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
Québec
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Title - Sujet Processing Software Solution	
Solicitation No. - N° de l'invitation 24062-180627/D	**Amendment No. - N° modif.** 009
Client Reference No. - N° de référence du client 24062-180627	**Date** 2020-09-18
GETS Reference No. - N° de référence de SEAG PW-$$XL-138-38306	
File No. - N° de dossier 138xl.24062-180627	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-09-28**	**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: Weinberger, Beth	**Buyer Id - Id de l'acheteur** 138xl
Telephone No. - N° de téléphone (819) 576-5319 ( )	**FAX No. - N° de FAX** (000) 000-0000
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

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

Canada

Solicitation No. – N° de l'invitation	Amd. No – N° de la modif.	Buyer ID – Id de l'acheteur
24062-180627/A	009	138XL
Client Ref. No. – N° de réf. De client	**File No. – N° du dossier**	**CCC No./ N° CCC – FMS No/ N° VME**
24062-180627		

Solicitation Amendment 009 is raised to respond to: (1) make revisions throughout the RFP in reference to the Supply Chain Integrity Process; (2) replace Annex E; (3) replace Form 5; and (4) respond to questions from Industry.

PART 1: make revisions throughout the RFP in reference to the Supply Chain Integrity Process:

Add as Part 1, Article 1.2 (j) the following:

Insert as sub-article 1.2 (j) the following:

1.2 (j) This bid solicitation contains a security requirement in relation to the supply chain of each of the Bidders including a separate closing date to provide this information to Canada; see Part 3 - Bid Preparation Instructions for additional information on the assessment of bidders' Supply Chain Security Information (SCSI).

Insert at Part 3, sub-article 3.1 (b)(iv) and (v) the following:

3.1 (b) (iv) Section IV: Additional Information
(v) Section V: Supply Chain Information

Delete Article 3.8 – Supply Chain Integrity (SCI) Requirements in its entirety.
Replace with the following:

3.8 Section V: Supply Chain Security Information

Bidders must submit specific information regarding each component of their proposed Solution's supply chain ("Supply Chain Security Information" or "SCSI") as defined in Annex E - Supply Chain Security Information Assessment Process. The Supply Chain Security Information must be submitted in this Section. The Supply Chain Security 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 Supply Chain Security Information assessment as described in Annex E - Supply Chain Security Information Assessment Process.

Insert as sub-article 4.1.7 the following:

4.1.7 Supply Chain Security Information Assessment Process

Canada will assess whether, in its opinion, each bidder's 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 Annex E - Supply Chain Security Information Assessment Process.

Delete sub-article 4.6 (b) in its entirety.
Replace with the following:

4.6 (b) To be declared responsive per Tier, a bid must:

(i) qualify pursuant to the Supply Chain Security Information Assessment Process;
(ii) comply with all the requirements of the bid solicitation;
(iii) meet all mandatory technical evaluation criteria; and
(iv) obtain the required minimum of 60% score for the technical evaluation criteria as stipulated in Annex G – Bid Evaluation and Capability and Usability Evaluation which are subject to point rating.

Subject to the Phased Bid Compliance Process, Bids not meeting (i) or (ii) or (iii) or (iv) will be declared non-responsive.

Insert as Part 7, Article 7.34 – Ongoing Supply Chain Security Information Assessment Process, as follows:

7.34 Ongoing Supply Chain Security Information Assessment Process

(a) **Supply Chain Security Information Assessment Process**: The Parties acknowledge that a Supply Chain Security Information Assessment Process was a key component of the procurement process that resulted in the award of this Contract. In connection with that assessment process, Canada assessed the Contractor's Supply Chain Security Information ("SCSI") without identifying any security concerns. The following SCSI was submitted:

(i) Supply Chain Security Information Submission Form

(ii) IT Product List; and,

(iii) Network Diagram.

This SCSI is included as Annex E - Supply Chain Security Information Assessment Process. The Parties also acknowledge that security is a critical consideration for Canada with respect to this Contract and that on-going assessment of SCSI will be required throughout the Contract Period. This Article governs that process.

