RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

Revision to a Request for Supply Arrangement - Révision à une demande pour un arrangement en matière d'approvisionnement

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
Mainframe & Business Software Procurement Division / Div des achats des ordi principaux et des logiciels de gestion
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Quebec
K1A 0S5

Title - Sujet RFSA - SaaS Method of Supply (GC)	
Solicitation No. - N° de l'invitation EN578-191593/F	**Date** 2019-12-03
Client Reference No. - N° de référence du client 20191593	**Amendment No. - N° modif.** 007
File No. - N° de dossier 003eem.EN578-191593	**CCC No./N° CCC - FMS No./N° VME**
GETS Reference No. - N° de référence de SEAG PW-$EEM-003-35660	
Date of Original Request for Supply Arrangement **Date de demande pour un arrangement en matière d'app. originale**	2019-05-10
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2022-05-10**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
Address Enquiries to: - Adresser toutes questions à: Boyer, Tania	**Buyer Id - Id de l'acheteur** 003eem
Telephone No. - N° de téléphone (613) 858-9232 ( )	**FAX No. - N° de FAX** ( ) -
Delivery Required - Livraison exigée See Herein	
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** DEPARTMENT OF PUBLIC WORKS AND GOVERNMENT SERVICES CANADA PORTAGE III 6B1 11 LAURIER ST Gatineau Quebec K1A0S5 Canada	
Security - Sécurité This revision does not change the security requirements of the solicitation. Cette révision ne change pas les besoins en matière de sécurité de l'invitation.	

Instructions: See Herein

Instructions: Voir aux présentes

Acknowledgement copy required **Accusé de réception requis**	**Yes - Oui** ☐	**No - Non** ☐

The Offeror hereby acknowledges this revision to its Offer.
Le proposant constate, par la présente, cette révision à son offre.

Signature **Date**

Name and title of person authorized to sign on behalf of offeror. (type or print)
Nom et titre de la personne autorisée à signer au nom du proposant.
(taper ou écrire en caractères d'imprimerie)

For the Minister - Pour le Ministre

Canada

Item Art.	Description	Dest. Code Dest.	Inv. Code Fact.	Quantity - Quantité Current Courant	Inc./Dec. Augm/dim.	Revised Révisée	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM Destination	Plant/Usine	Del. Req. Liv. Req.	Del. Offered Liv. offerte
1	PSPC CLOUD METHOD OF SUPPLY NPP Amendment D	EN578	EN578		1	1	LOT	$	$	See Herein	
5	PSPC CLOUD NPP AMENDMENT D	EN578	EN578		1	1	LOT	$	$	See Herein	
7	AMENDMENT 007	Total			1	1	Each	$	$		

PUBLIC SERVICE AND PROCUREMENT CANADA (PSPC)

Amendment no. 007 to Request for Supply Arrangement (RFSA) for

SaaS Method of Supply (GC CLOUD)

Buy&Sell Solicitation Reference Number: EN578-191593/F

THIS AMENDMENT 007 IS RAISED TO:	
1.0	Respond to questions received regarding the RFSA, as detailed in Section 1.0, below;
2.0	Modify the RFSA as detailed in Section 2.0, below;
3.0	Modify Annex F - Resulting Contract Clauses, as detailed in Section 3.0, below;
4.0	Delete Appendix E – Security Requirements for Canadian Contractor and Appendix F – Security Requirements for Foreign Contractor from the Resulting Contract Clauses and insert as Annex G – Security Requirements for Canadian Suppliers and Annex H – Security Requirements for Foreign Suppliers under the RFSA, as detailed in Section 4.0, below;
5.0	Insert Annex I – SRCL for SaaS under the RFSA, as detailed in Section 5.0, below;
6.0	Insert Annex J – SRCL Security Classification Guide under the RFSA, as detailed in Section 6.0, below;
7.0	Insert Annex K – PSPC Non-Disclosure Agreement related to Supply Chain Integrity under the RFSA, as detailed in Section 7.0, below;
8.0	Insert Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process under the RFSA, as detailed in Section 8.0, below;
9.0	Insert Appendix F – SRCL for SaaS under Annex F, Resulting Contact Clauses, as detailed in Section 9.0, below;
10.0	Insert Appendix G – SRCL Security Classification Guide under Annex F, Resulting Contact Clauses, as detailed in Section 10.0, below;
11.0	Modify Form 5 – Submission Completeness Review Checklist under the RFSA, as detailed in Section 11.0, below; and,
12.0	Modify Form 6 - SCI Submission Template under the RFSA, as detailed in Section 12.0, below.
NOTE: Respondents' clarification questions are numerically sequenced upon arrival at PSPC. Respondents are hereby advised that questions and answers for this solicitation may be issued via BuyandSell.gc.ca out of sequence.	

1.0 Respond to questions regarding the RFSA:

Note: Questions may have been modified and/or condensed.

DELETE	INSERT
Q.44 Section IV: Supply Chain Integrity Process of the RFSA and Annex G: Supply Chain Integrity Process Global hyperscale cloud providers deliver solutions at an unprecedented scale and as a result does not align with this requirement which was designed for custom-built hosted solutions. While the specific approach is intractable for global, hyper-scale cloud providers, there is broad alignment of the supply chain integrity processes with the NIST 800-161. Therefore we respectfully ask that cloud providers are asked to demonstrate alignment with NIST 800-161 rather than the Supply Chain Process in Section IV."	**A.44** The requirements for Supply Chain Integrity have been modified as per Section 2.0, below. Suppliers are required to demonstrate compliance with Sections 3.5 - Supply Chain Integrity Requirements and 4.3 - Supply Chain Integrity Process of the RFSA with regards to Supply Chain Integrity.
Q.45 Where a Bidder leverages a qualified Cloud Service Provider (CSP) please confirm that only the DUNS Number for the CSP is required to submit within	**A.45** PSPC confirms that the Supplier must provide Form 6 - SCI Submission Template as part of its Submission to be declared responsive. Canada

DELETE	INSERT
the Ownership Information section, and not the IT Products List. This level of detail is proprietary and protected by the CSP and thus would only be communicated directly to the CCCS.	provides additional protection for information submitted in response to Form 6 – SCI Submission Template, as provided by terms of the non-disclosure agreement contained in Annex K, PSPC Non-Disclosure Agreement related to Supply Chain Integrity. In accordance with Section 2.1 of this RFSA, Standard Acquisition Clauses and Conditions (SACC) Manual Clause 2008 Standard Instructions - Request for Supply Arrangements - Goods or Services forms part of the RFSA. SACC 2008 05(6) provides that "All arrangements will be treated as confidential, subject to the provisions of the *Access to Information Act* (R.S., 1985, c. A-1), and the *Privacy Act* (R.S., 1985, c. P-21)." Please also refer to Section 4.3, Supply Chain Integrity Process below, for more information about the SCI Process.
Q.46 After presenting my Submission PSPC realizes that documents are missing. Will my company be disqualified from the RFSA process?	**A.46** The RFSA is intended to be a collaborative qualification process. Submissions that do not meet all of the requirements of the RFSA will not be disqualified. Once a Submission is received and reviewed, PSPC will contact the Supplier and request clarifications and/or missing documents, if required.
Q.47 Under Annex A – Qualification Requirements Tier 2 Assurance (Up to and including Protected B Data) M7 Personnel Security states: The Supplier of the proposed Commercially Available Software as a Services must implement security measures that grant and maintain the required level of security screening for its respective personnel, as well as the personnel of any subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. Given M7 is under Tier 2 that includes Protected B Data, can the Crown please confirm that the level of the security screening for its respective personnel will be at the Reliability level for this requirement. To reaffirm, if the Commercially Available Software as a Service has the ability to store and process protected B data, all personnel that has access privileges to the SaaS will be required to maintain a Government of Canada Reliability clearance.	**A.47** PSPC confirms that personnel, as well as the personnel of any subcontractor personnel that has access privileges to information system assets on which Canada's Data is stored and processed will be required to maintain a Government of Canada Reliability or Secret clearance. Please refer to Annex G – Security Requirements for Canadian Contractor Annex H – Security Requirements for Foreign Contractor, Annex I – SRCL for SaaS and Annex J – SRCL Security Classification Guide under the RFSA, as applicable. As requested under the requirements outlined in Annex A – Qualification Requirements, M4, Tier 1 and M7, Tier 2 (Personnel Security) of the RFSA must be met to be declared responsive. Different or additional security levels may apply to Clients using the SA or their Work requirements, for example, security clearances for Suppliers or Supplier resources. In the event that a Contract issued against a Supply Arrangement includes different or additional security levels, they will be included in Appendix I (SRCL) and Appendix J (SRCL Security Classification Guide) to the Contract. The requirements for Security Clearance have been modified as per Section 2.0, below. Suppliers are required to demonstrate compliance with Sections 3.6 - Section V: Security Clearance Requirements of the RFSA with regards to Security Clearance.

