, and Access Management Solution?**
   a. Is your pricing model based on:
      i. Number of concurrent sessions; please describe as required
      ii. Number of transactions/logged events; please describe as required
      iii. Number of authenticated external clients; please describe as required
      iv. Per CPU with bands of the number of external clients per CPU; please describe as required
      v. Data volume (e.g., Gigabytes per day); please describe as required
      vi. If your pricing model is based on licensing, what is your license type? (e.g. subscription, perpetual, other?)
      vii. Other; please describe

   b. Please provide the following information to support an understanding of the relevant technology cost factors for your Identity, Credential, and Access Management Solution and total cost of ownership:

i. Initial infrastructure requirements (if any) such as hardware, networks storage, and other components required to create an operating environment for your solution); please describe as required.
ii. Are there any initial licensing fee, connection, start-up costs? Please described as required.
iii. Are there any costs for development licenses?
iv. Are there anticipated future expenditures for asset lifespan / replacement schedule (if applicable); please describe as required.
v. Are there any assumptions related to cost increases over the contract periods? Please describe as required.

c. Provide a detailed description of your pricing model; including any changes to pricing based on the volume of authenticated external clients, volume of concurrent external clients, number of CPUs or other basis.

d. Canada is targeting a 5-year contract with five 1-year optional years. Are there are any concerns with the proposed contract period? Please comment as required.

e. Please provide any other relevant information to support understanding of your costing model and associated costs to Canada.

4. Are Canada's requirements clearly communicated? Answer by "Yes" or "No" to the following questions, and provide an explanation as required.

a. Are the sources and documents referenced in the SOW and the requirements workbook clearly communicated? If "No", please explain what changes are required to further clarify.

b. Are the compliance requirements of the Government of Canada and industry's policies, standards, guidelines and trust frameworks clear? If "No", please explain what further clarifications are required.

c. If applicable, please describe what needs to be clarified in the Annex A, Statement of Work to be able to bid on the proposed RFP, and how it can be clarified.

d. If applicable, please describe what needs to be clarified in the requirements workbook *Appendix 2 to Annex A, Functional and Non-Functional Requirements* to be able to bid on the proposed RFP, and how it can be clarified.

5. Supplier's ability to respond to the proposed RFP based on the current mandatory requirements (functional and non-functional)?

a. Would the mandatory functional and non-functional requirements prevent you from bidding on the proposed RFP? If "Yes", please detail which requirements would prevent you from responding to the proposed RFP with supporting rationale.

b. Describe what additional changes (if any) are required to enable you to bid on the proposed RFP.

c. In case the requirement is not updated, indicate if you plan to submit a bid for the proposed RFP.

6. Do the requirements clearly translate the desired outcomes of the iSAMS for Canada?

a. Do the draft Functional and Non-Functional requirements clearly communicate that Canada is seeking an adaptive authentication solution (i.e., make authentication requirements a function of the risk presented by the transaction)? Please elaborate if required.

b. Do the draft Functional and Non-Functional requirements clearly communicate that Canada wants to empower Clients by providing them with control over their Personal Information without compromising security or privacy? Please elaborate if required.

c. Do the draft Functional and Non-Functional requirements clearly communicate that Canada wants to enable the electronic delegation of authority by removing the need for paper-based delegation processes? Please elaborate if required.

d. Do the draft Functional and Non-Functional requirements clearly communicate that Canada wants to minimize breach risks associated with the iSAMS while providing a client centric eservices experience? Please elaborate if required.

7. Solution Scalability:

ESDC will depend on iSAMS to successfully deliver on current and future authentication requirements for the Department. However, the Department, in conjunction with other Government of Canada departments, is seeking information on whether the solution could be used by other Departments - scaling the solution to programs and services outside of ESDC to allow for clients ID proofed at the enterprise level to access any services across departments that fit the level of ID proofing already completed. To this end, ESDC is seeking industry feedback on the following questions:

a. What infrastructure (if any), services or additional support would be required to support your proposed solution if Canada chooses to scale the solution to other Government of Canada organizations? Which components would be common? Please describe whether you recommend a centralized or distributed system and explain why.

b. What other considerations should Canada consider in order to scale from a solution supporting one Department to many?