(b) Assessment of New SCSI: During the Contract Period, the Contractor may need to modify the SCSI contained in Annex E - Supply Chain Security Information Assessment Process. In that regard:

(i) The Contractor, starting at Contract award, must revise its SCSI at least once a month to show all changes made, as well as all deletions and additions to the SCSI that affect the services under the Contract (including Products deployed by its subcontractors) during that period; the list must be marked to show the changes made during the applicable period. If no changes have been made during the reporting month, the Contractor must advise the Contracting Authority in writing that the existing list is unchanged.

(ii) The Contractor agrees that, during the Contract Period, it will periodically (at least once a year) provide the Contracting Authority with updates regarding upcoming new Products that it anticipates deploying in the Work (for example, as it develops its "technology roadmap" or similar plans). This will allow Canada to assess those Products in advance so that any security concerns can be identified prior to the Products being deployed in connection with the services being delivered under the Contract. Canada will endeavour to assess proposed new Products within 30 calendar days, although lengthier lists of Products may take additional time.

(iii) Canada reserves the right to conduct a complete, independent security assessment of all new SCSI. The Contractor must, if requested by the Contracting Authority, provide any information that Canada requires to perform its assessment.

(iv) 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 provided by the Contractor or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of any proposed new SCSI.

(c) Identification of New Security Vulnerabilities in SCSI already assessed by Canada:

(i) The Contractor must provide to Canada timely information about any vulnerabilities of which it becomes aware in performing the Work, including any weakness, or design deficiency, identified in any Product used to deliver services that would allow an unauthorized individual to compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications it hosts.

(ii) The Contractor acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified and, that being the case, new security vulnerabilities may be identified in SCSI that have already been the subject of an SCSI assessment and assessed without security concerns by Canada, either during the procurement process or later during the Contract Period.

(d) Addressing Security Concerns:

(i) If Canada notifies the Contractor of security concerns regarding a Product that has not yet been deployed, the Contractor agrees not to deploy it in connection with this Contract without the consent of the Contracting Authority.

(ii) At any time during the Contract Period, if Canada notifies the Contractor that, in Canada's opinion, there is a Product that is being used in the Contractor's Solution (including use by a subcontractor) that has been assessed as having the potential to compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, then the Contractor must:

(A) provide Canada with any further information requested by the Contracting Authority so that Canada may perform a complete assessment;

(B) if requested by the Contracting Authority, propose a mitigation plan (including a schedule), within 10 business days, such as migration to an alternative Product. The Contracting Authority will notify the Contractor in writing if Canada approves the mitigation plan, or will otherwise provide comments about concerns or deficiencies with the mitigation plan; and

(C) implement the mitigation plan approved by Canada. This process applies both to new Products and to Products that were already assessed pursuant to the Supply Chain Security Information Assessment Process by Canada, but for which new security vulnerabilities have since been identified.

(iii) Despite the previous Sub-article, if Canada determines in its discretion that the identified security concern represents a threat to national security that is both serious and imminent, the Contracting Authority may require that the Contractor immediately cease deploying the identified Product(s) in the Work. For Products that have already been deployed, the Contractor must identify and/or remove (as required by the Contracting Authority) the Product(s) from the Work according to a schedule determined by Canada. However, prior to making a final determination in this regard, Canada will provide the Contractor with the opportunity to make representations within 48 hours of receiving notice from the Contracting Authority. The Contractor may propose, for example, mitigation measures for Canada's consideration. Canada will then make a final determination.

(e) **Cost Implications:**

(i) Any cost implications related to a demand by Canada to cease deploying or to remove a particular Product or Products will be considered and negotiated in good faith by the Parties on a case-by-case basis and may be the subject of a Contract Amendment, however, despite any such negotiations, the Contractor must cease deploying and/or remove the Product(s) as required by Canada. The negotiations will then continue separately. The Parties agree that, at a minimum, the following factors will be considered in their negotiations, as applicable:

(A) with respect to Products already assessed without security concerns by Canada pursuant to an SCI assessment, evidence from the Contractor of how long it has owned the Product;

(B) with respect to new Products, whether or not the Contractor was reasonably able to provide advance notice to Canada regarding the use of the new Product in connection with the Work;

(C) evidence from the Contractor of how much it paid for the Product, together with any amount that the Contractor has pre-paid or committed to pay with respect to maintenance and support of that Product;

(D) the normal useful life of the Product;

(E) any "end of life" or other announcements from the manufacturer of the Product indicating that the Product is or will no longer be supported;

(F) the normal useful life of the proposed replacement Product;

(G) the time remaining in the Contract Period;