DELETE	INSERT
Q.48 Can the Crown please announce when Supply Arrangements are awarded to compliant Bidders? The announcement would include the name of the compliant bidder and the tier of the award.	**A.48** Suppliers may present a Submission for a Supply Arrangement at any time by responding to the most recent terms and conditions posted on Buy&Sell. Canada reserves the right to issue Supply Arrangements to Suppliers who present a Submission that meets all of the mandatory criteria of the RFSA throughout the entire period of the RFSA. Evaluations of such Submissions will be processed on an ongoing basis. Once a Supply Arrangement has been issued, the title of the SA, the description and the start date will appear under solicitation number EN578-191593/F on Buy and Sell.
Q.49 Does there need to be a written response submitted for Annex B – Security and Privacy Obligations? Or is this something that needs to be signed and acknowledged?	**A.49** PSPC confirms that Suppliers must comply with Annex B – Security and Privacy Obligations at the Submission stage and for the duration of their Supply Arrangement. Suppliers will demonstrate compliance with Annex B – Security and Privacy Obligations by demonstrating compliance with the requirements detailed in Annex A – Qualification Requirements, Tier 1 or Tier 2 (as applicable). Section 3.2 (c) (vii) of the RFSA has been modified to provide clarity on the demonstration of compliance, as per Section 2.0 of this Amendment.
Q.50 Canada is requesting that industry submit certain sensitive and confidential information in the arrangement. What assurances will Canada provide to protect this information from being disclosed?	**A.50** 1. Section 2.1 of this RFSA states that Standard Acquisition Clauses and Conditions (SACC) Manual Clause 2008 Standard Instructions - Request for Supply Arrangements - Goods or Services forms part of the RFSA. SACC 2008 05(6) provides that: "All arrangements will be treated as confidential, subject to the provisions of the Access to Information Act (R.S., 1985, c. A-1), and the Privacy Act (R.S., 1985, c. P-21)." 2. Canada provides additional protection for information submitted in response to Form 6 – SCI Submission Template, as provided by terms of the non-disclosure agreement contained in Annex K, PSPC Non-Disclosure Agreement related to Supply Chain Integrity. 3. Canada recommends that Suppliers mark all confidential information as confidential, in accordance with Section 2.2, (d) of the RFSA. 4. The *ATIA* prohibits PSPC from disclosing such confidential information:

DELETE	INSERT
	ATIA Section 20 **Third Party Information** **20 (1)** Subject to this section, the head of a government institution shall refuse to disclose any record requested under this Part that contains (b) financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party and is treated consistently in a confidential manner by the third party; **In accordance with ATIA Section 27 (1) "**If the head of a government institution intends to disclose a record requested under this Part that contains or that the head has reason to believe might contain trade secrets of a third party, information described in paragraph 20(1)(b) or (b.1) that was supplied by a third party, or information the disclosure of which the head can reasonably foresee might effect a result described in paragraph 20(1)(c) or (d) in respect of a third party, the head shall make every reasonable effort to give the third party written notice of the request and of the head's intention to disclose within 30 days after the request is received." **In accordance with ATIA Section 28 (1)** Where a notice is given by the head of a government institution under subsection 27(1) to a third party in respect of a record or a part thereof, (a) the third party shall, within twenty days after the notice is given, be given the opportunity to make representations to the head of the institution as to why the record or the part thereof should not be disclosed; and (b) the head of the institution shall, within thirty days after the notice is given, if the third party has been given an opportunity to make representations under paragraph (a), make a decision as to whether or not to disclose the record or the part thereof and give written notice of the decision to the third party. **In accordance with ATIA Section 44 (1)** Any third party to whom the head of a government institution is required under paragraph 28(1)(b) to give notice of a decision to disclose a record or a part of a record under this Part may, within 20 days after the notice is given, apply to the Court for a review of the matter. **PSPC does not purport to provide any legal advice but provides excerpts, as identified by the PSPC ATIP Office describing the ATIP request handling**

DELETE	INSERT
	process. Suppliers seeking legal advice must consult independent legal counsel.

2.0 Modify the Request for Supply Arrangement (RFSA) as follows:

AT	DELETE	INSERT
Section 1.1.3, Structure of the RFSA	The Annexes include the Qualification Requirements, Security Requirements, and SaaS Solutions and Ceiling Prices, SaaS Service Level Agreement (SLA) the SaaS Bid Solicitation Template, Resulting Contract Clause, Supply Chain Integrity Process and Non-Disclosure Agreement related to Supply Chain Integrity.	The Annexes include the Qualification Requirements, Security Requirements, SaaS Solutions and Ceiling Prices, SaaS Service Level Agreement (SLA) the SaaS Bid Solicitation Template, Resulting Contract Clause, PSPC Non-Disclosure Agreement related to Supply Chain Integrity and SaaS IT Security (ITS) Assessment Program onboarding process.
Section 1.3 (c) Overview of the Submission Review Process	c) **Stream 3:** will include Submissions from Value-Added Resellers of SaaS Solutions and Services. Value-Added Resellers who intend to present a Submission to qualify as a Supplier must comply with Annex A, Qualification Requirements, Tier 1 and must submit certifications from the SaaS Publisher, in accordance with the SaaS Publisher Authorization Form (Form 3), to certify that the Supplier has been authorized to supply the SaaS Solution Publisher's Solution(s).	c) **Stream 3:** will include Submissions from Value-Added Resellers of SaaS Solutions and Services. Value-Added Resellers who intend to present a Submission to qualify as a Supplier must comply with Annex A, Qualification Requirements, Tier 1 for up to Protected A and must submit certifications from the SaaS Publisher, in accordance with the SaaS Publisher Authorization Form (Form 3), to certify that the Supplier has been authorized to supply the SaaS Solution Publisher's Solution(s). **Value-Added Resellers will not be permitted to qualify under Protected B.**
Section 2.2(d) Presentation of Submissions		(d) **Submission of Confidential Information.** Suppliers are asked to mark all confidential information included in their Submission as confidential. The confidential information must be clearly identified by marking each page containing such information as "Confidential" and by highlighting all confidential information therein.
Section 3.2 (c) (v) Service Level Agreements	(v) **Service Level Agreements (SLA):** Suppliers must submit their published Service Level Agreements (SLAs), to be included in Annex D – SaaS Solution Service Level Agreements (SLA).	(v) **Service Level Agreements (SLA):** Suppliers must submit their published Service Level Agreements (SLAs), to be included in Annex D – SaaS Solution Service Level Agreements (SLA). Similarly, any terms contained in Annex D – SaaS Solution Service Level Agreements which include pricing information, such as (but not limited to) those that attempt to impose financial conditions, pricing terms, or compliance penalties, shall be deemed stricken and are of no force or effect.
Section 3.2 (c) (v) Service Level Agreements	(v) Terms and conditions related to service levels and service delivery under the SLAs are limited to the following:	(v) Terms and conditions related to service levels and service delivery under the SLAs must include the following:
Section 3.2 (c) (vii)	(vii) **Compliance with Annex B – Security & Privacy Obligations**: Suppliers must comply with security and privacy	(vii) **Compliance with Annex B – Security & Privacy Obligations.** Suppliers must comply with the obligations contained in

AT	DELETE	INSERT
Compliance with Annex B – Security & Privacy Obligations	obligations contained in Annex B – Security & Privacy Obligations. The Suppliers must provide the written evidence or certification documents to demonstrate their compliance to the Security & Privacy Obligations as detailed in Annex B.	Annex B – Security & Privacy Obligations when presenting a Submission and for the duration of their Supply Arrangement. Suppliers must demonstrate that they meet the security and privacy obligations detailed in Annex B by responding to the mandatory requirements detailed in Annex A – Qualification Requirements, Tier 1 & Tier 2 (as applicable). Suppliers may be requested to demonstrate their ongoing compliance with Annex B – Security & Privacy Obligations upon request throughout the period of any Contract issued against the Supply Arrangement.
Section 3.2 (c) (ix) Confirmation of registration for the SaaS IT Security (ITS) Assessment: Onboarding		(viii) **Confirmation of registration for the SaaS IT Security (ITS) Assessment: Onboarding Program (Stream 1, Stream 2 and Stream 3):** The response must include documentation confirming that the SaaS Publisher or the Value Added Reseller of the proposed Solution(s) is registered for the SaaS Security Assessment Process as described in Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process.
Section 3.3, Section II: Financial Submission	(a) Where a link is provided to an online catalogue in accordance with option 1, Canada reserves the right to request that the Supplier include in their online catalogue all of the information requested in sub-section (d) below. Where a table is provided in accordance with option 2, Canada reserves the right to request that Suppliers make this information available via an online catalogue in the future.	(a) Where a link is provided to an online catalogue in accordance with option 1, Canada reserves the right to request that the Supplier include in their online catalogue all of the information requested in sub-section (d) below. Where a table is provided in accordance with option 2, Canada reserves the right to request that Suppliers make this information available via an online catalogue in the future. Any pricing information included elsewhere in the Supplier's Submission, including in Annex D – SaaS Solution Service Level Agreements shall be deemed stricken and is of no force or effect.
Section 3.5, (iv): Supply Chain Integrity Process	**3.5 Section IV: Supply Chain Integrity Process** (a) Suppliers must submit specific information regarding each component of their proposed Solution's supply chain ("Supply Chain Security Information" or "SCSI") as defined in Section 1.1 of **Annex G, Supply Chain Integrity Process** Section 4.3.	**3.5 Section IV: Supply Chain Integrity Requirements** (a) Suppliers must meet the SCI requirements outlined in Annex A – Qualification Requirements, M6 and M7, Tier 1 for up to Protected A and M10 and M11, Tier 2 for up to Protected B (Supply Chain Management) of the RFSA. The requirements must be met before a Supply Arrangement is awarded.