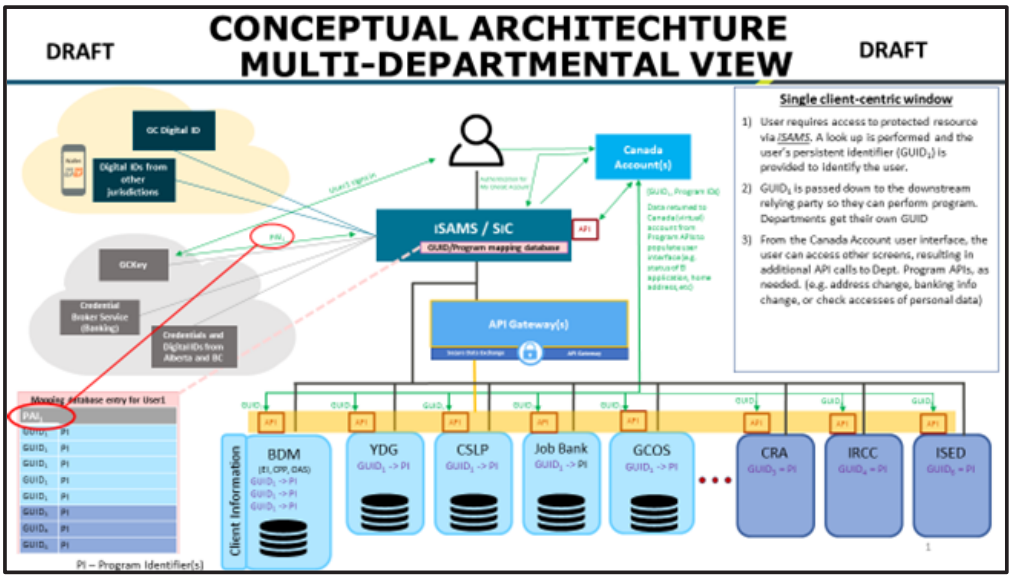
c. What additional information (if any) could Canada provide to Suppliers to allow you to describe how your solution could be scaled in such a way to minimize cost, complexity (including configuration) and maintain a common customer experience across Departments?

d. What variables would you need to understand in order to provide insight into pricing models for scalability either across Departments or as a centralized service?

e. Is there additional information Canada should request to ensure interoperability across the digital identity ecosystem which includes the Government of Canada's online services (relying parties), required credentials (Credential Service Providers), and Identity Providers?

f. When considering the federation of identity beyond ESDC, is there sufficient information in this package to ensure the continued use of open standards (OIDC, SAML, OAuth) and compliance to the Cyber Authentication Technical Specifications (CATS)?

The following diagram is intended as a high level, conceptual view of what an Identity Management system supporting multiple departments could look like. It is intended to primarily show a draft future state that will support an improved client experience across multiple departments.



8. **Is there any other information that Canada should consider?**
   a. Please provide any other recommendations or additional comments.

Note to Interested Suppliers

This is not a bid solicitation. This RFI will not result in the award of any contract; therefore, potential suppliers of any goods or services described in this RFI should not earmark stock or facilities, nor allocate resources, as a result of any information contained in this RFI. 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.

The draft Identity Services and Access Management Solution (iSAMS) Statement of Work, and its appendices including the iSAMS Requirements Workbook; the iSAMS Conformance Criteria Workbook; and the Client Identity and Access Management Legacy at ESDC and Characteristics of Target Solution for iSAMS, may potentially be modified as a result of this RFI process, and any finalized solicitation documents will be posted on the Government Electronic Tendering System (GETS) at a future date. Canada is issuing the drafts on GETS to help ensure it benefits fully from industry feedback prior to finalizing the solicitation documents. Through this RFI process, Canada intends to seek feedback in writing only.

Suppliers are advised that any information submitted to Canada in reply to this RFI may be used by Canada in the development of a subsequent competitive solicitation. Canada reserves the right to accept or not accept the input from industry, as well as alter, amend, delete or add, in whole or in part, any terms or provisions to or from the draft documents.

The issuance of this RFI does not create an obligation for Canada to issue a subsequent solicitation, and does not bind Canada legally or otherwise, to enter into any agreement or to accept any suggestions from respondents to this RFI. Participation in this RFI is not a condition or prerequisite for participation in any future procurement. The award of any contract resulting from any future procurement will be consistent with contracting policies, laws and regulations applicable to government contracting and applicable national and international trade agreements.

Non-Disclosure Agreement and Reference Material

Canada does not intend to make the draft Identity Services and Access Management Solution (iSAMS) Statement of Work, including the iSAMS Requirements Workbook; the iSAMS Conformance Criteria Workbook; and the Client Identity and Access Management Legacy at ESDC and Characteristics of Target Solution for iSAMS, publicly available. All suppliers who wish to gain access to these documents must send via e-mail to the PSPC Contracting Authority at TPSGC.DGAMVP-ABBDM.PWGSC@TPSGC-PWGSC.GC.CA:

- Attachment 1 – Non-Disclosure Agreement (NDA), signed by an authorized representative of the supplier.

Following receipt of the signed NDA the PSPC Contracting Authority will provide access to the reference documents via epost connect.

Requested Format of Replies

Cover Page: If the feedback includes multiple volumes, suppliers are requested to indicate on the front cover page of each volume; the title of the feedback, the Request for Information number, the volume number and the full legal name of the supplier.