(H) whether or not the existing Product or the replacement Product is or will be used exclusively for Canada or whether the Product is also used to provide services to other customers of the Contractor or its subcontractors;

(I) whether or not the Product being replaced can be redeployed to other customers;

(J) any training required for Contractor personnel with respect to the installation, configuration and maintenance of the replacement Products, provided the Contractor can demonstrate that its personnel would not otherwise require that training;

(K) any developments costs required for the Contractor to integrate the replacement Products into the Service Portal, operations, administration and management systems, if the replacement Products are Products not otherwise deployed anywhere in connection with the Work; and

(L) the impact of the change on Canada, including the number and type of resources required and the time involved in the migration.

(ii) Additionally, if requested by the Contracting Authority, the Contractor must submit a detailed cost breakdown, once any work to address a security concern identified under this Article has been completed. The cost breakdown must contain an itemized list of all applicable cost elements related to the work required by the Contracting Authority and must be signed and certified as accurate by the Contractor's most senior financial officer, unless stated otherwise in writing by the Contracting Authority. Canada must consider the supporting information to be sufficiently detailed for each cost element to allow for a complete audit. In no case will any reimbursement of any expenses of the Contractor (or any of its subcontractors) exceed the demonstrated out-of-pocket expenses directly attributable to Canada's requirement to cease deploying or to remove a particular Product or Products.

(iii) Despite the other provisions of this Article, if the Contractor or any of its subcontractors deploys new Products that Canada has already indicated to the Contractor are the subject of security concerns in the context of the Work, Canada may require that the Contractor or any of its subcontractors immediately cease deploying or remove that Product. In such cases, any costs associated with complying with Canada's requirement will be borne by the Contractor and/or subcontractor, as negotiated between them. Canada will not be responsible for any such costs.

(f) General:

(i) The process described in this Article may apply to a single Product, to a set of Products, or to all Products manufactured or distributed by a particular supplier.

(ii) The process described in this Article also applies to subcontractors. With respect to cost implications, Canada acknowledges that the cost considerations with respect to concerns about subcontractors (as opposed to Products) may be different and may include factors such as the availability of other subcontractors to complete the work.

(iii) Any service levels that are not met due to a transition to a new Product or subcontractor required by Canada pursuant to this Article will not trigger a Service Credit, nor will a failure in this regard be taken into consideration for overall metric calculations, provided that the Contractor implements the necessary changes in accordance with the migration plan approved by Canada or proceeds immediately to implement Canada's requirements if Canada has determined that the threat to national security is both serious and imminent.

(iv) If the Contractor becomes aware that any subcontractor is deploying Products subject to security concerns in relation to the Work, the Contractor must immediately notify both the Contracting Authority and the Technical Authority and the Contractor must enforce the terms of its contract with its subcontractor. The Contractor acknowledges its obligations pursuant to General Conditions 2030 Higher Complexity - Goods, Subsection 9(3).

(v) Any determination made by Canada will constitute a decision with respect to a specific Product or subcontractor and its proposed use under this Contract, and does not mean that the same Product or subcontractor would necessarily be assessed in the same way if proposed to be used for another purpose or in another context.

(g) Subcontracting

(i) Despite the General Conditions, none of the Work may be subcontracted (even to an affiliate of the Contractor) unless the Contracting Authority has first consented in writing. In order to seek the Contracting Authority's consent, the Contractor must provide the following information:

(A) the name of the subcontractor;

(B) the portion of the Work to be performed by the subcontractor;

(C) the Designated Organization Screening or the Facility Security Clearance (FSC) level of the subcontractor;

(D) the date of birth, the full name and the security clearance status of individuals employed by the subcontractor who will require access to Canada's facilities;

(E) completed sub-SRCL signed by the Contractor's Company Security Officer for CISD completion; and

(F) any other information required by the Contracting Authority.

(ii) For the purposes of this Article, a "subcontractor" does not include a supplier who deals with the Contractor at arm's length whose only role is to provide telecommunications or other equipment or software that will be used by the Contractor to provide services, including if the equipment will be installed in the backbone or infrastructure of the Contractor.

