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

Request For Supply Arrangement - Demande pour un arrangement en matière d'approvisionnement

Offer to: Department of Public Works and Government Services

We hereby offer to provide to Canada, as represented by the Minister of Public Works and Government Services, in accordance with the terms and conditions set out herein or attached hereto, the goods, services, and construction detailed herein and on any attached sheets.

Offre au: Ministère des Travaux publics et des Services gouvernementaux

Nous offrons par la présente de fournir au Canada, représenté par le ministre des Travaux publics et des Services gouvernementaux, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici et sur toute feuille ci-annexée.

Comments - Commentaires

Title - Sujet
RFSA - SaaS Method of Supply (GC)

Solicitation No. - N° de l'invitation	**Date**
EN578-191593/F	2019-05-10
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
20191593	PW-$EEM-003-35660
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
003eem.EN578-191593	

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

Delivery Required - Livraison exigée
See Herein

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Boyer, Tania	003eem
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613)858-9232 ( )	( ) -

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 request for a Supply Arrangement does not include provisions for security.
Cette Demande pour un arrangement ne comprend pas des dispositions en matière de sécurité.

Instructions: See Herein

Instructions: Voir aux présentes

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

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

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

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

Signature **Date**

Issuing Office - Bureau de distribution
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

Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire FOB/FAM Destination	Plant/Usine	Delivery Req. Livraison Req.	Del. Offered Liv. offerte
2	NPP Amendment 01	EN578	EN578	1	LOT	$	$	See Herein	
3	NPP Amendment	EN578	EN578	1	LOT	$	$	See Herein	
4	RFI and Draft RFSA	EN578	EN578	1	LOT	$	$	See Herein	
6	NPP D	EN578	EN578	1	LOT	$	$	See Herein	

REQUEST FOR SUPPLY ARRANGEMENT (RFSA)

FOR

SOFTWARE AS A SERVICE (SaaS)

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Preamble

Public Services and Procurement Canada (PSPC), on behalf of the Government of Canada (GC), is issuing this Request for Supply Arrangement (RFSA) to establish a new method of supply to satisfy various Software as a Service (SaaS) requirements. This new method of supply is a key procurement enabler for the GC's Cloud First direction and is part of an envisioned GC Cloud Services Procurement Vehicle framework that will consist of various methods of supply to satisfy both classified and unclassified cloud requirements.

The objectives of this SaaS RFSA are to:

- simplify the procurement process to acquire SaaS Solutions and support GC procurement modernization and contract simplification initiatives;
- increase competition and access to the latest SaaS Solutions on the market for the GC; and
- increase transparency, openness and fairness in public sector procurement processes.

As highlighted in the GC *Digital Operations Strategic Plan: 2018-2022* published by the Treasury Board of Canada Secretariat, procurement enablers such as this SaaS RFSA will help position the GC and public sector partners to leverage the latest digital technologies to achieve better results for Canadians.

1.1.1 Background

The GC Cloud Services Procurement Vehicle framework represents an innovative approach to procure cloud by leveraging various methods of supply to satisfy cloud requirements for the GC and public sector entities, which may include but are not limited to provincial, territorial, and municipal governments.

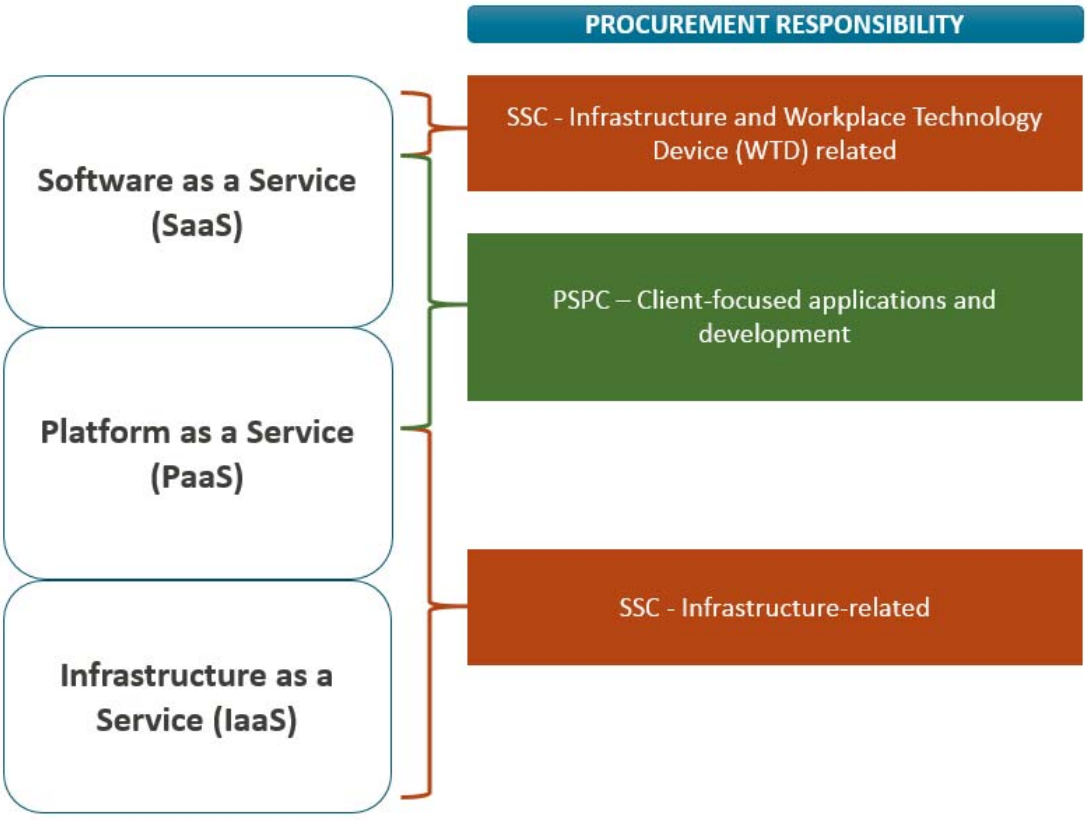
On September 7, 2018, Shared Services Canada (SSC) published an Invitation to Qualify (ITQ) as the first phase of the procurement process for the GC Cloud Services Procurement Vehicle (https://buyandsell.gc.ca/procurement-data/tender-notice/PW-18-00841719). In parallel, PSPC issued a Request for Information (RFI) on October 29, 2018 to seek feedback from the industry on proposed approach and requirements to procure SaaS Solutions. PSPC received 47 responses to the RFI, and conducted one-on-one sessions with interested suppliers to refine the approach and requirements of this RFSA, and better align with industry best practices on cloud procurement.

1.1.2 Organizing the GC to Effectively Deliver Cloud Procurements

Within the GC, PSPC and SSC jointly support federal organizations in procuring IT goods and services. With respect to procuring cloud-based offerings, the procurement responsibilities of each organization extends to the various elements of cloud stack from the infrastructure to the software application layers. The division of procurement responsibilities reflects the procurement mandate of each respective organization in supporting GC clients.

In line with each organization's mandate, SSC's procurement role in cloud-based offerings mirrors their responsibilities in managing the GC infrastructure, networks, common workplace technology devices and cyber security. PSPC's procurement role is primarily in software application and development space, supporting clients in their service delivery and back-office functions.

The diagram below represents the division of responsibilities only and is not specific to a requirement:



This RFSA will qualify Suppliers for issuance of Supply Arrangements with GC SaaS Catalogue and will facilitate simplified solicitation and contracting processes for individual client requirements.

PSPC and SSC are working closely to ensure the alignment of best practices on cloud procurement, including the development of a cloud commodity group to address limitation of liability as well as common security requirements. These elements lay the foundation of cloud procurement activities in the GC.

1.1.3 Structure of the RFSA

This RFSA is divided into seven parts plus attachments and annexes, as follows:

Part 1 **General Information**: provides a general description of the requirement;

Part 2 **Supplier Instructions**: provides the instructions applicable to the clauses and conditions of the RFSA;

Part 3 **Submission Preparation Instructions**: provides Suppliers with instructions on how to prepare their submission in response to this RFSA ("Submission") to address the evaluation criteria specified;

Part 4 **Evaluation Procedures and Basis of Selection**: indicates how the evaluation will be conducted, the evaluation criteria which must be addressed in the Submission and the basis of selection;

Part 5 **Certifications and Additional Information**: includes the certifications and additional information to be provided;

Part 6 **Supply Arrangement**: includes the Supply Arrangement (SA) with the applicable clauses and conditions; and

Part 7 **Bid Solicitation and Resulting Contract Clauses**: includes the instructions for the bid solicitation process within the scope of the SA and general information for the conditions which will apply to any contract entered into pursuant to the SA.

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.

Note: Capitalized words and technical terms used in this RFSA are defined in the Resulting Contract Clauses – **Appendix B - DEFINITIONS AND INTERPRETATION.**

1.2 Summary

(a) PSPC on behalf of Canada, is implementing this procurement vehicle for the delivery of various SaaS Solutions, including associated maintenance and support, training, and professional services, as required by Canada, in support of its various programs, operational needs and projects. The RFSA is also being used to establish Supply Arrangements with Aboriginal firms as defined under the Procurement Strategy for Aboriginal Business (PSAB) to allow for the possibility of Clients setting aside their requirements.

(b) Any requirement for delivery to a destination in a land claims area will be actioned as a separate requisition outside of the Supply Arrangements.

(c) Any resulting Supply Arrangements may be used by any Government Department, Departmental Corporation or Agency, or other Crown entity described in the Financial Administration Act (as amended from time to time), and any other party for which the Department of Public Works and Government Services may be authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act (each a “Client”).

(d) A Notice and the RFSA will be posted continuously on the Government Electronic Tendering Service (GETS) to allow Suppliers to become qualified at any given time.

(e) As cloud-based offerings increase in the marketplace, Canada recognizes the need to move in an agile manner to facilitate access to SaaS Solutions while balancing the complexities associated with adopting new IT delivery methods. Qualification for Supply Arrangements will be open to Suppliers with SaaS Solutions that reside on IaaS and PaaS meeting the GC Security Control Profile for Cloud-based GC Services (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) and associated IT security requirements as set forth in this RFSA.

(f) Canada will not award a Supplier an SA or delay award of contract(s) to other Suppliers if a Supplier has not submitted completed documentation in its response or has submitted documentation that deviates from the terms of the RFSA.

(g) Contracts resulting from the SaaS Supply Arrangements may be subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North

American Free Trade Agreement (NAFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), and the Canadian Free Trade Agreement (CFTA).

(h) This RFSA allows Suppliers to use the epost Connect service provided by Canada Post Corporation to transmit their Submission electronically. Suppliers must refer to Part 2 of this RFSA entitled Supplier Instructions for further information on using this method.

(i) The order of evaluation of Submissions will be at Canada's sole discretion.

(j) This RFSA is not a solicitation of bids or tenders. No contract will be awarded automatically as a result of the qualification under this RFSA.

1.3 Overview of the Submission Review Process

To best meet the needs of the GC and manage the volume of Submissions in response to this RFSA, the process to review Submissions and to qualify Suppliers will be prioritized as follows:

a) **Phase 1** will be used to evaluate Submissions from Suppliers with SaaS Solutions and Services that comply with Canada's requirements for storing and processing Protected B information as detailed in Annex A, Qualification Requirements, Tier 2.

b) **Phase 2** will be used to evaluate Submissions from Suppliers with SaaS Solutions and Services that comply with Canada's requirements for storing and processing information up to Protected A, as detailed in Annex A, Qualification Requirements, Tier 1.

c) **Phase 3** will be used to evaluate Submissions from Value-Added Resellers of SaaS Solutions and Services.

Canada intends to begin reviewing Submissions received under Phase 1 on June 17, 2019 and will prioritize review of the Submissions from Suppliers with SaaS Solutions and Services that are hosted by a "qualified" Cloud Service Provider. A "qualified" Cloud Service Provider has completed the CCCS Assessment Program (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100) and has met all of the requirements of Shared Services Canada's Invitation to Qualify for Government of Canada Cloud Service Procurement Vehicle (GC Cloud) (https://buyandsell.gc.ca/procurement-data/tender-notice/PW-18-00841719). Submissions from Suppliers with SaaS Solutions and Services that are not hosted by a "qualified" Cloud Service Provider, as well as Submissions classified under Phase 2 and 3, will be evaluated subsequently. Value-Added Resellers will only be considered under Phase 3.

Canada reserves the right to modify the submission review process and the prioritization sequence within and between the above Phases at any time in order to meet its business needs.

1.4 Security Requirements

There are security requirements associated with this RFSA, in particular as described in Annex A - Qualification Requirements, Annex B - Security & Privacy Obligations, and Annex F - Resulting Contract Clauses, including its Appendices. The SaaS Services and Work to be procured under this RFSA may also be subject to additional security requirements, depending on the clients' individual needs which will be captured in the bid solicitation and/or contract.

1.5 Debriefings

Suppliers may request a debriefing on the results of the RFSA process. Suppliers should make the request to the Supply Arrangement Authority within 15 working days of receipt of the results of the request for supply arrangements process. The debriefing may be in writing, by telephone or in person.

1.6 Key Terms

The definitions of key terms for the entirety of this RFSA, including attached Annexes and Appendices, are detailed in Appendix B of Annex F - Resulting Contract Clauses.

PART 2 - SUPPLIER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the Request for Supply Arrangements (RFSA) by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Services and Procurement Canada (PSPC).

Suppliers who present a Submission in response to this RFSA agree to be bound by the instructions, clauses and conditions of the RFSA and accept the clauses and conditions of the Supply Arrangement and resulting contract(s).

The 2008 (2018-05-22) Standard Instructions - Request for Supply Arrangements - Goods or Services, are incorporated by reference into and form part of the RFSA.

The 2008 standard instructions is amended as follows:

- Section 08, entitled Submission of arrangements, is amended as follows:
    - subsection 2. is deleted entirely and replaced with the following:

2. epost Connect

    a. Unless specified otherwise in the RFSA, the Submissions may be submitted by using the epost Connect service provided by Canada Post Corporation.

    The only acceptable email address to use with epost Connect for responses to RFSAs issued by PSPC headquarters is:

    tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

    b. To submit a Submission using epost Connect service, the Supplier must either:

        i. send directly its Submission only to specified PSPC Bid Receiving Unit using its own licensing agreement for epost Connect provided by Canada Post Corporation; or

        ii. send as early as possible, and in any case, at least six business days prior to the RFSA closing date and time, (in order to ensure a response), an email that includes the RFSA number to the specified PSPC Bid Receiving Unit requesting to open an epost Connect conversation. Requests to open an epost Connect conversation received after that time may not be answered.

    c. If the Supplier sends an email requesting epost Connect service to the specified Bid Receiving Unit in the RFSA, an officer of the Bid Receiving Unit will then initiate an epost Connect conversation. The epost Connect conversation will create an email notification from Canada Post Corporation prompting the Supplier to access and action the message within the conversation. The Supplier will then be able to transmit its Submission afterward at any time prior to the RFSA closing date and time.

    d. If the Supplier is using its own licensing agreement to send its Submission, the Supplier must keep the epost Connect conversation open until at least 30 business days after the RFSA closing date and time

    e. The RFSA number should be identified in the epost Connect message field of all electronic transfers.

f. It should be noted that the use of epost Connect service requires a Canadian mailing address. Should a supplier not have a Canadian mailing address, they may use the Bid Receiving Unit address specified in the RFSA in order to register for the epost Connect service.

g. For Submissions s transmitted by epost Connect service, Canada will not be responsible for any failure attributable to the transmission or receipt of the Submission including, but not limited to, the following:

i. receipt of garbled, corrupted or incomplete arrangement;
ii. availability or condition of the epost Connect service;
iii. incompatibility between the sending and receiving equipment;
iv. delay in transmission or receipt of the arrangement;
v. failure of the Supplier to properly identify the arrangement;
vi. illegibility of the Submission;
vii. security of Submission data; or
viii. inability to create an electronic conversation through the epost Connect service.

h. The Bid Receiving Unit will send an acknowledgement of the receipt of Submission document(s) via the epost Connect conversation, regardless of whether the conversation was initiated by the supplier using its own license or the Bid Receiving Unit. This acknowledgement will confirm only the receipt of Submission document(s) and will not confirm if the attachments may be opened nor if the content is readable.

i. Suppliers must ensure that that they are using the correct email address for the Bid Receiving Unit when initiating a conversation in epost Connect or communicating with the Bid Receiving Unit and should not rely on the accuracy of copying and pasting the email address into the epost Connect system.

j. A Submission transmitted by epost Connect service constitutes the formal Submission of the Supplier and must be submitted in accordance with section 05.