Title Page: The first page of each volume of the feedback, after the cover page, should be the title page, which should contain:

a) the title of the supplier's feedback and the volume number;

b) the name and address of the supplier;

c) the name, address and telephone number of the supplier's contact;

d) the date; and

e) the RFI number.

Numbering System: For replies to the 'Questions Associated with the Requirement" section of this RFI, suppliers are requested to prepare their feedback using a numbering system corresponding to the one in this RFI. All references to descriptive material, technical manuals and brochures included as part of the reply should be referenced accordingly.

Body: Suppliers are requested to clearly identify the section of the draft document to which the feedback pertains. The feedback should be labelled with the date and the supplier's name on each page, and pages should be sequentially numbered. It is preferred that all pertinent information be included in the feedback without the need to visit supplier websites. If necessary, however, website references may be provided for additional information, beyond that requested in this RFI. If this is the case, it should be noted that the information contained in such websites may not be used for the analysis of the feedback to this RFI.

Treatment of Feedback

1. **Use of Feedback**: Feedback will not be evaluated. However, the feedback received may be considered by Canada to refine any draft solicitation documentation. Canada will consider all feedback received in reply to this RFI.

2. **Review Team:** A review team composed of Government of Canada (Canada) representatives (including ESDC and PSPC) will review the feedback. Canada reserves the right to retain independent consultant advisors (who will be subject to confidentiality provisions or nondisclosure agreements), or use any Government resources that it deems necessary to review any feedback. Not all members of the review team will necessarily review all feedback.

3. **Confidentiality**: Suppliers should mark any portions of their feedback that they consider proprietary or confidential. Canada will treat those portions of the feedback as confidential to the extent permitted by the *Access to Information Act*.

4. **Clarifications**: Canada may, at its discretion, contact any suppliers to follow up with additional questions or for clarification of any aspect of feedback.

Fairness Monitor

To ensure the openness, fairness, transparency and integrity of the procurement process, a third-party fairness monitor has been engaged from the beginning of the process and will continue to be engaged for the entire process of this multi-phased procurement, including the RFI. The fairness monitor services are provided by: *Samson & Associates*.

Enquiries

All enquiries and other communications related to this RFI shall be directed to the BDM mailbox at: TPSGC.DGAMVP-ABBDM.PWGSC@TPSGC-PWGSC.GC.CA

Contracting Authority

Heather Wilson
Public Services and Procurement Canada
Acquisitions Branch
10 Wellington Street
Gatineau, Québec KIA 0S5

E-mail Address: TPSGC.DGAMVP-ABBDM.PWGSC@TPSGC-PWGSC.GC.CA
Telephone: 819-639-0671

ATTACHMENT 1

NON-DISCLOSURE AGREEMENT (NDA)

HER MAJESTY THE QUEEN IN RIGHT OF CANADA ("CANADA"), AS REPRESENTED BY THE MINISTER OF PUBLIC SERVICES AND PROCUREMENT CANADA

AND

_____

Supplier's legal name

_____

Supplier's address

The supplier signing this NDA is signing on its own behalf and on behalf of all supplier representatives (herein after referred to as "Participants") that may have access to the reference material from the RFI G9292- 227767/A. The onus is on the supplier to ensure that all Participants are aware of this NDA and that they will respect and act in accordance with its terms and conditions.

The reference material contains information that is sensitive and/or proprietary to Canada or to a third party (herein after referred to as "Sensitive Information") that is not to be disclosed or used in any way other than as set out below.

1. The supplier, as well as all Participants, agree:

   a) they must not, without first obtaining the written permission of the Contracting Authority, disclose to anyone, other than Participants, the Sensitive Information;

   b) they must not make copies of the Sensitive Information or use it for any purpose other than for the preparation of a reply to the Request for Information (RFI) G9292-227767/A;

   c) they will require any Participant to execute a NDA on the same conditions as those contained in this NDA. If requested by the Contracting Authority, the supplier must provide the Contracting Authority with a copy of all NDA(s) signed by the supplier and Participants;

   d) that they will be liable for any and all claims, losses, damages, costs or expenses incurred or suffered by Canada caused by the failure of the supplier or Participants, or by anyone to whom the supplier or Participants discloses the Sensitive Information, to comply with these conditions;

   e) should any unauthorized disclosure or use of the Sensitive Information be made by the supplier, Participants, or by anyone to whom the supplier or the Participants disclose the Sensitive Information, the supplier or Participants will: (i) immediately notify the Contracting Authority of same; (ii) take all reasonably necessary steps to prevent further unauthorized access and/or use; and (iii) cooperate with Canada in its efforts to secure the Sensitive Information and protect the proprietary rights of the owner of the Sensitive Information;

   f) in the event the Sensitive Information must be disclosed pursuant to judicial order or requirement of law, the supplier or Participants shall take reasonable steps to notify the Contracting Authority of such order or requirement; and

   g) Canada, or the third party, as the case may be, shall retain title to the Sensitive Information, and all copies thereof. Except for the limited use of the Sensitive Information authorized herein, no copyright, patent, trademark, trade secret or other intellectual property rights are granted to the supplier or Participants.