(h) Change of Control

(i) At any time during the Contract Period, if requested by the Contracting Authority, the Contractor must provide to Canada:

(A) an organization chart for the Contractor showing all related corporations and partnerships; for the purposes of this Sub-article, a corporation or partnership will be considered related to another entity if:

(i) they are "related persons" or "affiliated persons" according to the Canada *Income Tax Act*;

(ii) the entities have now or in the two years before the request for the information had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

(iii) the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

(B) a list of all the Contractor's shareholders; if the Contractor is a subsidiary, this information must be provided for each parent corporation or parent partnership, up to the ultimate owner; with respect to any publicly traded corporation, Canada anticipates that the circumstances in which it would require a complete list of shareholders would be unusual and that any request from Canada for a list of a publicly traded corporation's shareholders would normally be limited to a list of those shareholders who hold at least 1% of the voting shares;

(C) a list of all the Contractor's directors and officers, together with each individual's home address, date of birth, birthplace and citizenship(s); if the Contractor is a subsidiary, this information must be provided for each parent corporation or parent partnership, up to the ultimate owner; and

(D) any other information related to ownership and control that may be requested by Canada.

If requested by the Contracting Authority, the Contractor must provide this information regarding its subcontractors as well. However, if a subcontractor considers this information to be confidential, the Contractor may meet its obligation by having the subcontractor submit the information directly to the Contracting Authority. Regardless of whether the information is submitted by the Contractor or a subcontractor, Canada agrees to handle this information in accordance with **Subsection 23(3) of General Conditions 2030** (General Conditions – Higher Complexity – Goods), provided the information has been marked as either confidential or proprietary.

(ii) The Contractor must notify the Contracting Authority in writing of:

(A) any change of control in the Contractor itself;

(B) any change of control in any parent corporation or parent partnership of the Contractor, up to the ultimate owner; and

(C) any change of control in any subcontractor performing any part of the Work (including any change of control in any parent corporation or parent partnership of the subcontractor, up to the ultimate owner).

(iii) The Contractor must provide this notice by no later than 10 Federal Government Working Days (FGWD) after any change of control takes place (or, in the case of a subcontractor, within 15 FGWDs after any change of control takes place). Where possible, Canada requests that the Contractor provide advance notice of any proposed change of control transaction.

(iv) In this Article, a "change of control" includes but is not limited to a direct or indirect change in the effective control of the corporation or partnership, whether resulting from a sale, encumbrance, or other disposition of the shares (or any form of partnership units) by any other means. In the case of a joint venture Contractor or subcontractor, this applies to a change of control of any of the joint venture's corporate or partnership members. In the case of a Contractor or subcontractor that is a partnership or limited partnership, this requirement also applies to any corporation or limited partnership that is a partner.

(v) If Canada determines in its sole discretion that a change of control affecting the Contractor (either in the Contractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada may terminate the Contract on a "no-fault" basis by providing notice to the Contractor within 90 calendar days of receiving the notice from the Contractor regarding the change of control. Canada will not be required to provide its reasons for terminating the Contract in relation to the change of control, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security.

(vi) If Canada determines in its sole discretion that a change of control affecting a subcontractor (either in the subcontractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada will notify the Contractor in writing of its determination. Canada will not be required to provide the reasons for its determination, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security. The Contractor must, within 90 calendar days of receiving Canada's determination, arrange for another subcontractor, acceptable to Canada, to perform the portion of the Work being performed by the existing subcontractor (or the Contractor must perform this portion of the Work itself). If the Contractor fails to do so within this time period, Canada will be entitled to terminate the Contract on a "no-fault" basis by providing notice to the Contractor within 180 calendar days of receiving the original notice from the Contractor regarding the change of control.

(vii) In this Article, termination on a "no-fault" basis means that neither party will be liable to the other in connection with the change of control or the resulting termination, and Canada will only be responsible for paying for those services received up to the effective date of the termination.

Despite the foregoing, Canada's right to terminate on a "no-fault" basis will not apply to circumstances in which there is an internal reorganization that does not affect the ownership of the ultimate parent corporation or parent partnership of the Contractor or subcontractor, as the case may be; that is, Canada does not have a right to terminate the Contract pursuant to this Article where the Contractor or subcontractor continues, at all times, to be controlled, directly or indirectly, by the same ultimate owner. However, in any such case, the notice requirements of this Article still apply.

PART 2:

Delete Annex E in its entirety.
Replace with the following:

ANNEX E - 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 Annex. 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 (refer to Appendix A to Annex E – Conceptual View of 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.