Subsection 5.4 of 2008, Standard Instructions - Request for Supply Arrangements - Goods or Services, is amended as follows:

Delete: 60 days
Insert: 180 days

2.2 Presentation of Submissions

(a) If Suppliers chooses to present their Submissions electronically using epost Connect service, Canada requests that Suppliers submit in accordance with section 08 of the 2008 Standard Instructions. Suppliers are required to provide their Submission in a single transmission. The epost Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation. The approved formats for documents are any combination of:

A. PDF documents; and
B. Documents that can be opened with either Microsoft Word or Microsoft Excel.

(b) If Suppliers choose to present their Submission by email, Canada requests that Suppliers submit in accordance with the following:

(i) **Email submission**: Submissions must be submitted by email to:

TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

(ii) **Format of Email Attachments**: The approved formats for email attachments are any combination of:

A. PDF documents; and
B. Documents that can be opened with either Microsoft Word or Microsoft Excel.

(iii) **Email Size:** Suppliers should ensure that they submit their response in multiple emails if any single email, including attachments, exceeds 5 MB.

(iv) **Email Title: Suppliers are requested to include the RFSA No. in the "subject" line of each email forming part of the response.**

(c) Due to the nature of the RFSA, transmission of responses by mail or by facsimile to PSPC will not be accepted.

2.3 Federal Contractors Program for Employment Equity - Notification

The Federal Contractors Program (FCP) for employment equity requires that some contractors make a formal commitment to Employment and Social Development Canada (ESDC) - Labour to implement employment equity. In the event that this Supply Arrangement would lead to a contract subject to the Federal Contractors Program (FCP) for employment equity, the bid solicitation and resulting contract templates would include such specific requirements. Further information on the Federal Contractors Program (FCP) for employment equity can be found on Employment and Social Development Canada (ESDC) - Labour's website.

2.4 Enquiries - Request for Supply Arrangements

(a) All enquiries must be submitted in writing to the Supply Arrangement Authority.

(b) Suppliers should reference as accurately as possible the numbered item of the RFSA to which the enquiry relates. Care should be taken by Suppliers to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that Suppliers do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all Suppliers. Enquiries not submitted in a form that can be distributed to all Suppliers may not be answered by Canada.

2.5 Applicable Laws

(a) The SA and any contract awarded under the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario, Canada.

(b) Suppliers may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of the arrangement, by deleting the name of the Canadian province or territory specified in Article 6.10 and inserting the name of the Canadian province or territory of their choice on Form 1. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Suppliers.

2.6 Suppliers

(a) **SaaS Publishers:** SaaS Publishers are eligible to participate in Phase 1 and 2 of this RFSA. SaaS Publishers must submit Form 2 to certify their SaaS ownership rights. CSPs who are also SaaS

Publishers must submit Form 2 for their own SaaS and Form 3 for third-party hosted SaaS, as applicable.

(b) **Value-Added Resellers**: Value-Added Resellers are eligible to participate in Phase 3 of this RFSA. VARs must submit Form 3 to demonstrate their authority to supply the SaaS to Canada.

PART 3 - SUBMISSION PREPARATION INSTRUCTIONS

3.1 Submission Preparation Instructions

The Submission must be gathered per section and separated as follows:

Section I: Technical Submission
Section II: Financial Submission
Section III: Certifications and additional information
Section IV: Supply Chain Integrity Information

3.2 Section I: Technical Submission

(a) In the Technical Submission, Suppliers should explain and demonstrate how they propose to meet the requirements contained in the RFSA and provide all documents and information that is requested. The Technical Submission should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the Submission will be evaluated.

(b) Canada requests that the Suppliers address and present topics and information in the format outlined in the applicable annex and/or form of the RFSA.

(c) The Technical Submission consists of:

(i) **Request for Supply Arrangement Submission Form**: Form 1 – Request for Supply Arrangement Submission Form must accompany the Submission. It provides a common form in which Suppliers can provide information required, such as the Supplier's contact information, Procurement Business Number (PBN), status under the Federal Contractors Program for Employment Equity, etc. If Canada determines that the information requested in the Request for Supply Arrangement Submission Form is incomplete or requires correction, Canada will provide the Supplier with an opportunity to submit the required corrections.

(ii) **SaaS Publisher as Supplier Form**: Form 2 (if applicable) – If the SaaS Publisher (defined as the entity or person who is the owner of the copyright in any SaaS Solution included in the Submission and who has the right to the license and to authorize others to use its SaaS Solution and any underlying components) intends to submit a Submission and qualify itself as a Supplier, such SaaS Publishers must submit the certification Form 2.

(iii) **Value-Added Reseller and Cloud Services Providers as Suppliers Form:** Form 3 (if applicable) – If an entity other than the SaaS Publisher who is authorized to distribute and re-sell the SaaS Solutions(s) intends to submit a Submission and qualify itself as a Supplier, such entity must submit certification from the SaaS Publisher, in accordance with Form 3, to certify that such entity has been authorized to supply the SaaS Solution Publisher's SaaS Solution(s).

(iv) **Substantiation of Compliance with Qualification Requirements**: Suppliers must substantiate compliance with the qualification requirements contained in Annex A – Qualification Requirements. The substantiation must not simply be a repetition of the requirements, but must explain and demonstrate how the Supplier meets the requirements. Simply stating that the Supplier or its proposed SaaS Solutions comply is not sufficient. Where Canada determines that the substantiation is not complete, Canada will provide the Supplier with an opportunity to submit the required substantiation.

(v) **Service Level Agreements:** Suppliers must submit their published Service Level Agreements (SLAs), to be included in Annex D – SaaS Solution Service Level Agreements (SLA).

The service level commitments (detailed in the published service level agreements) must provide commercial clients support which includes, at the minimum, any published and commercially available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the SaaS Solution.

SLAs may consist of a single document which applies to all SaaS Solutions, or may consist of multiple SaaS Solution-specific documents. Should a Supplier submit multiple SaaS Solution-specific SLA documents, the Supplier must clearly outline which SaaS Solution listed in Annex C - SaaS Solutions and Ceiling Prices, the SLAs apply to. If SLA terms are already specified in the SaaS Usage Terms and Conditions, duplicate terms need not be provided.

The following are examples of terms that may be addressed in the Supplier's SLA:

A. period during which the Supplier will support the Client;
B. contact and procedure information for accessing support;
C. procedures for resolution of problems;
D. response times;
E. procedures on how and when all telephone, fax or email communications will be responded to;
F. website support availability to Clients (e.g. 24 hours a day, 365 days a year, and 99.9% of the time); and,
G. maintenance entitlements (e.g. patches, updates, major/minor releases, etc.)

By presenting a Submission, the Supplier acknowledges and agrees that any terms contained in Annex D - SaaS Solution Service Level Agreements that purport to interpret the RFSA, are the same or similar subject matter, or are related to the terms contained in the RFSA and Resulting Contract Clauses, are deemed stricken and are of no force or effect.

(vi) **Form 5 - Submission Completeness Review Checklist** must accompany the Submission. It provides a common form in which Suppliers can verify that their Submission includes all of the required information to be deemed complete prior to submitting. If Canada determines that the checklist and/or Submission is incomplete or requires correction, Canada will provide the Supplier with an opportunity to submit the required corrections.

(vii) **Compliance with Annex B – Security & Privacy Obligations**: Suppliers must comply with security and privacy 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.

(d) By presenting a Submission, the Supplier acknowledges and agrees that all other terms submitted as part of the Technical Submission are deemed stricken and form no part of the SA.

3.3 Section II: Financial Submission

(a) In the Financial Submission, Suppliers must submit a list of proposed SaaS Solutions with their commercial pricing and applicable percentage discount, and any prices or rates applicable for professional services to be provided by the Supplier. It is required that the list of SaaS Solutions and Commercial Prices section of the Submission be presented as per the template provided in **Annex C – SaaS Solutions and Ceiling Prices** of the RFSA. All Annex C – SaaS Solutions and Ceiling Prices documents from all SAs issued under this RFSA will be used to create a GC SaaS Catalogue. The Financial Submission should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the Submission will be evaluated.

(b) The following must be addressed in the Supplier's **Annex C – SaaS Solutions and Ceiling Prices**:

(i) **SaaS Publisher's Part No.:** Suppliers should provide the part number that the SaaS Publisher uses to identify the SaaS Solution commercially;

(ii) **SaaS Solution's Name:** Suppliers must provide the commercial name that the SaaS Publisher uses to identify the SaaS Solution commercially.

(iii) **SaaS Publisher's Name:** Suppliers must provide the name of the SaaS Publisher that owns the Intellectual Property rights to the SaaS Solution;

(iv) **Cloud Service Provider (CSP)'s name:** Suppliers must identify the existing Cloud Service Provider (CSP) that hosts the proposed SaaS Solution.

(v) **Ceiling Prices:** Suppliers must submit ceiling prices for all SaaS Solutions and any applicable professional services proposed in Annex C – SaaS Solution and Ceiling Prices. The prices must be:

A. the Supplier's commercial pricing less the applicable percentage discount,

B. in Canadian dollars; and,

C. exclusive of Goods and Services Tax or Harmonized Sales tax.

(vi) **Unit of Measure:** Suppliers must enter the unit of measure for their SaaS Solution Ceiling Prices (such as "per user", "per entity", etc.) under which the SaaS Solutions will be provided to Canada;

(vii) **Applicable Percentage Discount** : Suppliers must enter the percentage discount that will be applied to the Ceiling Commercial Unit Prices for the duration of the SA

(viii) **Language(s) available:** Suppliers must indicate the language(s) under which the SaaS Solution is available, designated as "EN" for English, "FR" for French, or "EN, FR" for both;

(ix) **SaaS Solution Information:** Suppliers may provide a web site URL containing information on the SaaS Solution.

(x) **Keywords**: Suppliers should provide keywords associated with their SaaS Solution(s) that will help the Clients to easily search and find SaaS Solutions in the GC SaaS Catalogue that meet their needs.

(c) **Price reference**: Suppliers must provide a price reference(s) to substantiate that their proposed prices are fair and reasonable. Examples of acceptable price references include, but are not limited to, the following:

(i) a current published price list indicating the percentage discount available to Canada; or

(ii) copies of paid invoices for the like quality and quantity of the goods, services or both sold to other customers; or

(iii) any other supporting documentation as requested by Canada.

3.4 Section III: Certifications and additional information

Suppliers must submit the certifications and additional information required under Part 5.

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**. 4.3

(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.**

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Submissions will be assessed in accordance with the entire requirement of the RFSA including but not limited to the technical and financial evaluation criteria, certifications, and security requirements.

(b) An evaluation team composed of representatives of Canada will evaluate the Submissions.

(c) **Requests for Clarifications**: If Canada seeks clarification or verification from a Supplier about its Submission, the Supplier will have 2 working days (or a longer period if specified in writing by the Supply Arrangement Authority) to provide the necessary information to Canada. Failure to meet any deadline will render the Submission non-responsive, on "hold", or will create delay in processing a Supplier's SA

(c) **Right of Canada:**

a. Canada reserves the right to reject any of the SaaS Solutions proposed by a Supplier and enter into negotiation related to any ceiling prices under Annex C– SaaS Solutions and Ceiling Prices;

(i) Canada reserves the right to reject or negotiate any of the terms and conditions proposed by a Supplier and submitted under Annex D – SaaS Solution Service Level Agreements (SLA). No SA will be awarded unless and until Canada has approved all such terms and conditions;

4.2 Technical and Financial Evaluation

(a) Submissions will be reviewed to determine whether they meet the mandatory requirements of the RFSA. All elements of the RFSA that are mandatory requirements are identified specifically with the words "must" or "mandatory". Suppliers with Submissions that do not comply with each and every mandatory requirement will be notified by the Supply Arrangement Authority and will be provided with a time frame within which to meet the requirement. Failure to comply with the request of Canada and meet the requirements within that time period will render the Submission non-responsive, disqualified**,** on "hold", or will create delay in processing a Supplier's SA.

4.2.1 Mandatory Technical Criteria

The mandatory technical requirements are as follows:

(i) Request for Supply Arrangement Submission Form as per Article 3.2 (c)(i);

(ii) Substantiation of compliance with Qualification Requirements as per Article 3.2(c)(iv);

(iii) Service Level Agreement(s) as per Article 3.2 (c) (v);

(iv) Certifications as per Article 3.4; and,

(v) Financial Viability as per Article 4.5.

4.2.2 Mandatory Financial Evaluation

The mandatory financial requirements are as follows:

(i) SaaS Solutions and Ceiling Prices as per Article 3.3 (a) and (b); and

(ii) Price reference(s) as per Article 3.3 (c).

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 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**.

4.4 Basis of Selection

A Submission must comply with the requirements of the Request for Supply Arrangements, meet all mandatory technical and financial evaluation criteria, and provide all of the mandatory certifications in order to be declared responsive.

4.5 Financial Viability

SACC Manual clause S0030T (2014-11-27) Financial Viability apply to and form part of this RFSA.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

(a) Suppliers must provide the required certifications and additional information to be issued a SA.

(b) The certifications provided by Suppliers to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a Submission non-responsive, or will declare a Supplier in default if any certification made by the Supplier is found to be untrue whether made knowingly or unknowingly during the Submission evaluation period, or during the period of any SA arising from this RFSA and any resulting contracts.

(c) The Supply Arrangement Authority will have the right to ask for additional information to verify the Supplier's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Supply Arrangement Authority may render the Submission non-responsive, or constitute a default under the Supply Arrangement.

5.1 Certifications Required with the Submission

Suppliers must submit the following duly completed certifications as part of their Submission:

5.1.1 Integrity Provisions - Declaration of Convicted Offences

In accordance with the Integrity Provisions of the Standard Instructions, all Suppliers must provide with their Submission, **if applicable**, the declaration form available on the Forms for the Integrity Regime website (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html), to be given further consideration in the qualification process.

5.1.2 Additional Certifications Required with the Submission

The following additional certification documents are required as part of the Submission (as applicable):

Form 2 Software as a Service Publisher Certification Form
Form 3 Software as a Service Publisher Authorization Form
Form 4 Certification Requirements for the Set-Aside Program for Aboriginal Business
Form 5 - Submission Completeness Review Checklist

PART 6 - SUPPLY ARRANGEMENT

6.1 Supply Arrangement

Supply Arrangement(s) (SAs) will be issued to allow Canada to acquire Software as a Service (SaaS) Solutions, including associated maintenance and support, training and other professional services, as required by Canada, in support of its various programs, operational needs and projects.

The objectives of this method of supply are to:

a) simplify the procurement process to acquire SaaS Solutions;

b) and support GC procurement modernization and contract simplification initiatives;

c) increase competition and access to the latest SaaS Solutions on the market for the GC; and

d) increase transparency, openness and fairness in public sector procurement processes.

6.2 Security Requirements

The Supplier must meet the security requirements as indicated in Annex A, Qualification Requirements and Annex B – Security & Privacy Obligations.