AT	DELETE	INSERT
	(b) Suppliers must submit Supply Chain Security Information submitted in **Form 6 – SCI Submission Template,** and must keep current, or update, any SCSI as required by the Supply Chain Security Authority. The Supply Chain Security Information will be used by Canada to assess whether, in its opinion, a Supplier's proposed supply chain creates the possibility that the Supplier's proposed SaaS Solutions 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 Integrity Process as described in **Annex G, Supply Chain Integrity Process**. (c) By submitting its SCSI, and in consideration of the opportunity to participate in this procurement process, the Supplier agrees to the terms of the non-disclosure agreement contained in **Annex H, Non-Disclosure Agreement related to Supply Chain Integrity.**	(b) Suppliers must submit Supply Chain Security Information detailed in Form 6 – SCI Submission Template, and must keep current, or update, any SCSI as required by the Supply Chain Security Authority. The Supply Chain Security Information will be used by Canada to assess whether, in its opinion, a Supplier's proposed supply chain creates the possibility that the Supplier's proposed SaaS Solutions 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 Integrity Process as described in Section 4.3, Supply Chain Integrity Process. (c) By submitting its SCSI, and in consideration of the opportunity to participate in this procurement process, the Supplier agrees to the terms of the non-disclosure agreement contained in Annex K, PSPC Non-Disclosure Agreement related to Supply Chain Integrity.
Section 3.6 , (v) Security Clearance Requirements		**3.6 Section V: Security Clearance Requirements** (a) **Security Clearance Requirements**: Suppliers must meet the security clearance requirements outlined in Annex A – Qualification Requirements, M4, Tier 1 for up to Protected A and M7, Tier 2 for up to Protected B (Personnel Security) of the RFSA. The requirements must be met before a Supply Arrangement is awarded. (b) **Contractor/Sub-processor/Subcontractor:** Contractor/Sub-processor/Subcontractor must meet the security requirements outlined in Annex G – Security Requirements for Canadian Contractor Annex H – Security Requirements for Foreign Contractor, Annex I – SRCL for SaaS and Annex J – SRCL Security Classification Guide, as applicable. (c) **Timing**: Suppliers should take steps to obtain the required security clearances promptly. The security clearance requirements must be met before the award of a Supply Arrangement.

AT	DELETE	INSERT
		(d) **Joint Venture Supplier:** Unless otherwise specified in the solicitation, in the case of a joint venture, each member of the joint venture must meet the security requirements, outlined in (b) above. (e) **CCCS Conducts Clearance Process**: PSPC has an arrangement with the Canadian Centre for Cyber Security to process security clearances in parallel with the SaaS IT Security (ITS) Assessment, and does not control the process itself. It can be a lengthy process and Suppliers should initiate it as soon as possible. For additional information on security requirements, Suppliers should refer to: contact@cyber.gc.ca.
Section 4.2.3 Mandatory Security Evaluation		**4.2.2 Mandatory Security Evaluation** The mandatory security requirements are as follows: (i) Organization and personnel clearances (as per Annex G – Security Requirements for Canadian Contractor Annex H – Security Requirements for Foreign Contractor, Annex I – SRCL for SaaS and Annex J – SRCL Security Classification Guide of the RFSA) (ii) Supply Chain Integrity (as per 4.3) (iii) SaaS IT Security (ITS) Assessment Program: Onboarding Process (as per Annex L)
Section 4.3 Supply Chain Integrity Process	**4.3 Supply Chain Integrity Process** During the RFSA process, the SA period and any resulting contract period, the Supply Chain Security Authority identified by Canada, may, based on its National Security mandate to protect Canada's IT infrastructure as well as to assess threats, risks and vulnerabilities, assess the Supplier SCSI. Canada will assess whether, in its opinion, the Supplier's supply chain creates the possibility that supplier's supply chain or proposed solution could compromise or be used to compromise	**4.3 Supply Chain Integrity Process** (a) Supply Chain Integrity (SCI) is examined during the SaaS IT Security (ITS) Assessment. SCI assessments are another level of assurance to confirm that implemented security controls are less likely to be maliciously undermined by threat actors through supply chain attacks. (b) For SaaS providers, the SCI process initiated by Shared Services Canada (SSC) is used. In this process, the SaaS provider gives a list of the software, hardware, contractors, and suppliers that are used to deliver the service offering. The provider also updates the GC periodically to note any changes to the initial list. If the GC determines that the list of

AT	DELETE	INSERT
	the security integrity of Canada's equipment, firmware, software, systems or information, or represents a threat to Canada's National Security, in accordance with Section 2 of Annex G, Supply Chain Integrity Process. It is a condition precedent to any contract award that a Supplier successfully satisfy the Security Authority's Supply Chain Integrity assessment. Canada will assess whether, in its opinion, the Supplier's supply chain creates the possibility that Suppliers' proposed solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information in accordance with Section 4 of Annex G, Supply Chain Integrity Process.	software, hardware, contractors, and suppliers is extensive, level one SCI safeguards may be required. (c) **SCI Process:** PSPC has an arrangement with the Canadian Centre for Cyber Security in consultation with Shared Services Canada where applicable to process SCI assessment in parallel with the IT Security Assessment, and does not control the process itself. It can be a lengthy process and Suppliers should initiate it as soon as possible. For additional information on security requirements, Suppliers should refer Please refer to Annex L: SaaS IT Assessment (ITS) Program: Onboarding Process for more details on the onboarding process. (d) Please refer to Annex L: SaaS IT Assessment (ITS) Program: Onboarding Process for more details on the onboarding process. For additional information on security requirements, Suppliers should refer to: contact@cyber.gc.ca.
Section 6.8 Priority of Documents	**6.8 Priority of Documents** (a) The articles of the Supply Arrangement; (b) The general conditions 2020 (2017-09-21), General Conditions - Supply Arrangement - Goods or Services; (c) Annex A, Qualification Requirements; (d) Annex B, Security & Privacy Obligations; (e) Annex F, Resulting Contract Clauses; (f) Annex E, Bid Solicitation Template; (g) Annex G, Supply Chain Integrity; (h) Annex H, Non-Disclosure Agreement; and, (i) The Supplier's Submission dated _____ (*insert date of Submission) (if the Submission was clarified or amended, insert at the time of issuance of the Supply Arrangement:* "as clarified on _____" ***or*** "as amended _____". *(Insert date(s) of clarification(s) or amendment(s), if applicable)*.	**6.8 Priority of Documents** (a) The articles of the Supply Arrangement; (b) The general conditions 2020 (2017-09-21), General Conditions - Supply Arrangement - Goods or Services; (c) Annex A, Qualification Requirements; (d) Annex B, Security and Privacy Obligations (e) Annex C, SaaS Solutions and Professional Services Ceiling Prices (f) Annex D, SaaS Service Level Agreements (SLA) (g) Annex E, Bid Solicitation Template; (h) Annex F, Resulting Contract Clauses; (i) Annex G, Security Requirements for Canadian Contractor; (j) Annex H, Security Requirements for Foreign Contractor; (k) Annex I, SRCL of SaaS; (l) Annex J, SRCL Security Classification Guide; (m) Annex K, PSPC Non-Disclosure Agreement related to Supply Chain Integrity; (n) Annex L, SaaS IT Security (ITS) Assessment Program: Onboarding Process and, (o) The Supplier's Submission dated _____ (*insert date of Submission) (if*

AT	DELETE	INSERT
		the Submission was clarified or amended, insert at the time of issuance of the Supply Arrangement: "as clarified on _____" ***or*** "as amended _____". *(Insert date(s) of clarification(s) or amendment(s), if applicable)*.
Annex G – Supply Chain Integrity Process	Annex G – Supply Chain Integrity Process in its entirety.	Annex G – Security Requirements for Canadian Contractor, as detailed in Section 4.0, below.
Annex H – Non-Disclosure Agreement related to Supply Chain Integrity	Annex H – Non-Disclosure Agreement related to Supply Chain Integrity.	Annex H – Security Requirements for Foreign Contractor, as detailed in Section 4.0, below.
Annex I – SRCL for SaaS		Annex I – SRCL for SaaS is hereby added to the RFSA, as detailed in Section 5.0, below.
Annex J – SRCL Security Classification Guide		Annex J – SRCL Security Classification Guide is hereby added to the RFSA, as detailed in Section 6.0, below.
Annex K – PSPC Non-Disclosure Agreement related to Supply Chain Integrity		Annex K – PSPC Non-Disclosure Agreement related to Supply Chain Integrity is hereby added to the RFSA, as detailed in Section 7.0, below.
Annex L – SaaS ITS Assessment Program: Onboarding Process		Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process is hereby added to the RFSA, as detailed in Section 8.0, below.