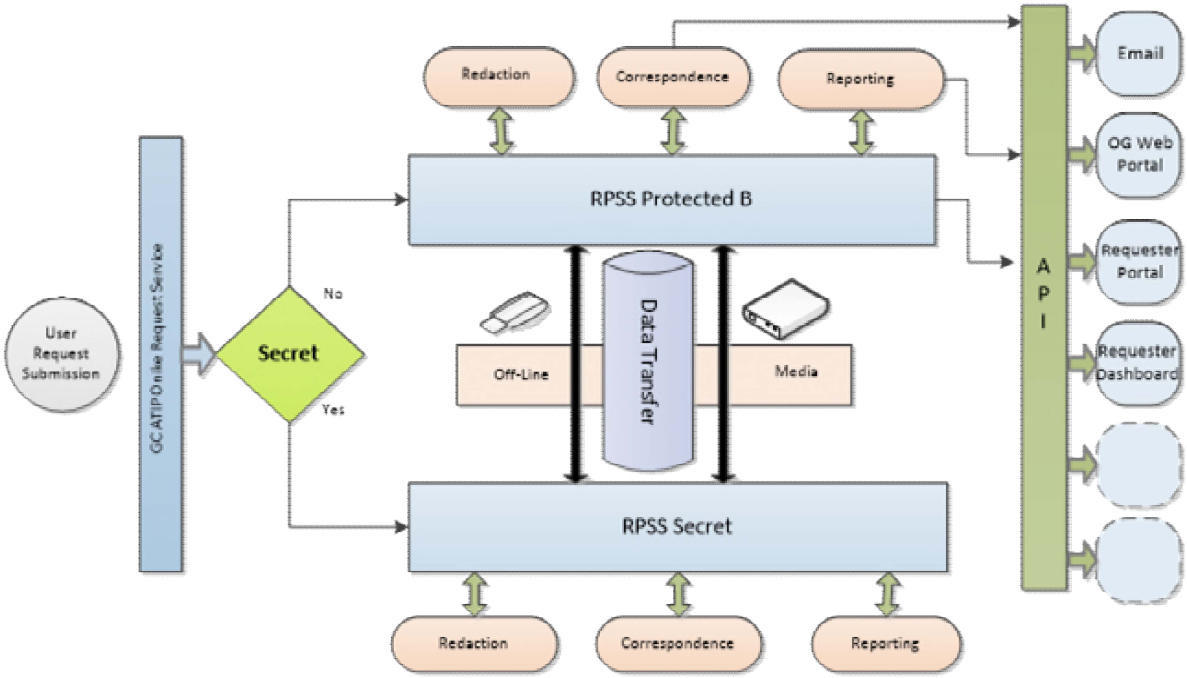
Tab B – IT PRODUCT LIST

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Supplier Name	Supplier DUNS Numb	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						

Insert as Appendix A to Annex E – Conceptual View of Technical Environment, the following:



PART 3:

Delete Form 5 in its entirety.

Replace with the following:

FORM 5 – DECLARATION FORM

This declaration form must be submitted as part of the bidding process with your e-Bid submission. Please complete and label as **"Protected"** and submit in accordance with Article 3.1 of the RFP. This form is considered "Protected B" when completed.	
Complete Legal Name of Company:	
Company's address:	
Company's Procurement Business Number (PBN):	
Bid Number:	
Date of Bid: (YY-MM-DD)	

Have you ever, as the bidder, your affiliates or as one of your directors, been convicted or have pleaded guilty of an offence in Canada or similar offence elsewhere under any of the following provisions [1] :

	Yes	No	Comments
Financial Administration Act			
80(1) d): False entry, certificate or return	☐	☐	
80(2): Fraud against Her Majesty			
154.01: Fraud against Her Majesty			
Criminal Code			
121: Frauds on the government and contractor subscribing to election fund		☐	
124: Selling or Purchasing Office	☐		
380: Fraud – committed against Her Majesty			
418: Selling defective stores to Her Majesty			
In the last 3 years, have you, as the bidder, your affiliates or one of your directors, been convicted or have pleaded guilty of an offence in Canada or elsewhere under any of the following provisions [1]:			
Criminal Code			
119: Bribery of judicial officers,	☐	☐	
120: Bribery of officers			
346: Extortion			
366 to 368: Forgery and other offences resembling forgery			
382: Fraudulent manipulation of stock exchange transactions			
382.1: Prohibited insider trading			
397: Falsification of books and documents			
422: Criminal breach of Contract			
426: Secret commissions			
462.31 Laundering proceeds of crime			
467.11 to 467.13: Participation in activities of criminal organization			
Competition Act			
	☐	☐	

45: Conspiracies, agreements or arrangements between competitors 46: Foreign directives 47: Bid rigging 49: Agreements or arrangements of federal financial institutions			

[1] for which no pardon or equivalent has been received.