Note to Suppliers: This RFSA contains the essential mandatory security requirements to qualify as a Supplier in the SA. 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. Additional security requirements may be included in a subsequent bid solicitation, contract or task authorization under a contract issued under this SA, as applicable.

6.3 Standard Clauses and Conditions

All clauses and conditions identified in the Request for Supply Arrangement and resulting contract(s) by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by PSPC.

6.3.1 General Conditions

2020 (2017-09-21) General Conditions - Supply Arrangement - Goods or Services, apply to and form part of the Supply Arrangement.

6.3.2 Supply Arrangement Reporting

The Supplier must compile and maintain records on its provision of goods, services or both to the federal government under contracts resulting from the SA. This data must include all purchases, including those paid for by a Government of Canada Acquisition Card.

The data must be submitted to the Supply Arrangement Authority or made available for download on a quarterly basis, no later than 30 calendar days after the end of each reporting period.

The quarterly reporting periods are defined as follows:

(a) 1st quarter: April 1 to June 30;
(b) 2nd quarter: July 1 to September 30;

(c) 3rd quarter: October 1 to December 31;
(d) 4th quarter: January 1 to March 31.

6.4 Term of Supply Arrangement

6.4.1 Period of the Supply Arrangement

The period for awarding contracts under the SA is from the date of issuance of an SA to a Supplier, up to and including the date that the Supply Arrangement is terminated or expires.

6.4.2 Comprehensive Land Claims Agreements (CLCAs)

The SA is for the delivery of the requirements detailed in the SA to the Identified Clients across Canada (as defined in Article 6.6, below), excluding locations within Yukon, Northwest Territories, Nunavut, Quebec, and Labrador that are subject to Comprehensive Land Claims Agreements (CLCAs). Any requirement for deliveries to locations within CLCAs areas within Yukon, Northwest Territories, Nunavut, Quebec, or Labrador will have to be treated as a separate procurement, outside of the SA.

6.5 Authorities

6.5.1 Supply Arrangement Authority

The Supply Arrangement Authority is:

Name: Elizabeth Quenville
Title: A/Supply Team Leader

Public Works and Government Services Canada
Acquisitions Branch
Software Procurement Directorate

Les Terrasses de la Chaudière, 4th Floor
10 Wellington St.
Gatineau, Quebec K1A 0H4

Telephone: 613-858-6142
Facsimile: 819-956-2675
E-mail address: TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

The Supply Arrangement Authority is responsible for the issuance of the SA, its administration and its revision, if applicable.

6.5.2 Supplier's Representative

Fill in or delete, as applicable.

6.5.3 Supply Chain Security Authority

The Supply Chain Security Authority for the Contract is:

Name: _____
Title: _____
SSC : _____

Address: _____
Telephone: _____
E-mail address: _____

The Supply Chain Security Authority is the SSC representative and is responsible for all matters concerning the ongoing Supply Chain Integrity Process under the Contract. Neither the Contracting Authority nor the Technical Authority have any authority to advise or authorize any information in relation to the Supply Chain Integrity Process. All other security-related matters remain the responsibility of the Supply Chain Security Authority.

6.6 Identified Clients

The SA may be used to acquire SaaS Solutions by any Government Department, Departmental Corporate or Agency, or other body of Canada (including those described in the Financial Administration Act as amended from time to time), and any other party for which PSPC has been authorized to act.

6.7 On-going Opportunity for Qualification

A Notice will be posted continuously on the Government Electronic Tendering Service (GETS) to allow new Suppliers to become qualified.

6.8 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list:

(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)*.

6.9 Certifications and Additional Information

6.9.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Supplier in its Submission or precedent to issuance of the SA, and the ongoing cooperation in providing additional information are conditions of issuance of the SA and failure to comply will constitute the Supplier in default. Certifications are subject to verification by Canada during the entire period of the SA and of any resulting contract that would continue beyond the period of the SA.

6.10 Applicable Laws

The Supply Arrangement (SA) and any contract resulting from the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____ *(insert the name of the province or territory as specified by the Supplier in the Submission, if applicable).*

PART 7 - CONTRACTOR SELECTION AND RESULTING CONTRACT CLAUSES

7. 1 Contracting Authorities and Limits

Client and PSPC contracting officers who have been given the authority by PSPC to use the SA can issue resulting contracts using their existing delegated contract approval and signing authorities.

7. 2 Contractor Selection

(a) **Requirements valued at less than $25,000.00 CAD (GST/HST/QST included)**

(i) **Sole Source:** For requirements under $25,000.00 CAD (Applicable Taxes included), Canada may choose, at its sole discretion, to direct contracts to a Supplier or to issue contracts following Bid Solicitations.

(ii) If only one source of supply exists for the required SaaS Solution, Canada may request that the Supplier submit price support prior to any contract award. Canada reserves the right to negotiate with the Supplier if it is determined that the prices being offered do not represent good value to Canada.

(b) **Requirements valued at $25,000.00 CAD (Applicable Taxes included) or greater**

(i) **Bid Solicitation:** If multiple SaaS Solutions are available from the GC SaaS Catalogue that can meet Canada's technical requirements, Canada may issue a bid solicitation. If Canada determines that there is no sufficient capability under the GC SaaS Catalogue or it is a complex and/or specialized requirement, Canada may acquire the SaaS Solution outside the GC SaaS Catalogue and extend the competition to all firms by posting a formal bid solicitation document on the Government Electronic Tendering Service (GETS).

(c) **Set-Aside / Aboriginal Business**

(i) At the discretion of each Client, some solicitations against the resulting SAs may be set-aside for Aboriginal Business under the federal government's PSAB.

(ii) In the event that Canada wishes to issue a Contract under the PSAB, Canada may do so by utilizing the Aboriginal Suppliers' SAs. All the terms and conditions as stated in this SA apply to the Aboriginal Suppliers SAs.

7. 3 Bid Solicitation Process

(a) Bids will be solicited for specific requirements within the scope of the SA from Suppliers who have been issued a SA.

(b) The bid solicitation will be posted on the GETSor sent directly to Suppliers.

(c) Suppliers will have a minimum of 15 calendar days to respond to Canada or as specified by the Contracting Authority, whichever is longer.

(d) The bid solicitation will contain as a minimum the following:

(i) Additional or updated security requirements (*if applicable*);

(ii) a complete description of the SaaS Solution to be provided;

(iii) 2003, Standard Instructions - Goods or Services - Competitive Requirements;

Subsection 3.a) of Section 01, Integrity Provisions - Bid of the Standard Instructions 2003 incorporated by reference above is deleted in its entirety and replaced with the following:

"at the time of submitting an arrangement under the Request for Supply Arrangements (RFSA), the Bidder has already provided a list of names, as requested under the *Ineligibility and Suspension Policy*.During this procurement process, the Bidder must immediately inform Canada in writing of any changes affecting the list of directors."

(iv) bid preparation instructions;

(v) instructions for the submission of bids (address for submission of bids, bid closing date and time);

(vi) evaluation procedures and basis of selection;

(vii) financial capability (*if applicable*);

(viii) certifications*; and,*

(ix) conditions of the resulting contract.

(e) Annex E – SaaS Bid Solicitation Template may be used to conduct Bid Solicitations.

7. 4 Resulting Contract Clauses

(a) It is a condition of the Supply Arrangement that the Resulting Contract Clauses included in Annex F apply and are incorporated in each and every Contract issued against the Supply Arrangement. The Resulting Contract Clauses may include additional requirements identified by the Client.

Annex A – Qualification Requirements

The following fifteen (15) Security requirements must be met in order to demonstrate compliance with Tier 1 Assurance **(Up to and including Protected A Data).**

1. Tier 1 Assurance (Up to and including Protected A Data).

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M1	Roles and Responsibilities for Security	The Supplier must clearly delineate the roles and responsibilities for the security controls and features of the Solution between the Supplier (any Supplier Sub-processors, as applicable) and Canada.	In the document, the Supplier must include, at a minimum, the parties' roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.
M2	Data Protection	The physical locations of the Commercially Available Public Software as a Service[1] (which may contain Canada's data) and define in the must be located in either: a) A country within the North Atlantic Treaty Organization (NATO); b) A country within the European Union (EU); or c) A country with which Canada has an international bilateral industrial security instrument Suppliers please note Additional information on countries within NATO can be located at the following link: https://www.nato.int/cps/en/natohq/nato_countries.htm Additional information on countries within the EU can be located at the following link: https://europa.eu/european-union/about-eu/countries_en The Contract Security Program has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time	The Supplier must provide documentation that demonstrates how the proposed Commercially Available Public Software as a Service submitted meets the mandatory requirement outlined in Data Protection Requirements. To be considered compliant, the provided documentation must include: a) an up-to-date list of the physical locations (including city and country) for each data centre that may contain Canada's data including in backups or for redundancy purposes. The substantiation required for Data Protection Requirements. The documentations cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Software as a Service Provider meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers

[1] For the purposes of this annex A, Commercially-Available Solution. Solution that is a commercially-available solution provided to other customers. As part of the subscription to use the Solution, the Contractor agrees to make available to Canada all the features and functionalities included in the commercially available version of the Solution, and the incidental and required information technology infrastructure services required to deliver the Solution, all of which is included in the subscription price.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M3	Data Center Facilities	The Supplier of the proposed Commercially Available Public Software as a Service must implement security measures that ensure the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. This includes, at a minimum a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; b) proper handling of IT media; c) controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; d) controlled access to information system output devices to prevent unauthorized access to Canada's data; e) limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; f) escorting visitors and monitoring visitor activity; g) maintaining audit logs of physical access; h) controlling and managing physical access devices; i) enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.	The Supplier must provide documentation that demonstrates how the Software as a Service Provider (and if applicable the Alternative Service Provider) of the proposed Services complies with the requirements in Data Center Facilities Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are used to ensure the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. The substantiation required for Data Center Facilities Requirements documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M4	Personnel Security	The Supplier of the proposed Commercially Available Public 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. Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada. This includes, at a minimum: a) description of the employee and subcontractor positions that require access to Canada's Data or have the ability to affect the confidentiality, integrity or availability of the Services; b) process for ensuring that employees and contractors understand, are aware, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered; c) process for security awareness and training as part of employment onboarding and when employee and subcontractor roles change; d) process that is enforced when an employee or subcontractor changes their role or when employment is terminated; and e) approach for detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of Software as a Services hosting GC assets and data	The Supplier must provide documentation that demonstrates how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in the Personnel Security Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, process and procedures that are used to grant and maintain the required level of security screening for the Software as a Service Provider and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. The substantiation required in the Personnel Security Requirements documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M5	Third Party Assurance	The Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Public Software as a Service, including, implementing information security policies, procedures, and security controls	The Supplier must provide documentation to Canada that demonstrates how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in the Third Party Assurance Requirements. Compliance must be demonstrated by providing one or more of the following industry certifications identified below, and validated through independent third party assessments. The Supplier must provide the following industry certifications for the proposed Service to demonstrate compliance: 1) One of the following: (i) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; or (ii) AICPA Service Organization Control (SOC) 2 Type II 2) Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version. Each provided certification and assessment report must: a) Be valid as of the Submission date; b) Identify the legal business name of the proposed Supplier, and applicable Supplier Sub-processor, including CSP; c) Identify the current certification date and/or status; d) identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report. e) The scope of the report must map to locations and services offered by the proposed Supplier. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included; and f) Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality management system standard. Please note • Certifications must be provided for all portions of the proposed Service identified • Certifications must be accompanied by assessment reports. • Certifications must be valid and within the 12 months prior to the start of a contract

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M6	Supply Chain Management	The Supplier must provide a third party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, including Cloud Service Providers, etc.) that would provide Canada with the proposed Commercially Available Public Software as a Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Software as a Service Provider of the proposed Commercially Available Public Software as a Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Public Software as a Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Public Software as a Services of the Software as a Service Provider that have been proposed by the Supplier. Please note Suppliers are advised that subsequent procurement phases may require the Supplier to notify Canada regularly when there are updates to the list of third party suppliers.	The Supplier must provide documentation list of Sub-processors that could be used to perform any part of the Services in providing Canada with the Services. 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 location(s) where the Sub-processor would perform the activities required to support the Services. (1) For SaaS, the Contractor must demonstrate that the IaaS/PaaS leveraged by the Services: (a) Supplier Sub-processors have been assessed by the CCCS Program as per ;and (b) Supplier meet the security obligations for Sub-Processors and/or Subcontractors outlined by the Supplier, for the life of the contract. If the Supplier of the proposed Commercially Available Public Software as a Service does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Public Software as a Service, the Supplier is requested to indicate this in their response to this requirement.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M7	Supply Chain Risk Management	The Supplier of the proposed Commercially Available Public Software as a Service must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services. 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.	The Supplier must demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in Supply Chain Risk Management Requirements as documented under the Software as a Service Provider Information Technology Security Assessment program. To be considered compliant, the provided documentation demonstrating compliance by providing at least one of the following three options: 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Software as a Service Provider's approach to SCRM and demonstrate how the Supplier of the proposed Commercially Available Public Software as a Service will reduce and mitigate supply chain risks

M8	Privileged Access Management	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrate how to the Software as a service is able to meet the following security requirements Privileged Access Management Requirements: (a) Manage and monitor privileged access to the Solution, including the underlying infrastructure, to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services; (b) Restrict and minimize access to the Services and Canada's Data's to only authorized devices and End Users with an explicit need to have access; (c) Enforce and audit authorizations for access to the Services and Canada's Data's; (d) Constrain all access to service interfaces that host Assets and Canada's Data's to uniquely identified, authenticated and authorized End Users, devices, and processes (or services); (e) Implement password policies to protect credentials from compromise by either on-line or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (f) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets; (h) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles; (i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets;	The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to meet the security requirements related to the Privileged Access Management Requirements: To be considered compliant, the provided documentation must include: a) System documentation or white paper that outlines the policies, processes and procedures used to manage privileged access management. The substantiation required for the Privileged Access Management documentation, cannot simply be a repetition of the mandatory requirement but must explain and demonstrate and indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers., on how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
		(j) Access controls on objects in storage and granular authorization policies to allow or limit access (k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Services and Supplier Infrastructure; (l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and (m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.	

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M9	Federation of Identity	**Federation of Identity** The Supplier must have the ability for Canada to support federated identity integration including: (a) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and (c) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding cloud service user account(s).	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Federation of Identity. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Federation of Identity. The substantiation required for in the Federation of Identity cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M10	Endpoint Protection	**Endpoint Protection** The Supplier must implement, manage, and monitor security-hardened endpoints to prevent against attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Endpoint Protection. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Endpoint Protection. The substantiation required for in the Endpoint Protection the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M11	Secure Development	**Secure Development** The Supplier must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Secure Development. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Secure Development. The substantiation required for in the Secure Development, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M12	Supplier Remote Management	**Supplier Remote Management** The Supplier must manage and monitor remote administration of the Supplier's Service that are used to host GC services and take reasonable measures to: (a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Employ a CSEC Approved Cryptographic Algorithmscryptographic mechanisms to protect the confidentiality of remote access sessions; (c) Route all remote access through controlled, monitored, and audited access control points; (d) Expeditiously disconnect or disable unauthorized remote management or remote access connections; (e) Authorize remote execution of privileged commands and remote access to security-relevant information.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Supplier Remote Management. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Supplier Remote Management The substantiation required for in the Supplier Remote Management , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M13	Information Spillage	**Information Spillage** (1) The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Submission; or (ii) another best practice of Leading Service Providers approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for identifying the specific Information Asset that is involved in an Asset's or System's contamination; (b) A process to isolate and eradicate a contaminated Asset or System; and (c) A process for identifying Assets or Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. (2) The Supplier must provide an up-to-date information spillage process to Canada on an annual basis, or promptly following any Change to the Supplier's information spillage process.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Information Spillage. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Information Spillage. The substantiation required for in the Information Spillage, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M14	Cryptographic Protection	**Cryptographic Protection** The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Cryptographic Protection. (a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods; (b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); (c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and (d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Cryptographic Protection To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Cryptographic Protection The substantiation required for in the Cryptographic Protection, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1
M15	Data Segregation	The Supplier must, for both Tiers, implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Supplier's Service's and Supplier Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support: (a) The separation between Supplier's internal administration from resources used by its customers; and (b) The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements.