3.0 Modify Annex F - Resulting Contract Clauses as follows:

AT	DELETE	INSERT
Section 2.1, c) and d) Auto Renewal Notification	c) **Auto-Renewal Notification.** The Contractor acknowledges that, despite Canada's agreement to the Contractor's standard commercial terms, Canada is subject to a legal regulatory framework governing financial expenditure authority. d) **Auto-Renewal Notification.** The Contractor agrees to provide notification functionality or tool to Canada as part of the Services, to assist Canada in administering the Contract. The Contractor further agrees to send notifications to both the Contracting Authority and the Technical Authority in advance of the expiry of the Contract Period. e) **Grace Period.** The Contractor agrees to provide Canada with an optional grace period of 4 weeks to terminate the Contract Period, in the event that Canada fails to stop its usage of the Service on or before the end of the defined Contract Period. At any time before the expiry of the grace period, and notwithstanding any auto-renewal clause elsewhere in the Contract, the Contracting Authority may terminate the Contract by providing written notice to the Contractor of Canada's decision to terminate the Contract. Upon delivery of the notice, the termination will take effect immediately or, at the time specified in the termination notice. Canada will be released from further obligation under the Contract after the termination date, and will be specifically released from any extended term resulting from an auto-renewal clause. The Contractor will apply no penalty or additional fees in these circumstances. f) **Canada's Responsibility.** Notwithstanding the provision of the grace period, Canada remains responsible to monitor its obligations under the Contract, including fees, renewal and expiry dates, consumption, usage, payment, termination and renewals.	c) **Auto-Renewal Notification.** The Contractor acknowledges that, despite Canada's agreement to the Contractor's standard commercial terms, Canada is subject to a legal regulatory framework governing financial expenditure authority. The Contractor agrees to provide notification functionality or tool to Canada as part of the Services, to assist Canada in administering the Contract. The Contractor further agrees to send notifications to both the Contracting Authority and the Technical Authority in advance of the expiry of the subscription services or Contract Period. d) **Grace Period.** The Contractor agrees to provide Canada with an optional grace period of 4 weeks to terminate the Contract Period, in the event that Canada fails to stop its usage of the Service on or before the end of the defined Contract Period. At any time before the expiry of the grace period, and notwithstanding any auto-renewal clause elsewhere in the Contract, the Contracting Authority may terminate the Contract by providing written notice to the Contractor of Canada's decision to terminate the Contract. Upon delivery of the notice, the termination will take effect immediately or, at the time specified in the termination notice. Canada will be released from further obligation under the Contract after the termination date, and will be specifically released from any extended term resulting from an auto-renewal clause. The Contractor will apply no penalty or additional fees in these circumstances. e) **Canada's Responsibility.** Notwithstanding the provision of the grace period, Canada remains responsible to monitor its obligations under the Contract, including fees, renewal and expiry dates, consumption, usage, payment, termination and renewals.
Appendix C – Security	**10. Supply Chain Risk Management**	**12. Supply Chain Risk Management**

AT	DELETE	INSERT
Obligations, Section 10. Supply Chain Risk Management	Within 30 days of contract award, the Contractor must provide an up-to-date Supply Chain Risk Management (SCRM) Plan that has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime. The SRCM Plan must be provided to Canada on an annual basis, or upon request, or promptly following any material Change to the SRCM Plan.	a) The Contractor must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide SaaS. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain. b) The Contractor must have a supply chain risk management approach including a Supply Chain Risk Management Plan that is aligned with one of the following best practices described under the Annex A – Qualification Requirements - Supply Chain Risk Management , mandatory requirement ID; M7 of Tier 1 and M11 of Tier 2: (i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); (ii) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or (iii) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan. c) Within 90 days of contract award, the Contractor must: (i) Provide an update that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime OR (ii) Provide Canada with a copy of the SRCM Plan on an annual basis, or upon request of Canada. In the situation where the Contractor is a SaaS Publisher using a GC-approved IaaS Provider that already complies with the Annex A – Qualification Requirements - Supply Chain Risk Management , mandatory requirement ID; M7 of Tier 1 and M11 of Tier 2 within 90 days of contract award, the SaaS

AT	DELETE	INSERT
		Publisher using a GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years."
Appendix C - Security Obligations Section 11. Sub-processors	(2) The Contractor must provide a list of Sub-processors that could be used to perform any part of the Public Cloud Services in providing Canada with the Solution. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the Public Cloud Services that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the Public Cloud Services. (3) The Contractor must provide a list of Sub-processors within ten days of the effective date of the Contract. The Contractor must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processors with access to Client Data or Personal Information.	a) The Contractor must provide a list of Sub-processors that could be used to perform any part of the Cloud Services in providing Canada with the Solution. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the scope activities that would be performed by the Sub-processor; and (iii) the country (or countries) where the Sub-processor would perform the activities required to support the Public Cloud Services. b) The Contractor must provide a list of Sub-processors within ten days of the Contract award date. The Contractor must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processors with access to Customer Data or Personal Data.
Appendix C - Security Obligations Section 13. On-going Supply Chain Integrity Process		a) The Parties acknowledge that security is a critical consideration for Canada with respect to this Contract and that on-going assessment of SaaS will be required throughout the Contract Period. b) The parties acknowledge that Canada reserves the right to review the native SaaS of any Contractor in whole or in part at any time for supply chain integrity concerns. This acknowledgement does not obligate the Contractor to support the SCI review. c) Throughout the Contract Period, the Contractor must provide to Canada information relating to any data breach of the Contractor's network of which it knows, that results in either (a) any unlawful access to Canada's content stored on Contractor's equipment or facilities, or (b) any unauthorized access to such equipment or

AT	DELETE	INSERT
		facilities, where in either case such access results in loss, disclosure or alteration of Canada's content in relation to change of ownership, to the SaaS under this Contract, that would compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications of Canada.
Annex F – Resulting Contract Clauses Section 14. Grant of Agent Authority		**14. Grant of Agent Authority** The Contractor advises Canada, and Canada acknowledges that the Contractor intends to appoint one of its Authorized Partners as its Authorized Agent ("Authorized Agent") to fulfill certain contractual obligations on behalf of the Contractor during the Contract, as defined in the Scope section below. The Contractor appoints its Authorized Partner, ***(to be completed at Contract Award)*** as its Authorized Agent under the Contract. The Authorized Agent Contact is: Name: Title: Telephone: Facsimile: E-mail address: The Contractor agrees to provide 30-days advance written notice to the Contracting Authority of any of the following: (i) its replacement of any Authorized Partner as Authorized Agent, (ii) any change to the scope of power delegated to the Authorized Agent, and (iii) the termination of the Authorized Agent. The Contractor agrees, upon request by the Contracting Authority, to immediately remove or replace the Authorized Agent. Removal or replacement of the Authorized Agent is in addition to any other remedy Canada may invoke. A breach by an Authorized Agent is a breach by the Contractor itself.

AT	DELETE	INSERT
Annex F – Resulting Contract Clauses Section 14.1 Grant of Agent Authority		**14.1 Scope of Agent Authority** The Contractor declares that the named Authorized Agent is authorized to transact business on the Contractor's behalf in matters relating to the supply of the goods and services under the Contract, limited to negotiating prices, providing billing information, invoicing, providing consumption reporting services, and receiving payment. The Contractor agrees that, upon proof of payment, any payment made by Canada to the Authorized Agent will be considered payment to the Contractor itself. This agency relationship (through which the Authorized Agent performs contractual obligations on behalf of the Contractor) does not amend, diminish or modify any of the responsibilities of the Contractor under the Contract. The Contractor agrees and understands that it is solely responsible for ensuring that all of its Authorized Agents comply with the applicable terms and conditions of the Contract, if the Authorized Agent fails to comply with the applicable terms and conditions, the Contractor must, upon written notification from the Contracting Authority, immediately complete and fulfill those obligations at no additional cost to Canada.
Appendix E – Security Requirements for Canadian Contractor	Appendix E – Security Requirements for Canadian Contractor	**Note to Suppliers:** Appendix E has been removed from the Resulting Contract Clauses and moved to Annex G – Security Requirements for Canadian Contractor because the security clearance assessment will be completed at the RFSA stage rather than the contracting stage.
Appendix F – Security Requirements for Foreign Contractor	Appendix F – Security Requirements for Foreign Contractor **Note to Suppliers:** Appendix F has been removed from the Resulting Contract Clauses and moved to Annex H – Security Requirements for Foreign Contractor because the security clearance assessment will be completed at the RFSA stage rather than the contracting stage.	Appendix F – SRCL for SaaS is hereby added to the RFSA, as detailed in Section 9.0, below.
Appendix G – Supply Chain Integrity Process	Appendix G – Supply Chain Integrity Process in its entirety.	Appendix G – SRCL Security Classification Guide is hereby added to the RFSA, as detailed in Section 10.0, below.

AT	DELETE	INSERT
	Note to Suppliers: Appendix G has been removed from the Resulting Contract Clauses and moved to Annex I: SaaS ITS Security Assessment Program: Onboarding Process because the SCI assessment will be completed at the RFSA stage rather than the contracting stage.	
Appendix H – Task Authorization Form	Appendix H – Task Authorization Form	Appendix E – Task Authorization Form.

4.0 DELETE Appendix E – Security Requirements for Canadian Contractor AND Appendix F – Security Requirements for Foreign Contractor from the Resulting Contract Clauses and INSERT Annex G – Security Requirements for Canadian Suppliers AND Annex H – Security Requirements for Foreign Suppliers under the RFSA as follows:

The CISD security requirements for Canadian and Foreign Contractor (Appendix E and Appendix F for reference) have been removed from the Software as a Service Resulting Contract Clauses and added to the RFSA stage (Annex G and Annex H for reference) to be assessed as part of the SaaS IT Security (ITS) Assessment prior to award of a Supply Arrangement.