2. Canada is providing the Sensitive Information “as is”. The supplier and Participants acknowledge and agree that Canada will not be liable for any damages arising out of the use of the Sensitive Information. Disclosure of the Sensitive Information containing business plans or relating to products under development or planned for development is for planning purposes only. Canada may change or cancel its plans at any time. Notwithstanding the foregoing, Canada warrants the accuracy of the Sensitive Information to the best of Canada’s knowledge and belief.

3. Nothing in this NDA should be construed as limiting the supplier's or Participants’ right to disclose any information to the extent that such information:
   a) is or becomes in the public domain through no fault of the supplier, Participants or anyone to whom the supplier or Participants disclose the Sensitive Information;

   b) is or becomes known from a source other than Canada, except any source that is known to the supplier or Participants to be under an obligation to Canada not to disclose the information;

   c) is independently developed by the supplier or Participants; or

   d) is disclosed under compulsion of a legislative requirement or any order of a court or other tribunal having jurisdiction.

4. General:
   a) Headings included in this Agreement are for convenience only and are not to be used to interpret the agreement between parties;

   b) If any part of this Agreement is held unenforceable or invalid, the remaining provisions shall continue in full force and effect;

   c) Neither party may assign its rights or delegate its duties or obligations under this Agreement without the prior written consent of the other party. Any attempt to do so is void;

   d) Only a written agreement signed by authorized representatives of both parties can modify this agreement; and

   e) This agreement shall be deemed to have been made in and shall be governed by and construed in accordance with the laws of the Province of Ontario.

The parties acknowledge they have read this agreement, understand it, and agree to be bound by its terms and conditions. Further, they agree that the complete, exclusive and final statement of the agreement between the parties relating to this subject shall consist of this agreement only.

By signing this document, the authorized signatory represents that he/she has full authority to bind the supplier as well as Participants and that the supplier and Participants agree to be bound by all the terms and conditions contained herein.

Full name of supplier’s authorized signatory	Title of supplier’s authorized signatory
Email of supplier’s authorized signatory	Telephone # of supplier’s authorized signatory
Signed by its authorized signatory	Date

ATTACHMENT 2

SECURITY REQUIREMENTS

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or sensitive site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CSP, PWGSC. Until the security screening of the Contractor personnel required by this Contract has been completed satisfactorily by the CSP, PWGSC, the Contractor personnel **MAY NOT HAVE ACCESS** to **PROTECTED** information or assets, and **MAY NOT ENTER** sites where such information or assets are kept, without an escort.

3. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED B including an IT Link at the level of PROTECTED B.

4. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CSP/PWGSC.

5. The Contractor/Offeror must comply with the provisions of the:

   (a) Security Requirements Check List and security guide (if applicable), attached at Annex _____;
   (b) Contract Security Manual (Latest Edition);
   (c) CSP website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src

SECURITY REQUIREMENTS FOR FOREIGN SUPPLIER

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation:

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming **Contractor** compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada the Work described in the Cloud Solutions, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

1. The Foreign recipient **Contractor** must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has

international bilateral security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

2. The Foreign recipient **Contractor** must at all times during the performance of the **contract** be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient **Contractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA, and identify the relevant national Privacy Authority. For European **Contractors**, this will be the national Data Protection Authority (DPA).

3. The Foreign recipient **Contractor** must, at all times during the performance of the **contract**, hold an equivalence to a valid Designated Organization Screening (DOS), issued by the Canadian DSA as follows:

   i. The Foreign recipient **Contractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

   ii. The Foreign recipient **Contractor** must not begin the work, services or performance until the Canadian Designated Security Authority (DSA) is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation must be provided, in writing, to the foreign recipient **Contractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

   iii. The Foreign recipient **Contractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent foreign recipient **Contractor's** Chief Executive officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the contract.

   iv. The Foreign recipient **Contractor** must not grant access to **CANADA PROTECTED A and/or B** information/assets, except to its personnel subject to the following conditions:

      a. Personnel have a need-to-know for the performance of the **contract**;

      b. Personnel have been subject to a Criminal Record Check, with favourable results, from a recognized governmental agency or private sector organization in **their country** as well as a Background Verification, validated by the Canadian DSA;

      c. The Foreign recipient **Contractor** must ensure that personnel provide consent to share results of the Criminal Record and Background Checks with the Canadian DSA and other Canadian Government Officials, if requested;

      d. Until the Foreign recipient **Contractor** has provided the Canadian DSA with the required written personnel security screening assurances, the Foreign recipient **Contractor** personnel MUST NOT HAVE ACCESS to **CANADA PROTECTED A and/or B** information/assets, and MUST NOT ENTER "Government of Canada" or "Contractor" sites where such information/assets are kept, without an escort. An escort is defined as "a Government of Canada" or "Contractor" employee who holds the appropriate Personnel Security Clearance at the required level; and

e. The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a foreign recipient **Contractor** for cause.