The following twenty (20) Security requirements must be met in order to demonstrate compliance with Tier 2 Assurance **(Up to and including Protected B Data).**

2. Tier 2 Assurance (Up to and including Protected B Data).

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M1	Roles and Responsibilities for Security	The Supplier must clearly delineate the roles and responsibilities for the security controls and features of the Services between the Supplier (any Supplier Sub-processors, as applicable) and Canada.	In the document, the Supplier must include, at a minimum, the parties' roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system backup; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.
M2	Master / Root Account Management	The Supplier of the proposed Commercially Available Software as a Service must have the ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. This includes ensuring that credentials remain within the geographic boundaries of Canada.	The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. 1) To be considered compliant, the provided documentation must include: 2) a) System documentation or white paper that outlines the policies, processes and procedures used to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. 3) The substantiation required for the Master / Root Account Management, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers. 4) Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
			Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

M3	Data Protection Isolation	The proposed Services must provide the GC the ability to isolate data in Canada in an approved data center. For the purposes of this solicitation, an Approved Data Centre is defined as the following: a) A data center that is geographically located in Canada; and b) A data centre that meets all security requirements and certifications identified. Data Center Facilities Requirements: The Supplier of the proposed Commercially Available Software as a Service must ensure that security measures are implemented for the protection of IT facilities and information system assets on which Canada data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. Physical protection measures must be applied in accordance with, or use an adequate risk-based approach aligned with the physical and environmental protection (PE), maintenance (MA), and media protection (MP) security controls outlined in ITSG-33 Government of Canada Security Control Profile for Cloud-Based GC IT Services for PBMM and the practices in the Royal Canadian Mounted Police (RCMP) guidance and standards on physical security. This includes, at a minimum a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; b) proper handling of IT media; c) controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; d) controlled access to information system output devices to prevent unauthorized access to Canada's data; e) limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; f) escorting visitors and monitoring visitor activity; g) maintaining audit logs of physical access;	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Data Center Facilities Requirements To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. The substantiation required for Data Center Facilities Requirements - , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		h) controlling and managing physical access devices; i) enforcing safeguarding measures for Canada data at alternate work sites (e.g., telework sites); and j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.	
M4	Data Segregation	The Supplier must, for both Tiers, implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Supplier's Service's and Supplier Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support: (a) The separation between Supplier's internal administration from resources used by its customers; and (b) The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M5	Data Protection	The Supplier of the proposed Commercially Available Software as a Services must have the ability or the Government of Canada to store and protect its information at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada. This includes: a) Identifying and providing the Government of Canada with an up-to-date list of physical locations including city which may contain Canada's data in Canada for each data centre that will be used to provide Services. b) Identifying which portions of the Services are delivered from outside of Canada including all locations where data is stored and processed and where they manage the service from. c) ensuring the infeasibility of finding a specific customer's data on physical media; and d) Employing encryption to ensure that no data is written to a disk in an unencrypted form. Suppliers please note Suppliers are advised that subsequent procurement phases may require the Supplier of the proposed Commercially Available Software as a Service to notify Canada when there are updates to the list of physical locations which may contain Canada's data.	The Supplier must demonstrate compliance by providing documentation outlining proposed Commercially Available Software as a Service's ability to isolate data in Canada in an approved data center. To be considered compliant, the provided documentation must include the following: a) Screen shots of the available data center where Canadian data centers are on the availability list; and b) A list or map indicating where geographically the data centers are located in Canada. The substantiation required for this criteria cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M6	Data Center Facilities	The Supplier of the proposed Commercially Available Software as a Service must ensure that security measures are implemented for the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. Physical protection measures must be applied in accordance with, or use an adequate risk-based approach aligned with the physical aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329) . The security measures required under this include, at a minimum; a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Data Center Facilities Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of IT facilities and information system assets on which Canada data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. The substantiation required for Data Center Facilities Requirements, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; b) proper handling of IT media; c) controlled maintenance of information systems and their components to protect their integrity and ensure their ongoing availability; d) controlled access to information system output devices to prevent unauthorized access to Canada's data; e) limiting physical access to its information system assets to authorized employees and contractors based on position or role and the need-to-access principle, and validated by two forms of identification; f) escorting visitors and monitoring visitor activity; g) maintaining audit logs of physical access; h) controlling and managing physical access devices; i) enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.	Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M7	Personnel Security	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. Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115) , or use an acceptable equivalent agreed to by Canada. This includes, at a minimum: a Personnel Security) description of the employee and subcontractor positions that require access to Canada's Data or have the ability to affect the confidentiality, integrity or availability of the Services;	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Personnel Security Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including the policies, processes and procedures that are used to grant and maintain the required level of security screening for the Supplier and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. The substantiation required in the Personnel Security Requirements , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		b) process for ensuring that employees and contractors understand, are aware, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered; c) process for security awareness and training as part of employment on boarding and when employee and subcontractor roles change; d) process that is enforced when an employee or subcontractor changes their role or when employment is terminated; and e) approach for detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of cloud services hosting GC assets and data	material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M8	Third Party Assurance	The Supplier of the proposed Commercially Available Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Software as a Service, including, implementing information security policies, procedures, and security controls. The Supplier of the proposed Commercially Available Software as a Service must also comply with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) for the scope of the proposed Commercially Available Software as a Service provided. Compliance will be validated and verified through the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100) . Any Supplier that has participated in the process must provide documentation to confirm that they have completed the on-boarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS. This will accelerate	The Supplier must demonstrate how the Supplier of the proposed Commercially Available Software as a Service complies with the requirements in the Third Party Assurance Requirements. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments. The Supplier must provide each of the following industry certifications to demonstrate compliance: 1) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and 2) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; and 3) AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. Each certification or assessment report must: a) Be valid as of the Submission date; b) Identify the legal business name of the proposed Commercially Available Software as a Service and Cloud Service Provider; c) Identify the current certification date and/or status; d) identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		the qualification process and at the same doesn't require the Supplier to demonstrate the compliance To initiate the on-boarding process, the Supplier should contact the CCCS Client Services to receive a copy of the onboarding submission form and any additional information related to the CSP IT Assessment Program.	e) The scope of the report must map to locations and services offered by the proposed Commercially Available Software as a Service. If the carved-out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included; and f) Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality system standard. The Supplier can provide additional supplementary evidence from system security plans, information system design, information system architecture, or documents that provide a comprehensive system description, such as assessment of its Services against the Cloud Security Alliance (CSA) Cloud Control's Matrix (CCM) version 3.01 or subsequent version, to support the claims from the above certifications, in order to demonstrate compliance to the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM). Please note • Certifications must be provided for all portions of the proposed Service. • Certifications must be accompanied by assessment reports.
M9	IT Security Assessment Program	The Supplier must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services available (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) for the scope of the Services provided by the Supplier in the IT Security Assessment Program.	The Supplier must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services available (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) for the scope of the Services provided by the Supplier in the IT Security Assessment Program (Section XX). Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments. Mapping of the Security Controls must a included; GC Security Control Profile for Cloud-Based GC IT Services , and Industry Certification in Third-Party Assurance (Section XX).

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M10	Supply Chain Management	The Supplier must provide a third-party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, etc.) that would provide Canada with the proposed Commercially Available Software as a Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Supplier of the proposed Commercially Available Software as a Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Software as a Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Software as a Services of the Supplier has been proposed by the Supplier. Please note: Suppliers are advised that subsequent procurement phases may require the Supplier to notify Canada regularly when there are updates to the list of third-party suppliers.	The Supplier must provide documentation that lists information on any third parties that could be used to perform any part of the supply chain that would provide Canada with the proposed Commercially Available Software as a Service whether they would be (i) subcontractors to the Supplier, or (ii) subcontractors to subcontractors of the Supplier down the chain, OR (iii) any subsidiaries. The Supplier must fill out the Form 6 - SCI Submission Template as provided under this RFSA. If the Supplier does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Software as a Service, the Supplier is requested to indicate this in their response to this requirement. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M11	Supply Chain Risk Management	The Supplier of the proposed Commercially Available Software as a Services 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 Services. 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.	The Supplier must demonstrate how the Supplier of the proposed Commercially Available Software as a Service complies with the requirements in the Supply Chain Risk Management Requirements as documented under the Supplier Information Technology Security Assessment program. To be considered compliant, the provided documentation must demonstrate that the Commercially Available Software as a Service supply chain risk management approach aligns with one of the following best practices. 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Supplier's approach to SCRM and demonstrate how the Suppliers of the proposed Commercially Available Software as a Service will reduce and mitigate supply chain risks. The SCRM Plan must be independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M12	Privacy	The Supplier of the proposed Commercially Available Software as a Service must demonstrate that it is compliant with the privacy policies, procedures, and provisions that meet the following industry certification: a) ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Please note: Suppliers are advised that subsequent procurement phases may require the Supplier to confirm to Canada on a regular basis that the proposed Commercially Available Software as a Service meets the above certification, and that the certification is valid for the full term of the procurement vehicle.	To demonstrate compliance to the certification, the Supplier must provide: a) A copy of the Commercially Available Software as a Service and Cloud Service Provider most recent and ISO 27018 certification documents, which must have been issued within 12 months prior to the Submission date; and b) A copy of the ISO 27018 assessment report for their current Commercially Available Software as a Services and Cloud Service Provider. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M13	Privacy by Design	The Supplier must demonstrate that it: (a) Implements a software development lifecycle that conforms to ISO 27032 and implements privacy by design; (b) Is compliant with the Privacy Management Framework and policy requirements that are specified in the ISO Standard 29100; and (c) Adheres to the privacy by design 7 foundational principles (see https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M14	Privileged Access Management	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrates how to the Software as a service is able to meet the following security requirements Privileged Access Management Requirements: (a) Manage and monitor privileged access to the Solution, including the underlying infrastructure, to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services; (b) Restrict and minimize access to the Services and Canada's Information Assets to only authorized devices and End Users with an explicit need to have access; (c) Enforce and audit authorizations for access to the Services and Information Assets; (d) Constrain all access to service interfaces that host Assets and Information Assets to uniquely identified, authenticated and authorized End Users, devices, and processes (or services); (e) Implement password policies to protect credentials from compromise by either on-line or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials (ii) unusual use of credentials, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (f) Implement multi-factor authentication mechanisms to authenticate (Tier 2 only) End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets; (h) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles	The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to meet the security requirements related to the Privileged Access Management Requirements: To be considered compliant, the provided documentation must include: a) System documentation or white paper that outlines the policies, processes and procedures used to manage privileged access management. The substantiation required for the Privileged Access Management , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		from operational roles, and access management roles from other operational roles; (i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets; (j) Access controls on objects in storage and granular authorization policies to allow or limit access (k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Services and Supplier Infrastructure; (l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and (m) Upon the termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.	

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M15	Federation of Identity	**Federation of Identity** The Supplier must have the ability for Canada to support federated identity integration including: (a) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and (c) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding cloud service user account(s).	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Federation of Identity. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Federation of Identity. The substantiation required for in the Federation of Identity cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M16	Endpoint Protection	**Endpoint Protection** The Supplier must implement, manage, and monitor security-hardened endpoints to prevent against attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Endpoint Protection. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Endpoint Protection. The substantiation required for in the Endpoint Protection the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M17	Secure Development	**Secure Development** The Supplier must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Secure Development. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Secure Development. The substantiation required for in the Secure Development, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M18	Supplier Remote Management	**Supplier Remote Management** The Supplier must manage and monitor remote administration of the Supplier's Service that are used to host GC services and take reasonable measures to: (a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Employ a CSEC Approved Cryptographic Algorithmscryptographic mechanisms to protect the confidentiality of remote access sessions; (c) Route all remote access through controlled, monitored, and audited access control points; (d) Expeditiously disconnect or disable unauthorized remote management or remote access connections; (e) Authorize remote execution of privileged commands and remote access to security-relevant information.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Supplier Remote Management. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Supplier Remote Management The substantiation required for in the Supplier Remote Management , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M19	Information Spillage	**Information Spillage** (1) The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Submission; or (ii) another best practice of Leading Service Providers approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for identifying the specific Information Asset that is involved in an Asset's or System's contamination; (b) A process to isolate and eradicate a contaminated Asset or System; and (c) A process for identifying Assets or Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. (2) The Supplier must provide an up-to-date information spillage process to Canada on an annual basis, or promptly following any Change to the Supplier's information spillage process.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Information Spillage. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Information Spillage. The substantiation required for in the Information Spillage, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M20	Cryptographic Protection	**Cryptographic Protection** The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Cryptographic Protection. (a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods; (b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); (c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and (d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Cryptographic Protection To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Cryptographic Protection The substantiation required for in the Cryptographic Protection, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Annex B – Security & Privacy Obligations

General

Purpose

The purpose of this Annex is to set forth the obligations of the Supplier relating to the proper configuration and management of Assets and Information Assets, in order to protect such Assets and Information Assets from unauthorized modification, access or exfiltration, all in accordance with the Supply Arrangement, this Annex, the Supplier's Specific Security Measures, and Canada's Security & Privacy Policies (collectively, the "Security & Privacy Obligations").

Flow-Down of Security & Privacy Obligations

The obligations of the Supplier contained in these Security & Privacy Obligations must be flowed down by the Supplier to Supplier Sub-processors, to the extent applicable to each Supplier Sub-processor, given the nature of the services provided by it to the Supplier.

Change Management

The Supplier must, throughout the period of the SA, take all steps required to update and maintain the Security & Privacy Obligations as needed to comply with the security practices of industry standards.

The Supplier must advise Canada of all improvements that affect the Services in the Supply Arrangement, including technological, administrative or other types of improvements. The Supplier agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

1. Acknowledgments

The parties acknowledge that:

(a) All Assets and Information Assets are subject to these Security & Privacy Obligations.

(b) Notwithstanding any other provision of this Annex, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Assets and Information Assets.

(c) The Supplier must not have or attempt to gain custody of any Information Asset, nor permit any Services Personnel to access any Information Asset prior to the implementation of the Security & Privacy Obligations as required under this Annex on or before Supply Arrangement award.

(d) Security Obligations apply to both Tier 1 (up to Protected A / Low injury) and for Tier 2 (up to Protected B / Medium injury), unless specified.

2. Securing Information Assets

The Supplier's SaaS Solution(s) must be designed to protect Assets and Information Assets from unauthorized access, modification, or exfiltration. This includes implementing and maintaining appropriate information security policies, procedures, and security controls to preserve the confidentiality, integrity, and availability of Assets and Information Assets (hereinafter referred to as the "Specific Security Measures").

3. Roles and Responsibilities for Security

The Supplier must provide to Canada an up-to-date document that delineates the roles and responsibilities between the Supplier, Supplier Sub-processors, and Canada for security controls and features: (i) on an annual basis; (ii) when there are significant changes to such roles and responsibilities as a result of a Change to the Services; or (iii) upon request of Canada.

4. Cloud Service Provider (CSP) IT Security Assessment Program

Upon request of Canada, additional supplementary evidence from the Supplier, including System security plans, designs, or architecture documents that provide a comprehensive System description, may be provided by the Supplier or a Supplier Sub-processor to supplement the certification and audit reports described in Section 5 (Auditing Compliance for Security Obligations) in order to demonstrate the Supplier's compliance with the required industry certifications.

5. Auditing Compliance for Security Obligations

(1) The Supplier must conduct the privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting Assets and Information Assets as follows:

(a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

(c) Each audit will be performed by qualified, independent, third party auditor that (i) are qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conform to the ISO/IEC 17020 quality management system standard at the Supplier's selection and expense.