Note to Contractors: Different or additional security levels may apply to Clients using the SA or their Work requirements, for example, security clearances for Suppliers or Supplier resources. In the event that a Contract issued against a Supply Arrangement includes different or additional security levels, they will be included in Appendix I (SRCL) and Appendix J (SRCL Security Classification Guide) to the Contract.

THE FOLLOWING SECURITY REQUIREMENTS MUST BE USED WHERE THE CONTRACTOR WILL HAVE ACCESS TO PROTECTED INFORMATION

The Contractor must comply with the requirements outlined in, as applicable:

(a) **Annex G – Security Requirements for Canadian Contractor**

(b) **Annex H – Security Requirements for Foreign Contractor**

Requirements being procured using the Supply Arrangement may also require Supplier (Canadian and foreign) to have Secret security clearance. Supplier can start the screening process for Organization and Personnel Security Screening at their earliest convenience. Details can be found at: https://www.tpsgcpwgsc.gc.ca/esc-src/enquete-screening-eng.html. If required, Supplier may contact the Supply Arrangement Authority who will sponsor any Organization and Personnel Security Screening requests.

ANNEX G – SECURITY REQUIREMENTS FOR CANADIAN CONTRACTOR

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 A or B (as applicable), issued by the Industrial Security Sector (ISS), **Public Services and Procurement Canada (PSPC), also referred to as PWGSC.**

2. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required by the security guide, granted or approved by the ISS/PWGSC.

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 A or B, as applicable, including an IT Link at the level of PROTECTED A or B, as applicable.
4. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of ISS/PWGSC.

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

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

NOTE: There are multiple levels of personnel security screenings associated with this file. In this instance, a security guide must be added to the SRCL clarifying these screenings. The security guide is normally generated by the organization's project authority and/or security authority.

ANNEX H – SECURITY REQUIREMENTS FOR FOREIGN CONTRACTOR

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). The Canadian DSA is the authority for confirming **Contractor/Subcontractor** compliance with the security requirements for foreign Contractors. The following security requirements apply to the foreign recipient **Contractor/Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada the Services and/or Work described in Contract, in addition to the Security Obligations and Privacy Obligations detailed in Appendix B & Appendix C, respectively.

1.1 The Foreign recipient **Contractor/Subcontractor** 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 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.

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

(a) The Foreign recipient **Contractor/Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

(b) The Foreign recipient **Contractor/Subcontractor** must not begin providing the Services and/or Work 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/Subcontractor** to provide confirmation of compliance and authorization for services to be performed.

(c) The Foreign recipient **Contractor/Subcontractor** 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/Subcontractor'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.

(d) The Foreign recipient **Contractor/Sub-processor/Subcontractor** must not grant access to **CANADA PROTECTED** information/assets, except to personnel who have been screened in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbssct.gc.ca/pol/doc-eng.aspx?id=28115), or use acceptable equivalent measures established by the Contractor in their publicly available documentation, and as agreed to by the Canadian DSA such as but not limited to:

(i) Personnel have a need-to-know for the performance of the **contract**;
(ii) 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;

(iii) The Foreign recipient **Contractor/Sub-processor/Subcontractor** 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; and

(iv) The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a foreign recipient **Contractor/Sub-processor/Subcontractor** for cause.

1.3 **CANADA PROTECTED** information/assets, provided to the foreign recipient **Contractor/Subcontractor** or produced by the Foreign recipient **Contractor/Subcontractor**, must:

(a) not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract / subcontract**, 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/subcontract** 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).

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

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

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

1.7 Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.

1.8 The Foreign recipient **Contractor/Subcontractor** must comply with the provisions of the attached Security Requirements Check List attached.

1.9 Canada has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor delivering Services to electronically access, process, produce, transmit or store **CANADA** PROTECTED A or B, as applicable, information/assets related to the delivery of Services and/or Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

1.10 Ownership of Personal Information and Records

To perform the Services and/or Work, the foreign recipient **Contractor/Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor/Subcontractor** 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/Subcontractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

1.11 Use of Personal Information

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

1.12 Collection of Personal Information

If the foreign recipient **Contractor/Subcontractor** must collect Personal Information from a third party to perform the Services and/Work, the foreign recipient **Contractor/Subcontractor** must only collect Personal Information that is required to perform the Services and/or Work. The foreign recipient **Contractor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor/Subcontractor** 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/Subcontractor**.

1.13 The foreign recipient **Contractor/Subcontractor** 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.

1.14 If requested by the Contracting Authority, the foreign recipient **Contractor/Subcontractor** 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/Subcontractor** 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.

1.15 At the time it requests Personal Information from any individual, if the foreign recipient **Contractor/Subcontractor** 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/Subcontractor** must ask the Contracting Security Authority for instructions.

1.16 Maintaining the Accuracy, Privacy and Integrity of Personal Information

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

(i) not use any personal identifiers (e.g. social insurance number) to link multiple databases

containing Personal Information;

(ii) segregate all Records from the foreign recipient **Contractor's/Subcontractor's** own information and records;

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

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

(v) if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor/Subcontractor** 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;

(vi) 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);

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

(viii) keep a record of the date and source of the last update to each Record;

(ix) 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/Subcontractor** and Canada at any time; and

(x) secure and control access to any hard copy Records.

1.17 Safeguarding Personal Information

(a) The foreign recipient **Contractor/Subcontractor** 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/Subcontractor** must:

(i) 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;

(ii) ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Services and/or Work;

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

(iv) 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;

(v) maintain a secure back-up copy of all Records, updated at least weekly;

(vi) implement any reasonable security or protection measures requested by Canada from time to time; and

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

1.18 Statutory Obligations

(a) The foreign recipient **Contractor/Subcontractor** 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/Subcontractor** 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.

(b) The foreign recipient **Contractor/Subcontractor** acknowledges that its obligations under the **contract/subcontract** 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/Subcontractor** believes that any obligations in the **contract/subcontract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor/Subcontractor** must immediately notify the Contracting Authority of the specific provision of the **contract/subcontract** and the specific obligation under the law with which the foreign recipient **Contractor/Subcontractor** believes it conflicts.

1.19 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/Subcontractor** must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

1.20 Complaints

Canada and the foreign recipient **Contractor/Subcontractor** 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.

1.21 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.

1.22 Auditing and Compliance

Canada may audit the foreign recipient including Contractor, and/or Sub-processor, and/or Subcontractor's, compliance with these supplemental general conditions at any time. If requested by the Contracting Authority, the foreign recipient Contractor/Sub-processor/Subcontractor 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/Sub-processor/Subcontractor must immediately correct the deficiencies at its own expense.

5.0 INSERT Annex I – SRCL for SaaS under the RFSA as follows:

ANNEX I – SRCL FOR SAAS

Clear Data - Effacer les données

Government of Canada / Gouvernement du Canada

English Instructions | Instructions français

Contract Number / Numéro du contrat

Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
4. Brief Description of Work - Brève description du travail	

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No / Non	☐ Yes / Oui
6. Indicate the type of access required - Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☑ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p.ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciales **sans** entreposage de nuit?	☑ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑ Not releasable / À ne pas diffuser ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	All NATO countries / Tous les pays de l'OTAN ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	No release restrictions / Aucune restriction relative à la diffusion ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Security Classification / Classification de sécurité
UNCLASSIFIED

TBS/SCT 350-103 (2004/12)

Canada

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets: ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :

Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET - SIGINT / TRÈS SECRET - SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : Refer to Appendix A - Security Classification Guide

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? ☐ No / Non ☑ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted: ☐ No / Non ☑ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? ☐ No / Non ☑ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

PART C *(continued)* / PARTIE C *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	Confidential Confidentiel	Secret	Top Secret Très Secret	NATO Restricted NATO Diffusion Restreinte	NATO Confidential NATO Confidentiel	NATO Secret	COSMIC Top Secret COSMIC Très Secret	Protected Protégé A	 B	 C	Confidential Confidentiel	Secret	Top Secret Très Secret
Information / Assets Renseignements / Biens	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Production	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
IT Media Support TI	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
IT Link Lien électronique	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?
☑ No Non ☐ Yes Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée.

12. b) Will the document attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?
☑ No Non ☐ Yes Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☐ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

17. Contracting Security Authority / Autorisé contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

Form

Next Page

Instructions for completion of a Security Requirements Check List (SRCL)

The instruction sheet should remain attached until Block #17 has been completed.

GENERAL - PROCESSING THIS FORM

The project authority shall arrange to complete this form.

The organization security officer shall review and approve the security requirements identified in the form, in cooperation with the project authority.

The contracting security authority is the organization responsible for ensuring that the suppliers are compliant with the security requirements identified in the SRCL.

All requisitions and subsequent tender / contractual documents including subcontracts that contain PROTECTED and/or CLASSIFIED requirements must be accompanied by a completed SRCL.

It is important to identify the level of PROTECTED information or assets as Level "A," "B" or "C," when applicable; however, certain types of information may only be identified as "PROTECTED". No information pertaining to a PROTECTED and/or CLASSIFIED government contract may be released by suppliers, without prior written approval of the individual identified in Block 17 of this form.

The classification assigned to a particular stage in the contractual process does not mean that everything applicable to that stage is to be given the same classification. Every item shall be PROTECTED and/or CLASSIFIED according to its own content. If a supplier is in doubt as to the actual level to be assigned, they should consult with the individual identified in Block 17 of this form.