4. **CANADA PROTECTED/PERSONAL** information/assets, provided to the foreign recipient **Contractor** or produced by the Foreign recipient **Contractor**, must:

   a. not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract**, without the prior written consent of Canada. Such consent must be sought from its national DPA, the Contracting Authority (in collaboration with the Canadian DSA); and

   b. not be used for any purpose other than for the performance of the **contract** without the prior written approval Canada. This approval must be obtained by contacting its national DPA, the Contracting Authority (in collaboration with the Canadian DSA).

5. The Foreign recipient **Contractor** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor** must ensure that its personnel are made aware of and comply with this restriction.

6. The Foreign recipient **Contractor** must not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **contract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

7. The Foreign recipient **Contractor** must, at all times during the performance of the **contract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED A and/or B**.

All **CANADA PROTECTED** information/assets, furnished to the foreign recipient **Contractor** or produced by the foreign recipient **Contractor**, must also be safeguarded as follows:

8. The Foreign recipient **Contractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/ assets pursuant to this **contract** has been compromised.

OR

9. The Foreign recipient **Contractor** must immediately report to its respective national DPA and the Contracting Authority (in collaboration with the Canadian DSA), all cases in which it is known or there is reason to suspect that any Personal Information provided or generated pursuant to this **contract** have been lost, or in contravention of these security requirements, accessed, used or disclosed to unauthorized persons.

10. The Foreign recipient **Contractor** must not disclose **CANADA PROTECTED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.

11. The Foreign recipient **Contractor** must provide the **CANADA PROTECTED** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.

12. Upon completion of the Work, the foreign recipient **Contractor** must return to the Government of Canada, all **CANADA PROTECTED** information/assets furnished or produced pursuant to this **contract**, including all **CANADA PROTECTED** information/assets released to and/or produced by its subcontractors.

13. The Foreign recipient **Contractor** requiring access to **CANADA PROTECTED** information/assets or Canadian restricted sites, under this contract, must submit a Request for Site Access to the Chief Security Officer of **Employment and Social Development Canada.**
14. The Foreign recipient **Contractor** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system or transfer via an IT link any **CANADA PROTECTED A and/or B** information until authorization to do so has been confirmed by the Canadian DSA.
15. The Foreign recipient **Contractor** must ensure that all the databases including the backup database used by organizations to provide the services described in the proposed Cloud Solutions, containing any **CANADA PROTECTED** Information, related to the Work, are located within Canada.
16. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.
17. All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.
18. All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.
19. The Foreign recipient **Contractor** must comply with the provisions of the Security Requirements Check List attached at Annex _____.
20. Canada has the right to reject any request to electronically access, process, produce, transmit or store **CANADA PROTECTED** information/assets related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

Protection and Security of Data Stored in Databases

1. The foreign recipient **Contractor** must ensure that all the databases used by organizations to provide the services described in the proposed Cloud Solutions containing any Personal Information, related to the Work, are located in Canada.
2. The foreign recipient **Contractor** must control access to all databases on which any data relating to the **contract** is stored so that only individuals with the appropriate security screening are able to access the database, either by using a password or other form of access control (such as biometric controls).
3. The foreign recipient **Contractor** must ensure that all databases on which any data relating to the **contract** is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases.
4. The foreign recipient **Contractor** must ensure that all data relating to the **contract** is processed only in Canada or in another country approved by the Contracting Authority under subsection 1.
5. The foreign recipient **Contractor** must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented

in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection 1.

6. Despite any section of the General Conditions relating to subcontracting, the foreign recipient **Contractor** must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the contract unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.

Personal Information

Interpretation

In the **contract**, unless the context otherwise requires,

"General Conditions" means the general conditions that form part of the **contract**;

"Personal Information" means information about an individual, including the types of information specifically described in the *Privacy Act*, R.S. 1985, c. P-21;

"Record" means any hard copy document or any data in a machine-readable format containing Personal Information;

Words and expressions defined in the General Conditions and used in these supplemental general conditions have the meanings given to them in the General Conditions.

If there is any inconsistency between the General Conditions and these Personal Information articles, these Personal Information articles prevail.

Ownership of Personal Information and Records

To perform the Work, the foreign recipient **Contractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor** acknowledges that it has no rights in the Personal Information or the Records and that Canada owns the Records. On request, the foreign recipient **Contractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

Use of Personal Information

The foreign recipient **Contractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Work in accordance with the **contract**.