(2) Each audit will result in the generation of an audit report that must be shared with Canada. The audit report must clearly disclose any material findings by the third party auditor. The Supplier must promptly remediate issues raised in any audit report to the satisfaction of the auditor, and must (i) provide Canada with the plan to correct any negative findings arising from such reports and (ii) provide implementation progress reports to Canada upon request within ten (10) Federal Government Working Days.

6. Application Programming Interface (API)

The Supplier (Tier 1 and 2) must:

(a) Provide Services that use open, published, supported, and documented Application Programming Interfaces (API) to support interoperability between components and to facilitate migrating applications.

(b) Take reasonable measures to protect both internal and external APIs through secure authentication methods. This includes ensuring that all externally exposed API queries require successful authentication before they can be called.

For SaaS, the Supplier must provide APIs that provide the ability to:

(a) Interrogate data at rest in SaaS applications; and

(b) Assess events and incidents stored in SaaS application logs.

7. Network and Communications Security

The Supplier (Tier 1 and 2) must:

(a) Provide the ability for Canada to establish secure connections to the Services, including providing data-in-transit protection between Canada and the Service using TLS 1.2, or subsequent versions, and using supported cryptographic algorithms and certificates, as outlined in Communication Security Establishment (CSE)'s ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111);

(b) Provides data-in-transit protection between microservices and applications used within the Services;

(c) Use correctly configured certificates within the TLS connections in accordance with CSE guidance.

(d) Disable known-weak protocols such as all versions of Secure Sockets Layer (SSL) (e.g. SSLv2 and SSLv3) and older versions of TLS (e.g. TLS 1.0 and TLS 1.1), as per CSE ITSP.40.062, and known-weak ciphers (e.g. RC4 and 3DES); and

(e) Provide the ability for Canada to implement network access controls and security rules that allow or deny network traffic to Canada resources.

8. Key Management

For Tier 2, the Supplier must have the ability to provide Canada with a unique dedicate key management service that enables:

(a) Creation/generation and deletion of encryption keys use for deliver the SaaS Solution to the GC;

(b) Definition and application of GC-specific policies that control how keys can be used;

(c) Protection of access to the key material including prevention from Supplier access to the key material in unencrypted fashion; and

(d) Audits all events related to key management services, including Supplier access for Canada's review.

9. Dedicated Connections

For Tier 2, the Supplier must provide the ability for the GC to establish private redundant connectivity to the Services. This includes:

(a) Support for virtualization and multi-tenancy for all network components;

(b) Support for dynamic routing protocols (BGP) for all connections;

(c) Support for GC-approved protocols as outlined in:

i. ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites
ii. ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information

(d) Provide a description of all the data centre geographical locations in Canada where the capability is available.

10. Logging and Auditing (Tier 1 and 2)

(1) The Supplier must implement log generation and management practices and controls for all Service components that store or process Assets and Information Assets, and that conform with the practices of Leading Service Providers, such as those found in NIST 800-92 (Guide to Computer Security Log Management), or an equivalent standard approved by Canada in writing.

(2) The Supplier must enable Canada to centrally review and analyze audit records from multiple components within the Services provided by the Supplier. This includes the ability for Canada to:

(a) log and detect audit events such as a minimum of (i) successful and unsuccessful account login attempts, (ii) account management, (iii) object access and policy change, (iv) privilege functions and process tracking, (v) system events, (vi) deletion of data;

(b) record in logs (or log files) audit events that are time synchronized and time-stamped in coordinated universal time (UTC) and protected from unauthorized access, modification, or deletion while in transit and at rest;

(c) separate Security Incidents and logs for different Client accounts to enable Canada to monitor and manage events within its boundary that are affecting its instance of an IaaS, PaaS or SaaS Service provided to it by the Supplier or a Supplier Sub-processor; and

(d) forward Client events and logs to a GC-managed centralized audit log system using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.).

11. Security Incident Management (Tier 1 and 2)

(1) The Supplier's Security Incident response process for the Services must encompass the

IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities, aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or (iv) other best practices of Leading Service Providers if Canada determines, in its discretion, that they meet Canada's security requirements.

(2) The Supplier's Security Incident response process must include the following:

(a) A documented process and procedures of how the Supplier will identify, respond, remediate, report, and escalate Security Incidents to Canada, including: (i) the scope of the Security Incidents that the Supplier must report to Canada; (ii) the level of disclosure and the measures used by the Supplier for detection of Security Incidents, and the Supplier's associated responses for specific types of Security Incident; (iii) the target timeframe in which notification and escalation of Security Incidents will occur; (iv) the procedure for the notification and escalation of Security Incidents; (v) contact information for the handling of issues relating to Security Incidents; and (vi) any remedies that apply if certain Security Incidents occur.

(b) Procedures for responding to requests for potential digital evidence or other information from within the Supplier's service environment or Supplier Infrastructure, including forensic procedures and safeguards for the maintenance of a chain of custody over Information Assets stored or processed by the Supplier or a Supplier Sub-processor. Forensic and digital evidence practices and controls must conform with the practices of Leading Service Providers, such as those found in NIST 800-62 (Guide to Integrating Forensic Techniques into Incident Submission), ISO 27037 (Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence), or an equivalent standard approved by Canada in writing.

12. Auditing Compliance FOR PRIVACY OBLIGATIONS

(1) In the event Canada needs to conduct security audits, inspections and/or review any additional information (e.g., documentation, data protection description, data architecture and security descriptions) pursuant to Annex B of the RFSA entitled "Security & Privacy Obligations", both Parties agree to negotiate a solution in good faith and consider both the rationale for Canada's request and the Contractor's processes and protocols.

(2) The Contractor must, engage a third party to conduct a privacy audit or provide evidence to confirm that it does not generate, collect, use, store or disclose any additional personal information as defined by Canada, other than Customer data as defined by the Contractor and does not specifically have Personal Identifiable Information in Support Data (collected in logs (e.g., telemetry data such as email message headers and content).

(3) The Contractor must conduct the privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing Canada's Data as follows:

(a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

(c) Each audit will be performed by qualified, independent, third party security auditors that (i) is qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conforms to the ISO/IEC 17020 quality management system standard at the Supplier's selection and expense.

(4) Each audit will result in the generation of an audit report that must be shared with Canada. The audit report must clearly disclose any material findings by the auditor. The Supplier must promptly remediate issues raised in any audit report to the satisfaction of the auditor, and must (i) provide Canada with the plan to correct any negative findings arising from such reports and (ii) provide implementation progress reports to Canada upon request within ten Federal Government Working Days.

(5) Upon request of Canada, additional supplementary evidence from the Supplier, including System security plans, designs, or architecture documents that provide a comprehensive System description, may be provided by the Supplier or a Supplier Sub-processor to supplement the certification and audit reports described in this in order to demonstrate the Supplier's compliance with the required industry certifications.

13. PROTECTING INFORMATION ASSETS

(1) Canada's Data including all Personal Information (PI) will be used or otherwise processed only to provide Canada the Services including purposes compatible with providing those Services. The Supplier must not use or otherwise process Canada's Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Canada retains all right, title and interest in and to Customer Data. The Supplier acquires no rights in Customer Data, other than the rights Customer grants to the Supplier to provide the Services to Customer.

14. Privacy Compliance

(1) The Supplier must demonstrate through third party assessment reports and audit reports that it:

(a) Restricts creating, collecting, receiving, managing, accessing, using, retaining, sending, disclosing and disposing of Personal Information to only that which is necessary to perform the work and;

(b) Has implemented updated security processes and controls such as access management controls, human resource security, cryptography and physical, operational and communications security that preserve the integrity, confidentiality and accuracy of all information and data and metadata, irrespective of format.

(2) This applies to all information, data and metadata in the Suppliers possession or under its care acquired pursuant to, or arises in any other way out of Contractor's responsibilities

and obligations under the Contract. The Contractor acknowledges that this is required in order to ensure that Canada can rely on the information, data and metadata and so that Canada can meet its own legal obligations, including statutory obligations. This is also required to ensure the information, data and metadata can be used as persuasive evidence in a court of law.

15. Privacy Officer

(1) The Supplier must, within 10 days of the issuance of the Supply Arrangement provide Canada with information that identifies an individual as a Privacy Officer to act as Contractor's representative for all matters related to the Personal Information and the Records. The Supplier must provide that person's name and contact information including the, individual’s business title, email address and phone number.

Annex C - SaaS Solutions and Ceiling Prices

Note to Supplier: This form must be completed and submitted as part of the Supplier's response to the RFSA.

PRODUCT LIST AND CEILING PRICES										
Item NO.	**SaaS Publisher's Part No.**	**SaaS Solution's Name**	**SaaS Publisher's Name**	**Cloud Service Provider's Name**	**Ceiling Prices**	**Unit of Measure**	**Applicable Percentage Discount**	**Language (s) available**	**SaaS Solution Information**	**Keywords/tags**
	(enter the Part Number that the SaaS Publisher uses to identify the SaaS Solution)	(enter the name that the SaaS Publisher uses to identify the SaaS Solution.	(enter the name of the SaaS Publisher that produces the SaaS Solution)	(enter the name of the Cloud Service Provider that hosts the SaaS)	(enter ceiling price for SaaS Solution per unit of measure in Canadian Dollars and any applicable professional Services)	(enter the unit of measure for the SaaS, such as "per user", "per entity", etc. **and** subscription, term)	(enter the percentage discount that will be applied to the Ceiling Commercial Unit Prices for the duration fo the SA)	(enter the language of the SaaS Solution, English and/or French)	(enter a web site URL containing SaaS Solution information)	(enter keywords associated with the SaaS Solution that will help the Clients to easily search and find SaaS Solutions that meet their needs
1										
2										
3										

Annex D – SaaS Service Level Agreements (SLA)

Only terms which are presented in the Submission form part of the Supply Arrangement. Suppliers may submit their SLAs by way of URLs. Suppliers are permitted to update their SLAs on an ongoing basis, providing that the changes to the SLA do not represent a decrease in the level of service being provided. Where a Supplier wishes to add a new SaaS Solution to their Supply Arrangement, the SLA(s) must be resubmitted to the Supply Arrangement Authority for acceptance prior to the SLA(s) being incorporated into the Supply Arrangement. Any terms or conditions that are purported to be incorporated by reference through URLs, read me files or otherwise form no part of the Supply Arrangement unless such terms are presented in full and included at Annex D – SaaS Service Level Agreements (SLA).

No terms purporting to abridge or extend the time to commence an action for breach, tort, or other action are of any effect.

Annex E – SaaS Bid Solicitation Template

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

This bid solicitation is issued against the GC SaaS Supply Arrangement with the PSPC file number XXX. All terms and conditions of the Supply Arrangement apply to and form part of this Bid Solicitation and any Resulting Contract.

The bid solicitation is divided into six parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided; and

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders.

1.2 Summary

Insert a brief description of the requirement. The description should include enough information for suppliers to decide whether to respond to the bid solicitation. For consistency, use the same wording to describe the requirement in the Notice of Proposed Procurement (NPP).

1.2.1 Description…

Include the following sentence if the requirement is subject to all trade agreements noted in the clause, otherwise modify this article accordingly.

1.2.2 The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), and the Canadian Free Trade Agreement (CFTA).

Include the following sentence for requirements that have been set aside under the federal government Procurement Strategy for Aboriginal Business (PSAB).

1.2.3 This procurement is set aside from the international trade agreements under the provision each has for measures with respect to Aboriginal peoples or for set-asides for small and minority businesses.

*Include the following sentence for requirements issued on behalf of a Department or Agency subject to the FCP, estimated at **$1,000,000 and above**, options excluded and Applicable Taxes included.*

1.2.4 The Federal Contractors Program (FCP) for employment equity applies to this procurement; refer to Part 5 – Certifications.

Include the following sentence to inform bidders that the epost Connect service is available as an electronic delivery method for submitting bids. The contracting officers must ensure that the Bid Receiving Unit email, address and fax number are included correctly within the solicitation.

1.2.5 This bid solicitation allows bidders to use the epost Connect service provided by Canada Post Corporation to transmit their bid electronically. Bidders must refer to Part 2 entitled Bidder Instructions, and Part 3 entitled Bid Preparation Instructions, of the bid solicitation, for further information.

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

1.4 Contracting Authority

Name:
Title:
Address:
Telephone:
E-mail:

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

The 2003 standard instructions is amended as follows:

- Section 08, entitled Transmission by facsimile or by epost Connect, is amended as follows: subsection 2. is deleted entirely and replaced with the following:

2. epost Connect

a. Unless specified otherwise in the bid solicitation, bids may be submitted by using the epost Connect service provided by Canada Post Corporation.

   i. PSPC, National Capital Region: The only acceptable email address to use with epost Connect for responses to bid solicitations issued by PSPC headquarters is:

   tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

   or, if applicable, the email address identified in the bid solicitation.

   ii. PSPC regional offices: The only acceptable email address to use with epost Connect for responses to bid solicitations issued by PSPC regional offices is identified in the bid solicitation.

b. To submit a bid using epost Connect service, the Bidder must either:

   i. send directly its bid only to the specified PSPC Bid Receiving Unit, using its own licensing agreement for epost Connect provided by Canada Post Corporation; or

   ii. send as early as possible, and in any case, at least six business days prior to the solicitation closing date and time, (in order to ensure a response), an email that includes the bid solicitation number to the specified PSPC Bid Receiving Unit requesting to open an epost Connect conversation. Requests to open an epost Connect conversation received after that time may not be answered.

c. If the Bidder sends an email requesting epost Connect service to the specified Bid Receiving Unit in the bid solicitation, an officer of the Bid Receiving Unit will then initiate an epost Connect conversation. The epost Connect conversation will create an email notification from Canada Post Corporation prompting the Bidder to access and action the message within the conversation. The Bidder will then be able to transmit its bid afterward at any time prior to the solicitation closing date and time.

d. If the Bidder is using its own licensing agreement to send its bid, the Bidder must keep the epost Connect conversation open until at least 30 business days after the solicitation closing date and time.

e. The bid solicitation number should be identified in the epost Connect message field of all electronic transfers.

f. It should be noted that the use of epost Connect service requires a Canadian mailing address. Should a bidder not have a Canadian mailing address, they may use the Bid Receiving Unit address specified in the solicitation in order to register for the epost Connect service.

g. For bids transmitted by epost Connect service, Canada will not be responsible for any failure attributable to the transmission or receipt of the bid including, but not limited to, the following:

i. receipt of a garbled, corrupted or incomplete bid;
ii. availability or condition of the epost Connect service;
iii. incompatibility between the sending and receiving equipment;
iv. delay in transmission or receipt of the bid;
v. failure of the Bidder to properly identify the bid;
vi. illegibility of the bid;
vii. security of bid data; or,
viii. inability to create an electronic conversation through the epost Connect service.

h. The Bid Receiving Unit will send an acknowledgement of the receipt of bid document(s) via the epost Connect conversation, regardless of whether the conversation was initiated by the supplier using its own license or the Bid Receiving Unit. This acknowledgement will confirm only the receipt of bid document(s) and will not confirm if the attachments may be opened nor if the content is readable.

i. Bidders must ensure that that they are using the correct email address for the Bid Receiving Unit when initiating a conversation in epost Connect or communicating with the Bid Receiving Unit and should not rely on the accuracy of copying and pasting the email address into the epost Connect system.

j. A bid transmitted by epost Connect service constitutes the formal bid of the Bidder and must be submitted in accordance with section 05.

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 _____ (*insert date*) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 3.a) of Section 01, Integrity Provisions - Bid of Standard Instructions 2003 incorporated by reference above is deleted in its entirety and replaced with the following:

a. at the time of submitting an arrangement under the Request for Supply Arrangements (RFSA), the Bidder has already provided a list of names, as requested under the *Ineligibility and Suspension Policy.* During this procurement process, the Bidder must immediately inform Canada in writing of any changes affecting the list of names.