PART A - CONTRACT INFORMATION

Contract Number (top of the form)

This number must be the same as that found on the requisition and should be the one used when issuing an RFP or contract. This is a unique number (i.e. no two requirements will have the same number). A new SRCL must be used for each new requirement or requisition (e.g. new contract number, new SRCL, new signatures).

1. **Originating Government Department or Organization**

   Form

   Enter the department or client organization name or the prime contractor name for which the work is being performed.

2. **Directorate / Branch**

   This block is used to further identify the area within the department or organization for which the work will be conducted.

3. a) **Subcontract Number**

   If applicable, this number corresponds to the number generated by the Prime Contractor to manage the work with its subcontractor.

   b) **Name and Address of Subcontractor**

   Indicate the full name and address of the Subcontractor if applicable.

4. **Brief Description of Work**

   Provide a brief explanation of the nature of the requirement or work to be performed.

5. a) **Will the supplier require access to Controlled Goods?**

   The Defence Production Act (DPA) defines "Controlled Goods" as certain goods listed in the Export Control List, a regulation made pursuant to the *Export and Import Permits Act* (EIPA). Suppliers who examine, possess, or transfer Controlled Goods within Canada must register in the Controlled Goods Directorate or be exempt from registration. More information may be found at www.cgd.gc.ca.

   b) **Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?**

   The prime contractor and any subcontractors must be certified under the U.S./Canada Joint Certification Program if the work involves access to unclassified military data subject to the provisions of the Technical Data Control Regulations. More information may be found at www.dlis.dla.mil/jcp.

6. **Indicate the type of access required**

   Identify the nature of the work to be performed for this requirement. The user is to select one of the following types:

   a) **Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?**

   The supplier would select this option if they require access to PROTECTED and/or CLASSIFIED information or assets to perform the duties of the requirement.

b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted.

The supplier would select this option if they require regular access to government premises or a secure work site only. The supplier will not have access to PROTECTED and/or CLASSIFIED information or assets under this option.

c) Is this a commercial courier or delivery requirement with no overnight storage?

The supplier would select this option if there is a commercial courier or delivery requirement. The supplier will not be allowed to keep a package overnight. The package must be returned if it cannot be delivered.

7. Type of information / Release restrictions / Level of information

Identify the type(s) of information that the supplier may require access to, list any possible release restrictions, and if applicable, provide the level(s) of the information. The user can make multiple selections based on the nature of the work to be performed.

Departments must process SRCLs through PWGSC where:

- contracts that afford access to PROTECTED and/or CLASSIFIED foreign government information and assets;
- contracts that afford foreign contractors access to PROTECTED and/or CLASSIFIED Canadian government information and assets; or
- contracts that afford foreign or Canadian contractors access to PROTECTED and/or CLASSIFIED information and assets as defined in the documents entitled Identifying INFOSEC and INFOSEC Release.

a) Indicate the type of information that the supplier will be required to access

Canadian government information and/or assets

If Canadian information and/or assets are identified, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by the Canadian government.

NATO information and/or assets

If NATO information and/or assets are identified, this indicates that as part of this requirement, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by NATO governments. NATO information and/or assets are developed and/or owned by NATO countries and are not to be divulged to any country that is not a NATO member nation. Persons dealing with NATO information and/or assets must hold a NATO security clearance and have the required need-to-know.

Requirements involving CLASSIFIED NATO information must be awarded by PWGSC. PWGSC / CIISD is the Designated Security Authority for industrial security matters in Canada.

Foreign government information and/or assets

If foreign information and/or assets are identified, this requirement will allow access to information and/or assets owned by a country other than Canada.

b) Release restrictions

If **Not Releasable** is selected, this indicates that the information and/or assets are for **Canadian Eyes Only (CEO)**. Only Canadian suppliers based in Canada can bid on this type of requirement. NOTE: If Canadian information and/or assets coexists with CEO information and/or assets, the CEO information and/or assets must be stamped **Canadian Eyes Only (CEO)**.

If **No Release Restrictions** is selected, this indicates that access to the information and/or assets are not subject to any restrictions.

If **ALL NATO countries** is selected, bidders for this requirement must be from NATO member countries only.

NOTE: There may be multiple release restrictions associated with a requirement depending on the nature of the work to be performed. In these instances, a security guide should be added to the SRCL clarifying these restrictions. The security guide is normally generated by the organization's project authority and/or security authority.

c) Level of information

Using the following chart, indicate the appropriate level of access to information/assets the supplier must have to perform the duties of the requirement.

Form | Next Page

PROTECTED	CLASSIFIED	NATO
PROTECTED A	CONFIDENTIAL	NATO UNCLASSIFIED
PROTECTED B	SECRET	NATO RESTRICTED
PROTECTED C	TOP SECRET	NATO CONFIDENTIAL
	TOP SECRET (SIGINT)	NATO SECRET
		COSMIC TOP SECRET

8. **Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?**

If Yes, the supplier personnel requiring access to COMSEC information or assets must receive a COMSEC briefing. The briefing will be given to the "holder" of the COMSEC information or assets. In the case of a "personnel assigned" type of contract, the customer department will give the briefing. When the supplier is required to receive and store COMSEC information or assets on the supplier's premises, the supplier's COMSEC Custodian will give the COMSEC briefings to the employees requiring access to COMSEC information or assets. If Yes, the Level of sensitivity must be indicated.

9. **Will the supplier require access to extremely sensitive INFOSEC information or assets?**

If Yes, the supplier must provide the Short Title of the material and the Document Number. Access to extremely sensitive INFOSEC information or assets will require that the supplier undergo a Foreign Ownership Control or influence (FOCI) evaluation by CIISD.

PART B - PERSONNEL (SUPPLIER)

10. a) **Personnel security screening level required**

Identify the screening level required for access to the information/assets or client facility. More than one level may be identified depending on the nature of the work. Please note that Site Access screenings are granted for access to specific sites under prior arrangement with the Treasury Board of Canada Secretariat. A Site Access screening only applies to individuals, and it is not linked to any other screening level that may be granted to individuals or organizations.

RELIABILITY STATUS	CONFIDENTIAL	SECRET
TOP SECRET	TOP SECRET (SIGINT)	NATO CONFIDENTIAL
NATO SECRET	COSMIC TOP SECRET	SITE ACCESS

If multiple levels of screening are identified, a Security Classification Guide must be provided.

b) **May unscreened personnel be used for portions of the work?**

Indicating Yes means that portions of the work are not PROTECTED and/or CLASSIFIED and may be performed outside a secure environment by unscreened personnel. The following question must be answered if unscreened personnel will be used:

Will unscreened personnel be escorted?

If No, unscreened personnel may not be allowed access to sensitive work sites and must not have access to PROTECTED and/or CLASSIFIED information and/or assets.

If Yes, unscreened personnel must be escorted by an individual who is cleared to the required level of security in order to ensure there will be no access to PROTECTED and/or CLASSIFIED information and/or assets at the work site.

PART C - SAFEGUARDS (SUPPLIER)

11. **INFORMATION / ASSETS**

a) **Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information and/or assets on its site or premises?**

If Yes, specify the security level of the documents and/or equipment that the supplier will be required to safeguard at their own site or premises using the summary chart.

b) **Will the supplier be required to safeguard COMSEC information or assets?**

If Yes, specify the security level of COMSEC information or assets that the supplier will be required to safeguard at their own site or premises using the summary chart.

PRODUCTION

c) **Will the production (manufacture, repair and/or modification) of PROTECTED and/or CLASSIFIED material and/or equipment occur at the supplier's site or premises?**

Using the summary chart, specify the security level of material and/or equipment that the supplier manufactured, repaired and/or modified and will be required to safeguard at their own site or premises.

INFORMATION TECHNOLOGY (IT)

d) Will the supplier be required to use its IT systems to electronically process and/or produce or store PROTECTED and/or CLASSIFIED information and/or data?

If Yes, specify the security level in the summary chart. This block details the information and/or data that will be electronically processed or produced and stored on a computer system. The client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document. The supplier must also direct their attention to the following document: Treasury Board of Canada Secretariat - Operational Security Standard: Management of Information Technology Security (MITS).

e) Will there be an electronic link between the supplier' IT systems and the government department or agency?

If Yes, the supplier must have their IT system(s) approved. The Client Department must also provide the Connectivity Criteria detailing the conditions and the level of access for the electronic link (usually not higher than PROTECTED B level).

SUMMARY CHART

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier' site(s) or premises.

For users completing the form **online** (via the Internet), the Summary Chart is automatically populated by your responses to previous questions.

PROTECTED	CLASSIFIED	NATO	COMSEC
PROTECTED A	CONFIDENTIAL	NATO RESTRICTED	PROTECTED A
PROTECTED B	SECRET	NATO CONFIDENTIAL	PROTECTED B
PROTECTED C	TOP SECRET	NATO SECRET	PROTECTED C
	TOP SECRET (SIGINT)	COSMIC TOP SECRET	CONFIDENTIAL
			SECRET
			TOP SECRET

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?

If Yes, classify this form by annotating the top and bottom in the area entitled "ecurity Classification".

b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?

If Yes, classify this form by annotating the top and bottom in the area entitled "ecurity Classification"and indicate with attachments (e.g. SECRET with Attachments).