Collection of Personal Information

1. If the foreign recipient **Contractor** must collect Personal Information from a third party to perform the Work, the foreign recipient **Contractor** must only collect Personal Information that is required to perform the Work. The foreign recipient **Contractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:
   a. that the Personal Information is being collected on behalf of, and will be provided to, Canada;
   b. the ways the Personal Information will be used;
   c. that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;
   d. the consequences, if any, of refusing to provide the information;
   e. that the individual has a right to access and correct his or her own Personal Information; and

f. that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the foreign recipient **Contractor**.

2. The foreign recipient **Contractor**, and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

3. If requested by the Contracting Authority, the foreign recipient **Contractor** must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The foreign recipient **Contractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.

4. At the time it requests Personal Information from any individual, if the foreign recipient **Contractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the foreign recipient **Contractor** must ask the Contracting Security Authority for instructions.

Maintaining the Accuracy, Privacy and Integrity of Personal Information

The foreign recipient **Contractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor** must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor** must:

a. not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;

b. segregate all Records from the foreign recipient **Contractor's** own information and records;

c. restrict access to the Personal Information and the Records to people who require access to perform the Work (for example, by using passwords or biometric access controls);

d. provide training to anyone to whom the foreign recipient **Contractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Work. The foreign recipient **Contractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor** must keep a record of the training and make it available to the Contracting Authority if requested;

e. if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor** provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;

f. keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);

g. include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

h. keep a record of the date and source of the last update to each Record;

i. maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the foreign recipient **Contractor** and Canada at any time; and

j. secure and control access to any hard copy Records.

Safeguarding Personal Information

The foreign recipient **Contractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. To do so, at a minimum, the foreign recipient **Contractor** must:

a. store the Personal Information electronically so that a password (or a similar access control mechanism, such as biometric access) is required to access the system or database in which the Personal Information is stored;

b. ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Work;

c. not outsource the electronic storage of Personal Information to a third party (including an affiliate) unless the Canadian DSA has first consented in writing;

d. safeguard any database or computer system on which the Personal Information is stored from external access using methods that are generally used, from time to time, by prudent public and private sector organizations in Canada in order to protect highly secure or sensitive information;

e. maintain a secure back-up copy of all Records, updated at least weekly;

f. implement any reasonable security or protection measures requested by Canada from time to time; and

g. notify the Contracting Authority and the Canadian DSA immediately of any security breaches; for example, any time an unauthorized individual accesses any Personal Information.

Appointment of Privacy Officer

The foreign recipient **Contractor** must appoint someone to be its privacy officer and to act as its representative for all matters related to the Personal Information and the Records. The foreign recipient **Contractor** must provide that person's name to the Contracting Authority and the Canadian DSA within ten (10) days of the award of the **contract**.

Quarterly Reporting Obligations

Within 30 calendar days of the end of each quarter (January-March; April-June; July-September; October-December), the foreign recipient **Contractor** must submit the following to the Contracting Authority:

a. a description of any new measures taken by the foreign recipient **Contractor** to protect the Personal Information (for example, new software or access controls being used by the foreign recipient **Contractor**);

b. a list of any corrections made to Personal Information at the request of an individual (including the name of the individual, the date of the request, and the correction made);

c. details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the foreign recipient **Contractor**; and

d. a complete copy (in an electronic format agreed to by the Contracting Authority and the foreign recipient **Contractor**) of all the Personal Information stored electronically by the foreign recipient C**ontractor**.

Threat and Risk Assessment

Within ninety (90) calendar days of the award of the **contract** and, if the **contract** lasts longer than one year, within thirty (30) calendar days of each anniversary date of the **contract**, the foreign recipient **Contractor** must submit to the Contracting Authority and the Canadian DSA a threat and risk assessment, which must include:

a. a copy of the current version of any request for consent form or script being used by the foreign recipient **Contractor** to collect Personal Information;

b. a list of the types of Personal Information used by the foreign recipient **Contractor** in connection with the Work;

c. a list of all locations where hard copies of Personal Information are stored;

d. a list of all locations where Personal Information in machine-readable format is stored (for example, the location where any server housing a database including any Personal Information is located), including back-ups;

e. a list of every person to whom the foreign recipient **Contractor** has granted access to the Personal Information or the Records;

f. a list of all measures being taken by the foreign recipient **Contractor** to protect the Personal Information and the Records;

g. a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and

h. an explanation of any new measures the foreign recipient **Contractor** intends to implement to safeguard the Personal Information and the Records.

Audit

Canada may audit the foreign recipient **Contractor's** compliance with these supplemental general conditions at any time. If requested by the Contracting Authority, the foreign recipient **Contractor** must provide Canada (or Canada's authorized representative) with access to its premises and to the Personal Information and Records at all reasonable times. If Canada identifies any deficiencies during an audit, the foreign recipient **Contractor** must immediately correct the deficiencies at its own expense.