Include the following modification to Standard Instructions 2003 when requiring bids to remain valid for more than 60 days. Insert the number of days the bid is to remain valid:

Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days

Insert: _____ days

2.2 Submission of Bids

Sections 05 to 10 of Standard Instructions 2003 provide additional instructions and guidance to Bidders on the submission of bids. Review these sections before adding additional clauses to ensure there is no duplication or contradictory information.

Include the following paragraph if the BRU address, BRU facsimile and BRU email address required for delivery and/or transmission of bids are provided on page 1 of the bid solicitation.

"Bids must be submitted only to Public Services Procurement Canada (PSPC) Bid Receiving Unit by the date, time and place indicated in the bid solicitation.

Note: For bidders choosing to submit using epost Connect for bids closing at the Bid Receiving Unit in the National Capital Region (NCR) the email address is:

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Note: Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

Or

Include the following paragraph if the BRU address, BRU facsimile and BRU email address required for delivery and/or transmission of bids are not provided on page 1 of the bid solicitation.

"Bids must be submitted only to the Public Services Procurement Canada (PSPC) Bid Receiving Unit specified below by the date and time indicated on page 1 of the bid solicitation:

_____ *(BRU identification)*

_____ *(physical delivery address)*

_____ *(city, province, postal code)*

_____ *(enter email address for epost Connect service)*

Note: Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

Due to the nature of the bid solicitation, bids transmitted by facsimile to PSPC will not be accepted.

2.3 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than _____ (*insert number of days*) calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as “proprietary” will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.4 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____ (*insert the name of the province or territory).*

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.

2.5 Improvement of Requirement during Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least _____ days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

a) If the Bidder chooses to submit its bid electronically, Canada requests that the Bidder submits its bid in accordance with section 08 of the 2003 standard instructions. The epost Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation.

The bid must be gathered per section and separated as follows:

Section I: Technical Bid

Section II: Financial Bid

Section III: Certifications

b) If the Bidder chooses to submit its bid on electronic media, Canada requests that the Bidder submits its bid in separately bound sections as follows:

Section I: Technical Bid (_____*soft copies on USB keys);*

Section II: Financial Bid (_____*soft copies on USB keys);*

Section III: Certifications (_____*soft copies on USB keys).*

c) If the Bidder is simultaneously providing copies of its bid using multiple acceptable delivery methods, and if there is a discrepancy between the wording of any of these copies and the electronic copy provided through epost Connect service, the wording of the electronic copy provided through epost Connect service will have priority over the wording of the other copies.

d) Due to the nature of the bid solicitation, bids transmitted in hard copies or by facsimile will not be accepted.

e) Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid. The Technical Bid and the Certifications may be included on the same USB Key.

Section I: Technical Bid

In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability _____ (*insert, if applicable:* "and describe their approach") in a thorough, concise and clear manner for carrying out the work.

The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

Section II: Financial Bid

3.1.1 Bidders must submit their financial bid in accordance with the Basis of Payment in Annex "X".

3.1.2 Electronic Payment of Invoices – Bid

If you are willing to accept payment of invoices by Electronic Payment Instruments, complete Annex "X" Electronic Payment Instruments, to identify which ones are accepted.

If Annex "X" Electronic Payment Instruments is not completed, it will be considered as if Electronic Payment Instruments are not being accepted for payment of invoices.

Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

3.1.3 Exchange Rate Fluctuation

The requirement does not offer exchange rate fluctuation risk mitigation. Requests for exchange rate fluctuation risk mitigation will not be considered. All bids including such provision will render the bid non-responsive.

3.1.4 Financial Capability

SACC Manual clause A9033T _____ (*insert date*) Financial Capability.

Section III: Certifications

Bidders must submit the certifications and additional information required under Part 5.

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria.

(b) An evaluation team composed of representatives of Canada will evaluate the bids.

4.1.1 Technical Evaluation

Mandatory *(and point rated, if applicable)* technical evaluation criteria are included in Annex ____.

4.1.2 Financial Evaluation

The price of the bid will be evaluated in Canadian dollars, Applicable Taxes excluded, FOB destination, Canadian customs duties and excise taxes included.

4.2 Basis of Selection

Select the appropriate option for the basis of selection depending on the mandatory and/or point-rated criteria being evaluated.

OPTION 1 – SIMPLE REQUIREMENTS

Use the following clause when the bid solicitation contains mandatory technical evaluation criteria only and the basis of selection will be the responsive bid with the lowest evaluated price.

4.2.1 Mandatory Technical Criteria

(a) A bid must comply with the requirements of the bid solicitation and meet all mandatory technical evaluation criteria to be declared responsive.

(b) The responsive bid with the lowest evaluated price will be recommended for award of a contract.

OPTION 2 – COMPLEX REQUIREMENTS

Use the following clause when the bid solicitation contains mandatory and point-rated technical evaluation criteria, and the basis of selection will be the responsive bid with the highest combined rating of technical merit and price.

4.2.1 Highest Combined Rating of Technical Merit and Price

(a) To be declared responsive, a bid must:

(i) comply with all the requirements of the bid solicitation; and

(ii) meet all mandatory technical evaluation criteria; and

(iii) obtain the required minimum of ____ (*insert minimum number of points*) points overall for the technical evaluation criteria which are subject to point rating. The rating is performed on a scale of ____ (*insert total number of available points*) points.

(b) Bids not meeting (i) or (ii) or (iii) will be declared non-responsive.

(c) The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be ____ % (*insert the percentage for technical merit*) for the technical merit and ____ % (*insert the percentage for price*) for the price.

(d) To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of ____ % (*insert the percentage for technical merit*).

(e) To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of ____ % (*insert the percentage for price*).

(f) For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

(g) Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

PART 5 – CERTIFICATIONS

Bidders must provide the required certifications to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Bid

Bidders must submit the following duly completed certifications as part of their bid.

5.1.1 Set-aside for Aboriginal Business

If the requirement has been set aside under the federal government Procurement Strategy for Aboriginal Business, insert SACC Manual clauses A3000T *and* A3001T *in full text, and if applicable,* A3002T.

5.2 Certifications Precedent to Contract Award

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.2.1 Federal Contractors Program for Employment Equity - Bid Certification

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list available at the bottom of the page of the Employment and Social Development Canada (ESDC) - Labour's website (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html#).

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid list at the time of contract award.

Insert the following paragraphs for requirements issued on behalf of a Department or Agency subject to the FCP, estimated at ***$1,000,000 and above****, options excluded and Applicable Taxes included: (consult* Annex 5.1 *of the Supply Manual)*

Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list during the period of the Contract.

The Bidder must provide the Contracting Authority with a completed annex titled Federal Contractors Program for Employment Equity - Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

ANNEX "X" - STATEMENT OF REQUIREMENT

(*insert if applicable*)

ANNEX "X" - BASIS OF PAYMENT

(*insert if applicable*)

ANNEX "X" - SECURITY REQUIREMENTS CHECK LIST

(*insert if applicable*)

ANNEX "X" - ELECTRONIC PAYMENT INSTRUMENTS

(*insert if applicable*)

As indicated in Part 3, clause 3.1.2, the Bidder must complete the information requested below, to identify which electronic payment instruments are accepted for the payment of invoices.

The Bidder accepts to be paid by any of the following Electronic Payment Instrument(s):

( ) VISA Acquisition Card;

( ) MasterCard Acquisition Card;

( ) Direct Deposit (Domestic and International);

( ) Electronic Data Interchange (EDI);

( ) Wire Transfer (International Only);

( ) Large Value Transfer System (LVTS) (Over $25M)

ANNEX "X" - FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY – CERTIFICATION (*insert if applicable*)

*Insert the following certification for requirements issued on behalf of a Department or Agency subject to the FCP, estimated at **$1,000,000 and above**, options excluded and Applicable Taxes included: (consult Annex 5.1 of the Supply Manual) (Refer also to Part 5 - Certifications and Additional Information)*

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit Employment and Social Development Canada (ESDC) – Labour's website.

Date:_____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the Employment Equity Act.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 permanent full-time and/or permanent part-time employees.

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1. The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with ESDC-Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions).

Annex F - Resulting Contract Clauses

(See Attached)

Annex G – Supply Chain Integrity Process

Supply Chain Integrity Process

1. Mandatory Requirements

1.1. Suppliers must submit, with their Submission, the following SCSI:

1.2.1 **IT Product List**: Suppliers must identify the SaaS Solutions over which Canada's Data would be transmitted and/or stored that will be used and/or installed to perform any part of the Work and/or Services described in the resulting contract, in regards to each SaaS Solution, by completing the Form 6-SCI Submission Template as provided in the RFSA, which includes following information :

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

b) **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 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.

c) **Product Name:** Enter the OEM's name for the product.

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

e) **Product URL:** Enter the URL of the OEM's webpage for the product.

f) **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 Vulnerability Information field, and include the filename(s) in the additional information column which provide the required vulnerability information.

1.2.2 **Ownership Information:** Suppliers must identify the original equipment manufacturer (OEM) of the product(s) or service(s) ordered, as well as the name of any supplier (i.e. sub-contractors (individuals or companies), sub-contractors of sub-contractors (individuals or companies) down the chain, re-seller, distributor, sub-processors, etc.) of the product(s) or service(s) that are being ordered.

This list must identify all third parties who may perform any part of the Work, whether they would be subcontractors to the Supplier, or subcontractors to subcontractors of the Supplier down the chain. Any subcontractor that could have access to Canada's Data must be identified. For the purposes of this requirement, a third party who is merely a supplier of goods to the Supplier, but who does not perform any portion of the Work, is not considered to be a subcontractor. Subcontractors would include, for example, technicians who might be deployed or maintain the Supplier's solution. If the Supplier does not plan to use any subcontractors to perform any part of the Work, the Supplier is requested to indicate this in its response.

Suppliers are requested to provide their information on form [insert]. It is requested that Suppliers indicate their legal name on each page, insert a page number as well as the total

number of pages. Suppliers are also requested to insert a separate row for each subcontractor and additional rows as may be necessary.

For each of these entities listed, provide either:

a) **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 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, 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.

b) **Country / Nationality**: The country which an individual listed has their primary nationality or the country in which a corporate entity is registered.

c) **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.

1.2.3 **Network Diagrams:** one or more conceptual network diagrams that collectively show the complete network proposed to be used to deliver the services described in the draft Statement of Work. The network diagrams are only required to include portions of the Suppliers's network (and its subcontractor' network(s)) over which Canada's Data, would be transmitted in performing any resulting contract. As a minimum the diagram must show:

a) The following key nodes for the delivery of the services under the resulting contract of this solicitation process, if applicable the role of the Supplier or subcontractor;

i. Service delivery points;

ii. Core network

iii. Subcontractor network (specifying the name of the subcontractor as listed in the **Ownership Information**);

b) The node interconnections, if applicable

c) Any node connections with the Internet; and

d) For each node, a cross-reference to the product that will be deployed within that node, using the Excel row number from the IT Product List.

2. Assessment of Supply Chain Security Information

2.1 Canada will assess whether, in its opinion, the Supply Chain Security Information creates the possibility that the Supplier's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.

2.2 In conducting its assessment:

(a) Canada may request from the Supplier any additional information that Canada requires to conduct a complete security assessment of the Supply Chain Security Information. The Supplier will have 2 working days (or a longer period if specified in writing by the Supply Chain Security Authority) to provide the necessary

information to Canada. Failure to meet this deadline will result in the response being disqualified.

(b) Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is included in the response or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of the Supply Chain Security Information.

2.3 If, in Canada's opinion, any aspect of the Supply Chain Security Information, if used in a solution, creates the possibility that the Supplier's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information:

(a) Canada will notify the Supplier in writing (sent by email) and identify which aspect(s) of the Supply Chain Security Information is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Supplier regarding its concerns will be determined based on the nature of the concerns. In some situations, for reasons of national security, it may not be possible for Canada to provide further information to the Supplier; therefore, in some circumstances, the Supplier will not know the underlying reasons for Canada's concerns with respect to a product, subcontractor or other aspect of the Supplier's Supply Chain Security Information.

(b) The notice will provide the Supplier with one opportunity to submit revised Supply Chain Security Information within the 10 calendar days following the day on which Canada's written notification is sent to the Supplier, (or a longer period specified in writing by the Supply Chain Security Authority).

(c) If the Supplier submits revised Supply Chain Security Information within the allotted time, Canada will perform a second assessment. If Canada determines that any aspect of the Supplier's revised Supply Chain Security Information could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, no further opportunities to revise the Supply Chain Security Information will be provided and the response will be disqualified.

2.4 By participating in this process, the Supplier acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. Also, the Supplier acknowledges that Canada's security assessment does not involve the assessment of a proposed solution. As a result:

(a) qualification pursuant to this RFSA does not constitute an approval that the products or other information included as part of the Supply Chain Security Information will meet the requirements of the subsequent bid solicitation or any resulting contract or other instrument that may be awarded as a result of any subsequent bid solicitation;

(b) qualification pursuant to this RFSA does not mean that the same or similar Supply Chain Security Information will be assessed in the same way for future requirements;

(c) at any time during the subsequent bid solicitation process, Canada may advise a Supplier that some aspect(s) of its Supply Chain Security Information has become the subject of security concerns. At that point, Canada will notify the Respondent and provide the Supplier with an opportunity to revise its Supply Chain Security Information, using the same process described above.

(d) during the performance of a subsequent contract, if Canada has concerns regarding certain products, designs or subcontractors originally included in the

Supply Chain Security Information, the terms and conditions of that contract will govern the process for addressing those concerns.

2.5 All Suppliers will be notified in writing regarding whether or not they have qualified under this RFSA to proceed to the next stage of the procurement process.

2.6 Any Supplier that has qualified under this RFSA will be required, when responding to any subsequent bid solicitation under this solicitation process, to propose a solution consistent with the final version of the Supply Chain Security Information it submitted with its response to this RFSA (subject to revision only pursuant to the paragraph below). Except pursuant to the paragraph below, no alternative or additional Products or subcontractors may be proposed in the Supplier's solution. This is a mandatory requirement of this solicitation process. The proposed solution during any subsequent bid solicitation does not need to contain all the Products within the final Supply Chain Security Information.

2.7 Once a Supplier has been qualified in response to this RFSA, no modifications are permitted to the Supply Chain Security Information except under exceptional circumstances, as determined by Canada. Given that not all the exceptional circumstances can be foreseen, whether changes may be made and the process governing those changes will be determined by Canada on a case-by-case basis.

Annex H – Non-Disclosure Agreement related to Supply Chain Integrity

Non-Disclosure Agreement

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.

FORMS

FORM 1 – REQUEST FOR SUPPLY ARRANGEMENT SUBMISSION FORM		
Supplier's full legal name		
Authorized Representative of Supplier for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Supplier's Procurement Business Number (PBN) [*See the Standard Instructions 2008*]		
List of the Board of Directors Member *[Suppliers are requested to indicate the name(s) of all of the Board of Director member(s) in its Company.]*	Name: Name: Name: ...	
Jurisdiction of Contract Province in Canada the Supplier wishes to be the legal jurisdiction applicable to the Supply Arrangement and to any resulting Contracts (if other than the province of Ontario (Canada).		
Number of FTEs *[Suppliers are requested to indicate, the total number of full-time-equivalent positions that would be created and maintained by the Supplier as a result of its participation within this procurement vehicle. This information is for information purposes only and will not be evaluated.]*		
Security Clearance Level of Supplier *[Suppliers are requested to include both the level and the date it was granted.]*		
Aboriginal Businesses *[Suppliers are requested to indicated if they meet the requirements as outlined in Set-Asides Program for Aboriginal Businesses (SPAB).]*		
Canadian Small and Medium Enterprises (CSME) *[Suppliers are requested to indicated if they meet the definition of a Canadian Small and Medium Enterprise (OSME indication: 100 to 500 Employees = Medium; 10 to 100 = Small; 1 to 10 = Micro).]*		
Canadian Enterprise *[Suppliers are requested to indicated if they are Canadian Suppliers.]*		
Green Procurement *[Suppliers must commit to providing delivery of all goods in an environmentally friendly manner.]*		
Green Company *[Suppliers are requested to identify if their facilities operate with an Environmental Management System (EMS) certified by a qualified registrar as complying with the ISO 14001 standard.]*		
Supplier Certification that all SaaS Solutions are Commercial [Suppliers are requested to certify that all proposed SaaS Solutions in response to this RFSA are Commercial Solutions, meaning that each software component is commercially available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any of the SaaS Solution proposed is a fully compatible extension of a field-proven product line, it must have been publicly announced on or before the date that the Submission is submitted. By submitting a Submission, the Supplier is certifying that all the SaaS Solutions proposed are Commercial Solutions.]		