PART D - AUTHORIZATION

13. Organization Project Authority

This block is to be completed and signed by the appropriate project authority within the client department or organization (e.g. the person responsible for this project or the person who has knowledge of the requirement at the client department or organization). This person may on occasion be contacted to clarify information on the form.

14. Organization Security Authority

This block is to be signed by the Departmental Security Officer (DSO) (or delegate) of the department identified in Block 1, or the security official of the prime contractor.

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?

A Security Guide or Security Classification Guide is used in conjunction with the SRCL to identify additional security requirements which do not appear in the SRCL, and/or to offer clarification to specific areas of the SRCL.

16. Procurement Officer

This block is to be signed by the procurement officer acting as the contract or subcontract manager.

17. Contracting Security Authority

This block is to be signed by the Contract Security Official. Where PWGSC is the Contract Security Authority, Canadian and International Industrial Security Directorate (CIISD) will complete this block.

6.0 INSERT Annex J – SRCL Security Classification Guide under the RFSA as follows:

ANNEX J – SRCL SECURITY CLASSIFICATIONS GUIDE

SRCL - Security Classification Guide

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Details
1.	Any Contractor personnel with physical access to the Contractor data centers	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	Reliability	This is for any Contractor personnel including facilities management resources that have physical access to the Cloud Services hardware equipment at the Contractor data centers.
2.	Any Contractor personnel who have limited logical access to the Contractor services.	• All Business Data • Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components	Both	Reliability	This is for any Contractor personnel that has logical access to the GC data hosted in the Contractor data centers and any sensitive system and security incident data. This can include Level 1 – Service Desk type resources.
3.	Any Contractor personnel with privileged roles and unrestricted logical access to GC assets within the Contractor services	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components • Assets include GC data and credentials	Both	Secret	This is for any Contractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers, any sensitive system and security incident data. This includes authorized access through an established process such as legal requests.

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Details
4.	Any contractor personnel with physical or logical access to detailed design documents.	• Detailed design documents including but not limited to detailed logical and physical application, technology infrastructure solution architectures, security architecture and controls, detailed component diagrams, source code, detailed use-cases and business process maps, detailed application, data flows and data models, database designs, system interfaces, internal controls, test plans and test results	Both	Reliability	This is mainly architecture and detailed design documentation access.
5.	Contractor Security Operations Center Personnel	• Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components	Both	Reliability	This is the Contractor SOC Personnel.

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Details
6.	4th Level OEM Support	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	N/A	The Contractor will use sub-contractors for some of their services as it related to data center operations. Any subcontractor should be properly engaged by the Contractor by having a contract and clear definition of work. This resource type will not have direct physical access to GC Data however they can work on issues/problems specific to their expertise level with security cleared Contractor resources who has access to the data. If the 4th Level OEM Support resource is at Contractor Data Centers, they will be escorted by cleared Contractor Operators. For example: Networking equipment support, HVAC support.

In addition to the roles above, the following covers roles related to transition/migration related services:

Track	Role	Responsibilities	Access to	Location (other than meetings)	Personnel Clearance Requirements (working assumption)
Governance	Delivery Executive, Program Manager or Project Manager	Governance / project management of the engagement	No access to physical systems (hands on keyboards) May attend meetings where protected system configuration data is displayed and/or discussed No access to user data	Onsite - N/A Remote - Yes	Reliability or equivalent
IT Service Management (Operational Guidance)	Architect and Consultant	Leading workshops, creation of documents (service maps, monitoring, etc.)	No access to physical systems (hands on keyboards) May attend meetings where protected system configuration data is displayed and/or discussed No access to user data	Onsite - N/A Remote - Yes	Reliability or equivalent
End User Adoption & Change Management	Architect and Consultant	Leading workshops, creation of documents, other change management activities required to onboard Office 365	No access to physical systems (hands on keyboards) May attend meetings where protected system configuration data is displayed and/or discussed No access to user data	Onsite - N/A Remote - Yes	None (assumes escorted when on Partner premises)
Microsoft Exchange Online Onboarding	Architect	Technical oversight of engagement, general guidance, document and deliverables review	No access to physical systems (hands on keyboards) Potential access to GoC documentation of various classifications No access to user data	Onsite - N/A Remote - Yes	Reliability or equivalent

	Deployment Consultant	**Remediation Phase** - Working side-by-side with SSC/GoC SME's to remediate any issues with on-premises Active Directory, lingering Exchange configuration on-premises, network and client readiness (desktop) **Enable Phase** - Working side-by-side with SSC/GoC SME's to deploy the various components (AAD Connect for synchronization, establishing Federation for authentication, Enabling Conditional Access, Azure Information Protection and Exchange Online configuration in the tenant)	Access to Systems (Office 365 tenant, on-premises Active Directory and Exchange) Access to GoC documentation as required to assist in the remediation and enablement Potential access to user data	Onsite - (if required by SSC) Remote - Yes	Reliability or equivalent (assumes SSC managing the environments independent of Partner email being migrated)
	Migration Consultant	Migration of data from YES to Exchange Online including creating the migration projects. Post-migration support to assist SSC/Partner Service Desks	Access to Systems (Office 365 tenant as Global Admin, on-premises Active Directory and Exchange, YES as either Organization Management or Recipient Management) Access/Potential Access to data (Full mailbox access in both YES and Exchange Online) Access to GoC documentation as required to complete migrations	Onsite - (if required by SSC) Remote - Yes	Secret or equivalent

7.0 INSERT Annex K – PSPC Non-Disclosure Agreement related to Supply Chain Integrity as follows:

ANNEX K – PSPC NON-DISCLOSURE AGREEMENT REALTED TO SUPPLY CHAIN INTERGRITY

PSPC Non-Disclosure Agreement

Note to Suppliers: Please note that this Non-Disclosure Agreement only covers SCI requirements under Section **3.5: Supply Chain Integrity Requirements**. Suppliers will be asked to enter into a bi lateral non-disclosure agreement (NDA) with the CCCS once they onboard on the SaaS ITS Program. For further information on the SaaS ITS Onboarding Program, please refer to Annex L below.

By presenting a Submission, the Supplier agrees to the terms of the non-disclosure agreement below (the "**Non-Disclosure Agreement**"):

1. The Supplier agrees to keep confidential any information it receives from Canada regarding Canada's assessment of the Supplier's Supply Chain Security Information (the "**Sensitive Information**") including, but not limited to, which aspect of the Supply Chain Security Information is subject to concern, and the reasons for Canada's concerns.

2. Sensitive Information includes, but is not limited to, any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form or otherwise and whether or not that information is labeled as classified, proprietary or sensitive.

3. The Supplier agrees that it will not reproduce, copy, divulge, release or disclose, in whole or in part, in whatever way or form any Sensitive Information to any person other than a person employed by the Supplier who has a security clearance commensurate with the level of Sensitive Information being accessed, without the prior written consent of the Supply Chain Security Authority. The Supplier agrees to immediately notify the Supply Chain Security Authority if any person, other than those permitted by this Article, accesses the Sensitive Information at any time.

4. All Sensitive Information will remain the property of Canada and must be returned to the Supply Chain Security Authority or destroyed, at the option of the Supply Chain Security Authority, if requested by the Supply Chain Security Authority, within 30 days following that request.

5. The Supplier agrees that a breach of this Non-Disclosure Agreement may result in disqualification of the Supplier at SA stage, or immediate termination of any resulting Contract(s). The Supplier also acknowledges that a breach of this Non-Disclosure Agreement may result in a review of the Supplier's security clearance and review of the Supplier's status as an eligible Supplier for other requirements.

6. This Non-Disclosure Agreement remains in force indefinitely.

8.0 INSERT Annex L – SaaS ITS Assessment Program: Onboarding Process as follows:

ANNEX L – SAAS IT SECURITY (ITS) ASSESSMENT PROGRAM: ONBOARDING PROCESS

1. Making a Submission to the SaaS IT Security Assessment Program

(a) To make a submission to the program, a Bidder must complete the following steps:

(b) Contact the CCCS Contact Centre: contact@cyber.gc.ca or 613-949-7048 or 1-833-CYBER-88.

(c) Prepare to enter into a bi lateral non-disclosure agreement (NDA) with the CCCS.

(d) Provide all documentation for the assessment to the CCCS Contact Centre. When providing documents, Pretty Good Privacy (PGP) encryption program credentials should be used to encrypt the documents. See section 2 – PGP Key for a copy of the PGP key.

2. PGP Key

(a) Email or phone the CCCS Contact Centre to request the necessary public key for the CCCS PGP key. Use this key to encrypt sensitive documents that you are submitting for the SaaS ITS Assessment Program.

3. Contacts and Assistance

(a) The CCCS Contact Centre is the point of contact for all document submissions related to the SaaS ITS Assessment Program. The SaaS Assessment team lead, or an authorized delegate, has access to this mailbox. All SaaS ITS Assessment documentation will be managed and protected using PGP encryption during transmission (see section 2 for a copy of the PGP key). All documentation will also be handled and managed following CCCS information management policies.