Statutory Obligations

1. The foreign recipient **Contractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act*, *Access to Information Act*, R.S. 1985, c. A-1, and *Library and Archives of Canada Act*, S.C. 2004, c. 11. The foreign recipient **Contractor** agrees to comply with any requirement established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

2. The foreign recipient **Contractor** acknowledges that its obligations under the **contract** are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province

or territory of Canada. If the foreign recipient **Contractor** believes that any obligations in the **contract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor** must immediately notify the Contracting Authority of the specific provision of the **contract** and the specific obligation under the law with which the foreign recipient **Contractor** believes it conflicts.

Disposing of Records and Returning Records to Canada

The foreign recipient **Contractor** must not dispose of any Record, except as instructed by the Contracting Authority. On request by the Contracting Authority, or once the Work involving the Personal Information is complete, the **contract** is complete, or the **contract** is terminated, whichever of these comes first, the foreign recipient **Contractor** must return all Records (including all copies) to the Contracting Authority.

Legal Requirement to Disclose Personal Information

Before disclosing any of the Personal Information pursuant to any applicable legislation, regulation, or an order of any court, tribunal or administrative body with jurisdiction, the foreign recipient **Contractor** must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

Complaints

Canada and the foreign recipient **Contractor** each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

Exception

The obligations set out in these supplemental general conditions do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the Contractor or any of its subcontractors, agents, or representatives, or any of their employees.

ATTACHMENT 3

DRAFT ANNEX A STATEMENT OF WORK

Note to Suppliers: the draft Annex A, Statement of Work includes the following Appendices; Appendix 1 to Annex A, Technical Standards; Appendix 2 to Annex A, Functional and Non-Functional Requirements; Appendix 3 to Annex A, Client Identity and Access Management Legacy at ESDC and Characteristics of Target Solution for iSAMS; Appendix 4 to Annex A, Conformance Criteria of the Public Sector Profile of the Pan-Canadian Trust Framework (PCTF)

(Please see section entitled “Non-Disclosure Agreement and Reference Material” for details on how to access the document)

ATTACHMENT 4

SUPPLY CHAIN SECURITY INFORMATION ASSESSMENT PROCESS

Introduction

Bidders must submit specific information regarding each component of their proposed Solution's supply chain. This information is referred to as *Supply Chain Security Information (SCSI)*. This information will be used by Canada to assess whether, in its opinion, a bidder's proposed supply chain creates the possibility that the bidder's proposed Solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information in accordance with the process found in this Attachment. This assessment is referred to as the SCSI Assessment Process.

Bidders must provide their SCSI for a solution that is hosted within Canada's technical environment.

Definitions

The following words and expressions used with respect to SCI Process have the following meanings:

a. "**OEM Name**" means the name of the original equipment manufacturer (OEM) of the product that is being ordered.

b. "**OEM DUNS Number**" means the Data Universal Numbering System (DUNS). It is a unique nine-digit number assigned to each physical location of a business. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.

c. **Product Name** means the OEM's name for the product;

d. **Model Number** means the OEM's model and/or version number of the product.

e. **Vulnerability Information** means the information concerning the last 5 security issues that were reported about the product. If the OEM posts this information to the CVE website, list the CVE numbers **separated by semi-colons (;)**. If the OEM does not post this information to the CVE website, you will need to ask the OEM directly for security vulnerability information and provide this information to the Canadian Centre for Cyber Security. If this is the case for a particular product, enter "see attached information" in the relevant field(s).

f. **Supplier Name** means the name of the supplier (i.e. sub-contractors, re-seller, distributor, sub-processors, etc.) of the product that is being ordered. This includes any business entity involved in producing products or services to help complete the bidding requirements.

g. **Supplier DUNS Number** is already explained above.

h. **Supplier URL** means the URL of the supplier's webpage for the product.

i. **Ownership** means the top 5, by percentage, owners of the OEM or Supplier. The names provided for owners should be those found in ownership documents for the company in question.

j. **Investors** means the top 5, by percentage, investor in the OEM or Supplier. The names provided for owners should be those found in investment documents for the company in question.

k. **Executives** means the executives and members of the board of directors for the company in question.

l. **Country / Nationality** means the country which an individual listed has their primary nationality or the country in which a corporate entity is registered.

m. **Corporate website link** means for each of OEM or Supplier name, Ownership, Investors, and Executives listed above provide a URI / URL to the information that supports the claims listed in each of the fields.

n. "**Supply Chain Security Information**" means any information that Canada requires a Bidder or Contractor to submit to conduct a complete security assessment of the SCSI as a part of the SCSI Assessment process.