On behalf of the Supplier, by signing below, I confirm that I have read the entire Request for Supply Arrangement including the documents incorporated by reference and I certify that: 1. The Supplier considers itself and its products able to meet all the mandatory requirements described in the RFSA; 2. All the information provided in response to the RFSA is complete, true and accurate; and 3. If the Supplier enters into a Supply Arrangement with Canada and if it is awarded Contracts, it will accept all the terms and conditions set out in the resulting Contract clauses included in the RFSA.	
Signature of Authorized Representative of Supplier	

Form 2

SaaS Publisher Certification Form

(to be used where the Supplier itself is the SaaS Publisher)

The Supplier certifies that it is the SaaS Publisher of all the following SaaS Solutions and that it has all the rights necessary to license them in accordance with the terms and conditions of the SA to Canada:

_____

_____

_____

_____

_____

[Suppliers should add or remove lines as needed, or attach the product list as an appendix.]

Name of SaaS Publisher _____

Signature of authorized signatory of SaaS Publisher

_____

Print Name of authorized signatory of SaaS Publisher

_____

Print Title of authorized signatory of SaaS Publisher

_____

Address for authorized signatory of SaaS Publisher

_____

Telephone no. for authorized signatory of SaaS Publisher

_____

Email for authorized signatory of SaaS Publisher _____

Date signed _____

RFSA Number _____

Form 3

SaaS Publisher Authorization Form

(to be used where the Supplier is not the SaaS Publisher)

This confirms that the SaaS Publisher identified below understands and acknowledges that the Supplier named below has submitted a Submission in response to the Request for Supply Arrangement dated _____, reference number _____ issued by PSPC.

The SaaS Publisher hereby confirms that

(i) The Supplier named below is authorized to supply the SaaS Publisher listed below or attached, through its SA; and
(ii) The SaaS Publisher agrees to grant all licenses to be acquired under the SA in accordance with the resulting Contract's terms and conditions set out in the SA.

The SaaS Publisher acknowledges that the reseller has proposed to the Crown, in response to the RFSA, the following SaaS Solutions and other proprietary products of the Corporation.

[*Identify all of the proprietary SaaS Solutions that are proposed by the Supplier*]

_____

_____

_____

_____

[*Suppliers should add or remove lines as needed,* or attach the product list as an appendix.]

Name of Supplier _____

Name of SaaS Publisher _____

Signature of authorized signatory of SaaS Publisher

_____

Print Name of authorized signatory of SaaS Publisher

_____

Print Title of authorized signatory of SaaS Publisher

_____

Address for authorized signatory of SaaS Publisher

_____

Telephone no. for authorized signatory of SaaS Publisher

_____

Email for authorized signatory of SaaS Publisher _____

Date signed _____

RFSA Number _____

Form 4

Certification Requirements for the Set-Aside Program for Aboriginal Business

The Supplier:
(i) certifies that it meets, and will continue to meet throughout the duration of the Supply Arrangement, the requirements described in Annex 9.4 Requirements for the Set-aside Program for Aboriginal Business, of the Supply Manual (https://buyandsell.gc.ca).
(ii) agrees that any subcontractor it engages under the Supply Arrangement must satisfy the requirements described in the above-mentioned annex.
(iii) agrees to provide to Canada, immediately upon request, evidence supporting any subcontractor's compliance with the requirements described in the above-mentioned annex.

The Supplier must check the applicable box below:
( ) The Supplier is an Aboriginal business that is a sole proprietorship, band, limited company, co-operative, partnership or not-for-profit organization.
OR
( ) The Supplier is either a joint venture consisting of two or more Aboriginal businesses or a joint venture between an Aboriginal business and a non-Aboriginal business.*

The Supplier must check the applicable box below:
( ) The Aboriginal business has fewer than six full-time employees.
OR
( ) The Aboriginal business has six or more full-time employees.

The Supplier must, upon request by Canada, provide all information and evidence supporting this certification. The Supplier must ensure that this evidence will be available for audit during normal business hours by a representative of Canada, who may make copies and take extracts from the evidence. The Supplier must provide all reasonably required facilities for any audits.

By submitting a Submission, the Supplier certifies that the information submitted by the Supplier in response to the above requirements is accurate and complete.

Name of Supplier _____

Signature of authorized signatory of Supplier _____

Print Name of authorized signatory of Supplier _____

Print Title of authorized signatory of Supplier _____

Address for authorized signatory of Supplier _____

Email for authorized signatory of Supplier _____

Date signed _____

RFSA Number _____

*** Aboriginal Joint Venture**: a joint venture consisting of two or more Aboriginal businesses or Aboriginal business(es) and a non-Aboriginal business(es), provided that the Aboriginal business(es) has at least 51 percent ownership and control of the joint venture. The joint venture has to respect the Aboriginal content requirement of 33% of the value of the work under a Contract has to be performed by the Aboriginal business(es).

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 Information

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 B – Security & Privacy Obligations ☐

Annex C - SaaS Solutions and Ceiling Prices ☐

- *a)* ☐ Must be submitted using the format outlined in Annex C
- *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** *(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) ☐ Hours of support; PAGE # _____

b) ☐ Contact and procedure information for accessing Support; PAGE # _____

c) ☐ Procedures for resolution of problems; PAGE # _____

d) ☐ Submission times; PAGE # _____

e) ☐ Procedures on how and when all telephone, fax or email communications will be responded to; PAGE # _____

f) ☐ Support web site availability to Canada's users (ex: 24 hours a day, 365 days a year, and 99% of the time). PAGE # _____

g) ☐ Maintenance entitlements (e.g. patches, updates, major/minor releases, etc.) PAGE # _____

Annex G - Supply Chain Integrity Process ☐

Name of Authorised Signatory of Supplier: _____

Signature of Authorised Signatory of Supplier: _____

Form 6 - SCI Submission Template
(See attached)

Software as a Service Resulting Contract Clauses

Software as a Service Solution

Resulting Contract Terms

***Note to Suppliers**: These Resulting Contract Clauses are intended to form the basis of any contract(s) resulting from the RFSA. Except where specifically set out in these Resulting Contract Clauses, acceptance by Suppliers of all the clauses is a mandatory requirement of this RFSA.*

No modification or other terms and conditions included in the Submission will apply to any resulting contract, despite the fact that the Submission may become part of the resulting contract.

Any Supplier providing a Submission containing statements implying that the Submission is conditional on modification of these Resulting Contract Clauses (including all documents incorporated by reference) or containing terms and conditions that purport to supersede these Resulting Contract Clauses will be considered non-responsive. As a result, Suppliers with concerns regarding the provisions of these Resulting Contract Clauses should raise those concerns in accordance with the RFSA.

If additional legal issues are raised by a Submission, Canada reserves the right to address those issues in any contract awarded as a result of this RFSA. If the additional provisions are unacceptable to the Supplier, the Supplier may withdraw its Submission.

This Contract is made on [CONTRACT DATE] between [CONTRACTOR NAME] (the "Contractor") and [GOVERNMENT OF CANADA ENTITY] ("Canada").

This Contract is issued in accordance with Supply Arrangement (SA) [SA number on page 1]. The Terms and Conditions set out in the SA form part of this Contract.

1. Requirement

1.1 The Contractor agrees to provide the Services and perform the Work described in the Contract in accordance with and at the prices set out in the Supply Arrangement, Annex C – SaaS Solution(s) and Ceiling Prices, or in the Contractor's bid, as applicable.

1.2 Services. The Contractor agrees to provide the following Services:

a) providing the Services identified in Appendix A, which includes, at a minimum:

i) granting usage rights to the Software as a Service (SaaS) Solutions ("Solution(s)") identified in Appendix A provided by or hosted by the Contractor;

ii) providing Solution Documentation;

iii) maintaining, upgrading, and updating the Solution(s);

iv) managing incidents and defects to ensure the Solution(s) operate at the applicable service levels; and

v) providing incidental and additionally required information technology infrastructure services.

vi) infrastructure services required to deliver the Solution.

1.3 Professional Services. The Contractor agrees to provide the following Professional Services, as and when requested by Canada, using the Task Authorization process:

i) Quick Start Guide ("QSG") training and services package;

ii) implementation services;

iii) training services;

iv) data cleansing, migration and transition services; and

v) advisory services.

1.4 Client. Under the Contract, the "Client" is _____.

1.5 Reorganization of Clients. The Contractor's obligation to provide the Services and perform the Work will not be affected by (and no additional fees will be payable as a result of) any form of reorganization or restructuring of any Client. Canada may designate replacement Contracting Authority or Technical Authority.

2. Term, Termination and Auto Renewal

NOTE: This Article will be adjusted at Contract award to include either the Fixed Term or Subscription Term clauses, as applicable to the commercial terms submitted by the Contractor in the applicable Annex D, Service Level Agreement or the winning bid.

2.1 Contract Period. The Contract Period includes the entire period of time during which the Contractor is obliged to provide the Services and perform the Work.

2.2 Initial Term. This Contract begins on the date the Contract is awarded and ends on [TERM expiry DATE/ # of years].

2.3 Option Periods. The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to [Number of extensions] [Period of extensions]-periods under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment. Canada may exercise the option(s) at any time by sending a written notice to the Contractor at least 90 calendar days before the expiry date of the Contract. The option may be exercised only by the Contracting Authority, and will be evidenced, for administrative purposes only, through an amendment to the Contract.

2.4 Auto-Renewal Opt Out. Canada hereby provides notice to the Contractor that it opts out of any auto-renewal of the term obligation. The Contractor acknowledges receipt of the notice, and represents that this Contract will be valid only until the end of the Contract Period, as defined above.

OR

2.1 Subscription Term

a) **Subscription Services.** Canada acknowledges that the Contractor will deliver the Services on a subscription basis without a prescribed Contract Period. Canada further understands that even if a defined Contract Period is identified, that the Contractor's commercial offering may provide for an automatic renewal of the subscription services.

b) **Metrics.** The Contractor agrees to provide Canada with access to the Solution on a subscription basis, all at the prices set out in the Supply Arrangement, Annex C – SaaS Solutions and Ceiling Prices, or in the Contractor's bid, as applicable.

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.

3. Solution

3.1 Software as a Service. The Contractor will deliver the Solution through a Software as a Service ("SaaS") delivery model, allowing Canada to access and use the Solution which is hosted by the Contractor.

3.2 Commercially-Available Solution. Canada acknowledges that the Solution is a commercially-available solution provided to other customers. As part of the subscription to use the Solution, the Contractor agrees to make available to Canada all the features and functionalities included in the commercially available version of the Solution, and the incidental and required information technology infrastructure services required to deliver the Solution, all of which is included in the subscription price.

3.3 Software Application Evolution; Features or Functionalities. Canada acknowledges that the Solution, underlying software application or associated infrastructure may evolve during the course of the Contract Period. The Contractor agrees to continue to provide the Services as the commercially available Solution, with functionality or features and on with terms that are no less favourable than as at the time of Contract award.

3.4 Improvements to and Evolution of the Solution. The parties acknowledge that technology and business models evolve quickly and that any Solution provided at the beginning of the Contract Period inevitably will be different from the Solution provided at the end of the Contract Period and the method(s) by which the Solution and any potential peripherals are delivered to Canada are likely to change or evolve and that, at the time of entering into this Contract, the parties cannot possibly contemplate all the goods or services that may be delivered under this Contract, other than they will be connected to delivering to Users. With that in mind, the parties agree that:

a) The Contractor must maintain and continuously improve the Solution and infrastructure throughout the Contract Period on a commercially reasonable basis, and must provide those improvements and enhancements to Canada as part of Canada's subscription, with no price adjustment if those improvements and enhancements are also offered to other customers at no additional cost.

b) If the Contractor removes any functions from the commercial offering to the Solution and offers those functions in any new or other services or products, the Contractor must continue to provide those functions to Canada as part of Canada's subscription to the Services, under the existing terms and conditions of the Contract regardless of whether those other services or products also contain new or additional functions. Contractor has no obligation to comply with this paragraph if the Solution acquired by Canada is still offered by Contractor in parallel with the new services offered to other customers.

3.5 Downgrade. If the Contractor is unable to provide the Services with no less favourable features and functionality, the Contractor will provide written Notice to Canada identifying the circumstance, and alternative options, specifically including a reduction in pricing. If no proposed alternative option is acceptable to Canada, the Contractor agrees to consent to a termination of the Contract, and pay all identifiable direct costs incurred by Canada to migrate and store Client's Data, and to procure equivalent replacement services.

4. Services

4.1 Solution Services

a) **Software as a Service.** The Contractor will provide all Services required for Canada to access and use the Solution as specified in Appendix A.

b) **Authority.** The Contractor represents and warrants that it owns or has obtained and will maintain throughout the Contract Period, all necessary authority specifically including intellectual property rights required to provide the Services in accordance with the terms of this Contract.

c) **Indemnification.** The Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any intellectual property infringement claim by a third party based on Canada's use of the Solution.

d) **Accessibility:** The Contractor must ensure that the Solution does not interfere with accessibility standards compliance, as specified in the Standard on Web Accessibility: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601#

e) **Usage Grant**. The Contractor grants to Canada the non-exclusive, non-assignable right to access and use the Solution from an unlimited number of locations, devices and operating environments, through secure, wireless, mobile or other connection, via the internet, a web browser or other access connection technology which may become available.

f) **Included.** The Contractor represents and warrants that the Services include

i) hosting and maintenance of the Solution,

ii) provision of all incidental and additional required information technology infrastructure services, in compliance with all required security standards,

iii) the technical infrastructure that complies with all required security standards, allowing Canada to use the Solution to process any of Client's Data in compliance with its expressed security standards, and

iv) unfettered access and use by the Client, regardless of the amount of data created, processed or stored by the Solution,

all of which is included in the price.

g) **Restricted Usage Rights.** Canada acknowledges that in providing the Services, the Contractor is not delivering ownership rights to any software product, component of the Solution or infrastructure used by the Contractor to provide the Services, except as expressly provided in a Task Authorization. Canada will not knowingly:

i) distribute, license, loan, or sell the Solution;

ii) impair or circumvent the Solution's security mechanisms; or

iii) remove, alter, or obscure any copyright, trademark, or other proprietary rights notice on or in the Solution.

h) **Applicable Terms and Conditions**. The Contractor has advised and Canada acknowledges that the Contractor may unilaterally modify the terms under which it provides its commercial offering of the Solution, without notice to its customers, including Canada. The Contactor represents and warrants that any such modification will not result in less favourable terms, specifically including price, service levels and remedies, regardless of any notification to the contrary.

i) **Additional Terms and Conditions.** The parties agree that any terms and conditions, including any "click-through" or "pop-up" notices, that apply to the Contractor's commercial offering of the Solution, including third party tools or incidental infrastructure, will not apply to Canada's use of the Solution if those terms conflict with the express terms of this Contract. The terms and conditions of third party tools not specified as a Service or Solution in Appendix A are not subject to this section.

j) **Commercial SaaS Offering.** Canada acknowledges that it will accept the Contractor's commercial SaaS offering, and states that, unless explicitly identified as Work or Services to be delivered under this Contract, Canada does not require custom development, alternative services, service levels, functionalities or features.