CCCS Contact Centre
contact@cyber.gc.ca
613-949-7048 or 1-833-CYBER-88

9.0 INSERT Appendix F – SRCL for SaaS, under the Annex F – SaaS Resulting Contract Clauses as follows:

APPENDIX F – SRCL FOR SAAS

(Insert if applicable)

Note to Contractors: Different or additional security levels may apply to Clients using the SA or their Work requirements, for example, security clearances for Suppliers or Supplier resources. In the event that a Contract issued against a Supply Arrangement includes different or additional security levels, they will be included in Appendix I (SRCL) and Appendix J (SRCL Security Classification Guide) to the Contract.

10.0 INSERT Appendix G – SRCL Security Classification Guide under the Annex F – SaaS Resulting Contract Clauses as follows:

APPENDIX G – SRCL SECURITY CLASSIFICATION GUIDE

(Insert if applicable)

Note to Contractors: Different or additional security levels may apply to Clients using the SA or their Work requirements, for example, security clearances for Suppliers or Supplier resources. In the event that a Contract issued against a Supply Arrangement includes different or additional security levels, they will be included in Appendix I (SRCL) and Appendix J (SRCL Security Classification Guide) to the Contract.

11.0 DELETE and INSERT Form 5 - Submission Completeness Review Checklist as follows:

If you wish to receive any editable documents and/or forms please send your request at: TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca.

Form 5 - Submission Completeness Review Checklist

SUPPLIER'S NAME:

1) Technical Submission, Financial Submission and Certifications, and Supply Chain Integrity Information:

- a) ☐ Technical Submission
- b) ☐ Financial Submission
- c) ☐ Certifications and additional information
- d) ☐ Supply Chain Integrity Requirements

FORMS:

1. **Submission Submission Form** (RFSA Form 1)

- a) ☐ Supplier's full legal name
- b) ☐ Authorized Representative of Supplier for the evaluation purposes
- c) ☐ Supplier's Procurement Business Number (PBN)
- d) ☐ List of the Board of Directors Member
- e) ☐ Jurisdiction of Contract
- f) ☐ Number of FTEs
- g) ☐ Security Clearance Level of Supplier
- h) ☐ Aboriginal Businesses
- i) ☐ Canadian Small and Medium Enterprises (CSME)
- j) ☐ Canadian Enterprise
- k) ☐ Green Procurement
- l) ☐ Green Company
- m) ☐ Supplier Certification that all SaaS Solutions are "Off-the-Shelf"
- n) ☐ Signature of Authorized Representative of Supplier

2. **SaaS Publisher Certification Form** *(Mandatory when the Supplier itself is the SaaS Publisher) (RFSA Form 2)* ☐

3. **SaaS Publisher Authorization Form** *(Mandatory when the Supplier is not the SaaS Publisher) (RFSA Form 3)* ☐

4. **Certification Requirements for the Set-Aside Program for Aboriginal Business** *(Mandatory when the Supplier is an aboriginal business and wants to be identified as such) (RFSA Form 5)* ☐

5. **SCI Submission Template (RFSA Form 6)** ☐

ANNEXES:

Annex A – Qualification Requirements ☐

Annex C – SaaS Solutions and Ceiling Prices ☐

- a) ☐ Must be submitted using the format outlined in Annex C or submitted via a web-site link.
- b) ☐ **Item No**. included for each product.
- c) ☐ **SaaS Publisher's Part No.** *(the part number the SaaS Publisher uses to identify the SaaS Solution commercially)*

d) ☐ **SaaS Solution Name** *(the commercial product name that the SaaS Publisher uses to identify the SaaS Solution.*

e) ☐ **SaaS Publisher's Name** *(the name of the SaaS Publisher that produces the SaaS Solution)*

f) ☐ **Cloud Service Provider's name (CSP):** Supplier must identify the existing Cloud Service Provider (CSP), who's Commercially Available Cloud Services will be used to supply to Canada the proposed Software as a Service (SaaS).

g) ☐ **Ceiling Unit Price Ceiling Prices for SaaS Solutions** *(required for every line item)*

h) ☐ **Unit of Measure** *(the unit of measure under which the SaaS Solution will be offered to Canada; such as "per user", "per entity " and whether the is per subscription term is monthly or annual, etc.)*

i) ☐ **Applicable percentage discount** *(enter the percentage discount that will be applied to the Ceiling Commercial Unit Prices for the duration for the SA)*

j) ☐ **Language(s) available** *(the language(s) under which the SaaS Solution is available such as English, French and/or other)*

k) ☐ **SaaS Solution Information** *(a web site URL containing SaaS Solution information)*

l) ☐ **Keywords/tags** (keywords associated with the SaaS Solution that will help the Clients to easily search and find SaaS *Solutions that meet their needs)*

Annex D – SaaS Solution Service Level Agreement(s)

Service Level Agreement (SLA):

a) ☐	Availability - Performance;	PAGE # _____
b) ☐	Downtime definition - scheduled and unscheduled;	PAGE # _____
c) ☐	Service credits – triggers and calculation;	PAGE # _____
d) ☐	Support services availability;	PAGE # _____
e) ☐	Self-service, knowledge base, online tutorials;	PAGE # _____
f) ☐	Errors: severity level definitions;	PAGE # _____
g) ☐	Mean Time-to-respond and repair;	PAGE # _____
h) ☐	Escalation Path and Procedure; and	PAGE # _____
i) ☐	Available Disaster recovery system;	PAGE # _____

Name of Authorized Signatory of Supplier: _____

Signature of Authorized Signatory of Supplier: _____

12.0 DELETE and INSERT Form 6 - SCI Submission Template as follows:

If you wish to receive any editable documents and/or forms please send your request at: TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca.

Government of Canada / Gouvernement du Canada

PROTECTED B
When Filled

A - 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 +

B -Product List

Example 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										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										

C - Ownership Information

F - Example Ownership Information

Use this form only for OEM and Suppliers that do not have a DUNS number.

Item	OEM or Supplier name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						

D - Help

Field	Guide	Notes
SCSI Form 2 Cover		
PROCUREMENT NAME	If not applicable, leave blank. Otherwise, provide any name associated with this multi-line procurement (i.e. WTD Print, Project Telesto).	
Date submitted:	YYYY-MM-DD	
SOLICITATION #:	If not applicable, leave blank. Otherwise, provide the solicitation number for this multi-line procurement.	
BIDDER NAME	If not applicable, leave blank. Enter the name of the lead organization providing the bid submission.	
BIDDER DUNS Number	If not applicable, leave blank. Enter the DUNS number of the lead organization providing the bid submission. 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.	
IT PRODUCT LIST		
OEM Name	Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered.	**Only products that qualify for supply chain integrity assessments should be included in this list. Power cables, rack blanking panels, warranty**

OEM DUNS Number	Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) 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.	**costs, shipping costs, and similar other non-ICT items should not be included. If these products are found in this form, it will be sent back as incorrect and no assessment will be performed.** **This should follow the "Product" definition of "hardware (or software) that operates at the data link layer of the Open Systems Interconnection model (OSI Model) Layer 2 and above"**
Product Name	Enter the OEM's name for the product.	
Model Number	Enter the OEM's model and/or version number of the product.	
Product URL	Enter the URL of the OEM's webpage for the product.	
Vulnerability Information	Enter 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).	
Supplier Name	Enter 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. **For PISA, NMSO, or similar lists, this field may be left blank.**	

Supplier DUNS Number	Enter the DUNS number of the Supplier. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a businesses. 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. **For PISA, NMSO, or similar lists, this field may be left blank.**	
Supplier URL	Enter the URL of the supplier's webpage for the product. **For PISA, NMSO, or similar lists, this field may be left blank.**	
OWNERSHIP INFORMATION		
OEM or Supplier name	Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered, or enter the name of the supplier (i.e. sub-contractors, re-seller, distributor, sub-processors, etc.) of the product or service that is being ordered.	**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.** **Each piece of provided information must be found on its own line in its own cell in the spreadsheet.**
Ownership	Ownership information consists of 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.	
Investors	Investor information consists of 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.	
Executives	List the executives and members of the board of directors for the company in question.	
Country / Nationality	The country which an individual listed has their primary nationality or the country in which a corporate entity is registered.	
Corporate website link	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.	

E - Example 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	Cie. ABC	137660665	1941	K9	Insert URL here	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW				PISA Example
2	Cie. ABC	137660665	1941	K9	Insert URL here	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW	LocalHardware	4567891234	https://www.lhinc.ca	ROC / Single Procurement Example

F - Example Ownership Information

OEM or Supplier name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
newkid software	Mr. A (60%)			Canada	newkid.com/profiles/mra
newkid software	Ms. B (30 %)			France	newkid.com/profiles/msb
newkid software	Mr. C (10%)			United States	newkid.com/profiles/mrc
newkid software		Company A (10%)		United States	newkid.com/investor_relations/filings
newkid software		Company B (9%)		China	newkid.com/investor_relations/filings
newkid software		Company C (8%)		South Korea	newkid.com/investor_relations/filings
newkid software		Company D (5%)		Canada	newkid.com/investor_relations/filings
newkid software		Company E (5%)		Spain	newkid.com/investor_relations/filings
newkid software			Mr. A	Canada	newkid.com/profiles/mra
newkid software			Ms. B	France	newkid.com/profiles/msb
newkid software			Mr. Q	Portugal	newkid.com/profiles/mrq

ALL OTHER TERMS AND CONDITIONS OF THE REQUEST FOR SUPPLY ARRANGEMENT REMAIN UNCHANGED.