Supply Chain Security Information Form Submission Requirements

Bidders must provide the following information by the bid closing date (see Part 2 – Bidder Instructions, Article 2.2 – Submission of Bids):

a. IT Product List**:** Bidders must identify the Products over which Canada's Data would be transmitted and/or on which Canada's Data would be stored, or that would be used and/or installed by the Bidder or any of its subcontractors to perform any part of the Work, together with the following information regarding each Product:

   i. OEM Name;

   ii. OEM DUNS Number;

   iii. Product Name;

   iv. Model Number;

   v. Vulnerability Information;

Bidders are requested to provide the IT Product information for their proposed Solution on *Page B – IT Product List*. Bidders are also requested to insert a separate row for each Product. Bidders are requested not to repeat multiple iterations of the same Product (e.g. if the serial number and/or color is the only difference between two products, they are considered the same Product within the confines of the SCI Assessment Process).

b. Ownership Information: "It is only necessary to fill out entries in ""C- Ownership Information"" if a DUNS number cannot be supplied for the OEM and/or supplier.

   i. Supplier Name;

   ii. Supplier DUNS Number;

   iii. Supplier URL;

   iv. Ownership;

   v. Investors;

   vi. Executives;

   vii. Country / Nationality;

   viii. Corporate website link.

Assessment of Supply Chain Security Information

a. Canada will assess whether, in its opinion, the SCSI creates the possibility that the Bidder's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.

b. In conducting its assessment:

   i. Canada may request from the Bidder any additional information that Canada requires to conduct a complete security assessment of the SCSI. The Bidder will have 2 working

days (or a longer period if specified in writing by Canada) to provide the necessary information to Canada.

ii. Canada may use any government resources to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is included in the bid or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of the SCSI.

c. If, in Canada's opinion, there is a possibility that any aspect of the SCSI, if used by Canada, could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information:

i. Canada will notify the Bidder in writing (sent by email) and identify which aspect(s) of the Bidder's SCSI is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Bidder regarding its concerns will be determined based on the nature of the concerns. In some situations, for reasons of national security, it may not be possible for Canada to provide further information to the Bidder; therefore, in some circumstances, the Bidder will not know the underlying reasons for Canada's concerns with respect to a product, subcontractor or other aspect of the Bidder's SCSI. With respect to any concerns, Canada may, in its discretion, identify a potential mitigation measure that the Bidder would be required to implement with respect to any portion of the SCSI if awarded a contract.

ii. Upon receipt of Canada's written notice, the Bidder will be given one opportunity to submit a revised SCSI. If Canada has identified a potential mitigation measure that the supplier would be required to implement if awarded a contract, the Bidder must confirm in its revised SCSI whether or not it agrees that any awarded contract will contain additional commitments relating to those mitigation conditions. The revised SCSI must be submitted within the **10 calendar days** following the day on which Canada's written notification is sent to the Bidder (or a longer period specified in writing by the Contracting Authority).

d. If the Bidder submits a revised SCSI within the allotted time, Canada will perform a second assessment. If in Canada's opinion, there is a possibility that any aspect of the Bidder's revised SCSI could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, the Bidder will be provided with the same type of notice described under paragraph c), above. Any further opportunities to revise the SCSI will be entirely at the discretion of Canada and all SCSI respondents will be offered the same opportunity. By participating in this process, the Bidder acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. As a result:

i. qualification pursuant to this SCSI Assessment Process does not constitute an approval that the products or other information included as part of the SCSI will meet the requirements of the resulting contract;

ii. qualification pursuant to this SCSI Assessment Process does not mean that the same or similar SCSI will be assessed in the same way for future requirements;

iii. at any time during this bid solicitation process, Canada may advise a Bidder that some aspect(s) of its SCSI has become the subject of security concerns. At that point, Canada will notify the Bidder and provide the Bidder with an opportunity to revise its SCSI, using the process described above; and,

iv. during the performance of any contract resulting from this bid solicitation, if Canada has concerns regarding certain products, designs or subcontractors originally included in the SCSI, the terms and conditions of that contract will govern the process for addressing those concerns.

Upon completion of the SCSI Integrity Assessment, Bidders will be notified of the results through the Contracting Authority.

Tab A – SCSI FORM 2 COVER

Supply Chain Security Information (SCSI) Vendor Submission Form

PART A - BIDDER INFORMATION	
Procurement Name:	
Date submitted:	
Solicitation Number:	
Bidder Name:	
Bidder DUNS Number:	

PART B - PRODUCT LIST
CLICK HERE TO ADD ITEMS +

PART C - OWNERSHIP INFORMATION
CLICK HERE TO ADD ITEMS +

Please save this form only in Excel format before submitting. Please do not use other formats.

Tab B – IT PRODUCT LIST

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Supplier Name	Supplier DUNS Number	Supplier URL	Additional Information
1										
2										
3										
4										
5										

Tab C – OWNERSHIP INFORMATION

Item	OEM or Supplier name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
1						
2						
3						
4						
5						