	Yes	No	Comments
52: False or misleading representation 53: deceptive notice of winning a prize			
Corruption of Foreign Public Officials Act 3: Bribing a foreign public official 4: Accounting 5: Offence committed outside Canada	☐	☐	
Controlled Drugs and Substance Act 5: Trafficking in substance 6: Importing and exporting 7: Production of substance	☐	☐	
Other Acts 239: False or deceptive statements of the Income Tax Act 327: False or deceptive statements of the Excise Tax Act	☐	☐	

Additional Comment

☐ I, (name)_____, (position)_____, of (company name bidder)_____ _____authorise PWGSC to collect and use the information provided, in additional to any other information that may be required to make a determination of ineligibility and to publicly disseminate the results.

☐ I, (name) _____, (position) _____, of (company name bidder)_____certify that the information provided in this form is, to the best of my knowledge, true and complete. Moreover, I am aware that any erroneous or missing information could result in the cancellation of my bid as well as a determination of ineligibility/suspension.

We appreciate your interest in doing business with The Government of Canada and your understanding on the additional steps that we need to take to protect the integrity of PWGSC's procurement process.

PART 4:

Question 58: Artificial Intelligence (AI) is an important technology that we feel is under-represented in the current set of requirements. Advanced AI capabilities such as discovery and associated improvements over time from machine learning, will be important for those departments where the ATIP service delivery costs attributable to human research/review efforts are large vs. the cost-savings that come from optimizing/standardizing workflows. We believe once the successful bidder(s) solution is deployed, departments with significant ATIP volumes will quickly want this and other functional enhancements.

Therefore, we recommend that a mandatory requirement (or alternatively, a high-value rated requirement) be added such that Canada can evaluate the level of effort required to INTEGRATE advanced Artificial Intelligence features specifically, and other capabilities generally, into any turnkey solution(s) procured as a result of this competition. This type of "extendable" architecture would benefit Canada and Canadians by allowing departments and third party ISVs and/or public cloud services providers to effectively "plug in" to add/replace/enhance important functionality at significantly lower costs over time.

Answer 58:

The GC recognizes the importance of Artificial Intelligence (AI) technology in supporting institutions achieve greater efficiencies in processing ATIP requests. In support of these capabilities the bid solicitation states that **the RPSS must achieve the following: (i) Automate or increase efficiency of electronically processing ATIP requests and administrative processes; (..) (xiii) Utilize innovative web**

technologies for integrated and cost-effective solutions; (xx) Offers a range of functionality levels for the processing of ATIP requests by GC institutions that have a need for higher levels of automation, integration and reporting; and (xxi) Offers additional functionality that can support GC institutions with advanced levels of automation, system integration, and specialized functionality for the delivery of their ATIP services.

As for adding an additional requirement to evaluate the level of effort required to integrate advanced AI features (and other capabilities) into a turnkey solution, the GC has allocated rated requirements R53 and R89 the highest scores (20 points) that can be given to a software feature. AI rates for almost 10% of the overall Tier II score. If the bidder's software solution is designed with extendable architecture, it is then up to the bidder to demonstrate how it can deliver with this type of architecture at a lower cost. If the proposed solution is modular, then each module should be detailed in the proposal and explain how each module can integrate with the proposed solution.

Question 59: Will Canada consider extending the Bid Solicitation period?

Answer 59: No further extensions will be made at this time.

Question 60: In instructions to bidder 2.1 and under epost connect, section 2a offers an ebid submission option from the vendor. Form 5 suggests we submit this form as part of our bid and on this form it is in a sealed envelope sent to Integrity, Departmental Oversight Branch. Is this sealed submission necessary or is this just an older form assuming we would be submitting hard copies and NOT submitting through epost?

Answer 60: Form 5 has been amended above in Part 3. Form 5 is to be submitted as part of the e-Bid submission.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.