5. Service Levels

Annex D, Service Level Agreement **contains the specific information defining the levels and standards for processes and performance expectations for the Services to be delivered under the Contract, and must be read in conjunction with the following section.**

5.1 Availability. The Contractor will make the Service available to Canada in strict compliance with Solution Documentation and Annex D, Service Level Agreement.

5.2 Service Credits. The Contractor will provide the applicable Service Credits to Canada for failing to achieve the uptime Solution Availability levels as defined in Annex D, Service Level Agreement.

5.3 Exclusions. The Contractor will expressly specify any exclusions to the Solution Availability levels identified in Annex D, Service Level Agreement.

5.4 Support Services. The Contractor will provide technical support assistance in strict compliance with Annex D, Service Level Agreement.

5.5 Escalation. The Contractor will provide an escalation process for dispute resolution, which is identified in Annex D, Service Level Agreement.

5.6 No Infringement. The Contractor warrants that nothing in the Solution, or in Canada's use of the Solution, will infringe or constitute a misappropriation of the intellectual property or other rights of a third party.

6. Documentation

6.1 Solution Documentation. The Contractor must provide or deliver access to the commercially available Solution Documentation to Canada upon Contract Award. The Contractor must update Solution Documentation on a commercially reasonable basis**.**

6.2 Other Documentation. The Contractor must provide or deliver access to any documentation required in performance of the Work.

6.3 Translation Rights. The Contractor agrees that Canada may translate any written deliverable, including the Solution Documentation or Training Materials into English or French. The Contractor acknowledges that Canada owns any translation and is under no obligation to provide it to the Contractor. Canada will include any copyright and/or proprietary right notice that was part of the original document in any translation. The Contractor will not be responsible for technical errors that arise as a result of any translation made by Canada.

6.4 Moral Rights. At the request of Canada, the Contractor may provide a written permanent waiver of moral rights, in a form acceptable to Canada, from every author that contributed to the written deliverable. If the Contractor is unable or unwilling to obtain the requested waivers, the Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any moral rights infringement claim by a third party based on Canada's translation of written documentation.

6.5 Defective Documentation. If at any time during the Contract Period, Canada advises the Contractor a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor will correct the defect or non-conformance must as soon as possible and at its own expense. Canada may provide the Contractor with information about defects or non-conformance in other documentation, including the Solution Documentation, for information purposes only.

7. Work ((Optional clauses to be used when professional services are required)

7.1 Professional Services

a) **Professional Services.** The Contractor must perform and deliver such Professional Services (the "Work") to Canada as detailed in a Task Authorization.

b) **Conduct of the Work; Warranty.** The Contractor represents and warrants that (a) it is competent to perform the Work, (b) it has everything necessary to perform the Work, including the resources, facilities, labour, technology, equipment, and materials; and (c) it has the necessary qualifications, including knowledge, skill, know-how and experience, to effectively perform the Work.

c) **Time is of the Essence.** It is essential that the Work be delivered within or at the time stated in a Task Authorization.

7.2 Remedies

a) **Work.** If at any time during the Contract Period the Work fails to meet its warranty obligations, the Contractor must as soon as possible correct at its own expense any errors or defects and make any necessary changes to the Work.

b) **Documentation.** If at any time during the Contract Period, Canada discovers a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor must as soon as possible correct at its own expense the defect or non-conformance.

c) **Canada's Right to Remedy.** If the Contractor fails to fulfill any obligation described herein within a reasonable time of receiving a notice, Canada will have the right to remedy or to have remedied the defective or non-conforming Work at the Contractor's expense. If Canada does not wish to correct or replace the defective or non-conforming Work, an equitable reduction will be made in the Contract Price.

7.3 Subcontracts

a) **Conditions to Subcontracting.** The Contractor may subcontract the performance of the Work, provided (a) the Contractor obtains the Contracting Authority's prior written consent, (b) the subcontractor is bound by the terms of this Contract, and (c) the Contractor remains liable to Canada for all the Work performed by the subcontractor.

b) **Exceptions to Subcontracting Consent.** The Contractor is not required to obtain consent for subcontracts specifically authorized in the Contract. The Contractor may also without the consent of the Contracting Authority: (i) purchase "off-the-shelf" items and any standard articles and materials that are ordinarily produced by manufacturers in the normal course of business (ii) subcontract any incidental services that would ordinarily be subcontracted in performing the Work; and (iii) permit its subcontractors at any tier to make purchases or subcontract as permitted in paragraphs (i) and (ii).

7.4 Excusable Delay

a) **No Liability.** The Contractor will not be liable for performance delays nor for non-performance due to causes beyond its reasonable control that could not reasonably have been foreseen or prevented by means reasonably available to the Contractor, provided the Contractor advises the Contracting Authority of the occurrence of the delay or of the likelihood of the delay as soon as the Contractor becomes aware of it (referred to as an "**Excusable Delay"**).

b) **Notice**. The Contractor must also advise the Contracting Authority, within 15 business days, of all the circumstances relating to the delay and provide to the Contracting Authority for approval a clear work around plan explaining in detail the steps that the Contractor proposes to take in order to minimize the impact of the event causing the delay.

c) **Delivery and Due Dates**: Any delivery date or other date that is directly affected by an Excusable Delay will be postponed for a reasonable time that will not exceed the duration of the Excusable Delay.

d) **Canada not responsible for Costs**: Unless Canada has caused the delay by failing to meet an obligation under the Contract, Canada will not be responsible for any costs incurred by the Contractor or any of its subcontractors or agents as a result of an Excusable Delay.

7.5 Right to Terminate. If such an event prevents performance under the Contract for more than 30 calendar days, then the Contracting Authority may elect to terminate the TA, or part or all of this Contract on a "no fault" basis, meaning neither party will be liable to the other in connection with the Excusable Delay or resulting termination, and Canada will only be responsible for paying for those services received up to the effective date of the termination.

7.6 Professional Services: Transition Services

a) **Migration.** The Contractor acknowledges that the nature of the Services provided under the Contract, Canada may require continuity. Prior to the transition to the new contractor or to Canada, the Contactor must provide all operational, technical, design and configuration

information and documentation for all Services required to complete the transition, provided that it is not Contractor confidential information. The Contractor represents and warrants that it will not directly or indirectly interfere with or impede Canada's access to or transfer of Client's Data.

b) **Migration and Transition Services.** The Contractor agrees that, in the period leading up to the end of the Contract Period, if Migration or Transition Services are requested by Canada, it will diligently assist Canada in the transition from the Contract to a new contract with another supplier and or migrate Client's Data to a new supplier environment, that there will be no charge for the services below other than those charges set out in the Basis of Payment.

7.7 Inspection and Acceptance of the Work

a) **Inspection by Canada**: All the Work is subject to inspection and acceptance by Canada. Canada's inspection and acceptance of the Work does not relieve the Contractor of its responsibility for defects or other failures to meet the requirements of the Contract. Canada will have the right to reject any work that is not in accordance with the requirements of the Contract and the Contractor is required to correct or replace it at its own expense.

b) **Acceptance Procedures**: Unless provided otherwise in the Contract, the acceptance procedures are as follows:

i) when the Work is complete, the Contractor must notify the Technical Authority in writing, with a copy to the Contracting Authority, by referring to this provision of the Contract and requesting acceptance of the Work;

ii) Canada will have 30 days from receipt of the notice to perform its inspection (the **"Acceptance Period**").

c) **Deficiencies and Resubmission of Deliverable**: If Canada provides notice of a deficiency during the Acceptance Period, the Contractor must address the deficiency as soon as possible and notify Canada in writing once the Work is complete, at which time Canada will be entitled to re-inspect the Work before acceptance and the Acceptance Period will begin again. If Canada determines that a deliverable is incomplete or deficient, Canada is not required to identify all missing items or all deficiencies before rejecting the deliverable.

d) **Access to Locations**: The Contractor must provide representatives of Canada access to all locations where any part of the Work is being performed, other than multi-tenant data centres, at any time during working hours. Representatives of Canada may make examinations and such tests of the Work as they may think fit. The Contractor must provide all assistance and facilities, test pieces, samples and documentation that the representatives of Canada may reasonably require for the carrying out of the inspection. The Contractor must forward such test pieces and samples to such person or location as Canada specifies.

e) **Contractor Inspection for Quality**: The Contractor must inspect and approve any part of the Work before submitting it for acceptance or delivering it to Canada. All deliverables submitted by the Contractor must be of a professional quality, free of typographical and other errors, and consistent with the highest industry standards.

f) **Inspection Records**: The Contractor must keep accurate and complete inspection records that must be made available to Canada on request. Representatives of Canada may make copies and take extracts of the records during the performance of the Contract and for up to three years after the end of the Contract.

g) **Informal Feedback**: Upon request by the Contractor, Canada may provide informal feedback prior to any deliverable being formally submitted for acceptance. However, this must not be

used as a form of quality control for the Contractor's Work. Canada is not obliged to provide informal feedback.

8. Task Authorization (TA) (Optional clauses to be used when professional services are required)

The Contractor's professional services performed under this Contract will be on an "as and when requested basis" using a Task Authorization.

8.1 Form and Content of TA. A TA will contain (a) Contract and TA number, (b) the details of the required activities and resources, (c) a description of the deliverables, (d) a schedule indicating completion dates for the major activities or submission dates for the deliverables, (e) security requirements, and (f) costs.

8.2 Contractor's Response to TA. The Contractor must provide to Canada, within the period specified in the TA, the proposed total price for performing the task and a breakdown of that cost, established in accordance with the fees. The Contractor will not be paid for preparing or providing its response or for providing other information required to prepare and validly issue the TA.

8.3 TA Limit and Authorities for Validly Issuing TAs. A validly issued TA must be signed by the appropriate Canadian Authority as set forth in this Contract. Any work performed by the Contractor without receiving a validly issued TA is done at the Contractor's own risk.

8.4 P**eriodic Usage Reports.** The Contractor must compile and maintain records on its provision of services to the federal government under the valid TAs issued under this Contract.

8.5 Consolidation of TAs for Administrative Purposes. This Contract may be amended from time to time to reflect all validly issued TAs to date, to document the Work performed under those TAs for administrative purposes.

9. Basis of Payment

NOTE: This Article will be adjusted at Contract award to include the Basis and Method of Payment submitted by the Contractor in the applicable Annex D, Service Level Agreement or the winning bid.

9.1 Subscription. For the Services, including access to and use of the Solution, Solution Documentation, Support Services, and incidental and additionally required information technology infrastructure services (all the Services described in this Contract that is not Work), Canada shall pay the prices detailed in Annex C – SaaS Solutions and Ceiling Prices, or in the Contractor's bid, as applicable.

9.2 Professional Services provided under a Task Authorization. (Optional clause to be used when professional services are required) For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked and any resulting deliverables / the firm price set out in the Task Authorization, in accordance with the firm all-inclusive per diem rates set out in Annex C – SaaS Solutions and Ceiling Prices or in the Contractors bid, as applicable. Applicable Taxes extra

9.3 On-Site Support Charges. (Optional clause to be used when on-site support services are required) If approved in advance by Canada, the Contractor will be paid the hourly or daily labour rates specified in the Contract, together with reasonable and proper travel and living costs incurred by the Contractor in connection with on-site services. Any travel and living costs will only be reimbursed in accordance with the applicable meal and private vehicle allowances provided in the

National Joint Council Travel Directive, as amended from time to time. All such pre-approved costs must be invoiced to Canada as a separate charge.

10. Payments

10.1. Invoices

(a) **Invoice Submission**. The Contractor must submit invoices for the Services and delivery of any Work, as applicable.

(b) **Invoice Requirements**. Invoices must be submitted in the Contractor's name and contain:

(i) the date, the name and address of the client department, item or reference numbers, deliverable/description of the Work, contract number, Client Reference Number (CRN), Procurement Business Number (PBN), and financial code(s);

(ii) details of expenditures (such as item, quantity, unit of issue, unit price, fixed time labour rates and level of effort, subcontracts, as applicable) in accordance with the Basis of Payment, exclusive of Applicable Taxes;

(iii) Applicable Taxes must be shown as a separate line item along with corresponding registration numbers from the tax authorities and all items that are zero-rated, exempt or to which Applicable Taxes do not apply, must be identified as such on all invoices

(iii) deduction for holdback, if applicable; and

(iv) the extension of the totals, if applicable.

(c) **Taxes**

(i) **Payment of Taxes**. Applicable Taxes will be paid by Canada as provided in the Invoice Submission section. It is the sole responsibility of the Contractor to charge Applicable Taxes at the correct rate in accordance with applicable legislation. The Contractor must remit to appropriate tax authorities any amounts of Applicable Taxes paid or due.

(ii) **Withholding for Non-Residents**. Canada must withhold 15 percent of the amount to be paid to the Contractor in respect of services provided in Canada if the Contractor is not a resident of Canada, unless the Contractor obtains a valid waiver from the Canada Revenue Agency. The amount withheld will be held on account for the Contractor in respect to any tax liability which may be owed to Canada.

(d) **Certification of Invoices**. By submitting an invoice, the Contractor certifies that the invoice is consistent with the Work delivered and is in accordance with the Contract.

10.2. Payment Period. Canada will pay the Contractor's undisputed invoice amount within 30 days of receipt. In the event, an invoice is not in acceptable form and content, Canada will notify the Contractor and the 30 day payment period will begin on receipt of a conforming invoice.

10.3. **Interest on Late Payments**. Canada will pay to the Contractor simple interest at the Average Rate plus 3 percent per year on any amount that is overdue, from the date that amount becomes overdue until the day before the date of payment, inclusive, provided Canada is responsible for the delay in paying the Contractor. Canada will not pay interest on overdue advance payments.

10.4. **Method of Payment**

(a) Canada will make payment to the Contract for the Services either in advance or in arrears, in accordance with Annex D Service Level Agreement or the Contractor's bid, as applicable. Where payment is made in advance, the advance payment period shall not exceed 12 months. Payment in advance does not prevent Canada from exercising any or all potential remedies in relation to this payment or the delivery of the Services.

(b) If Canada disputes an invoice for any reason, Canada will pay the Contractor the undisputed portion of the invoice, as long as the undisputed items are separate line items on the invoice and owed. In the case of disputed invoices, the invoice will only be considered to have been received for the purposes of the section 7.3 once the dispute is resolved.

10.5. **Limitation of Expenditure**. Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

10.6. **Electronic Payment of Invoices**. The Contractor accepts to be paid using any of the following Electronic Payment Instrument(s):

(a) Visa Acquisition Card:

(b) MasterCard Acquisition Card;

(c) Direct Deposit (Domestic and International);

(d) Electronic Data Interchange (EDI);

(e) Wire Transfer (International Only);

(f) Large Value Transfer System (LVTS) (Over $25M)

11. Insurance Requirements. The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection. It does not release the Contractor from or reduce its liability under the Contract.

12. Limitation of Liability

Note to Suppliers: PSPC and SSC are working to develop a Cloud Commodity Grouping to provide an updated Limitation of Liability Clause to be used by both PSPC and SSC for cloud procurement. This new Limitation of Liability clause will replace the current Limitation of Liability wording in these Resulting Contract Clauses as soon as it becomes available.

(a) Except as expressly provided in paragraph (b), the Contractor is liable to Canada for all direct damages it causes in performing or failing to perform the Contract in relation to:

1. The Contractor's acts or omissions under the Contract affecting real or tangible personal property owned, possessed or occupied by Canada;
2. The Contractor**'**s breach of confidentiality obligations under the Contract, but such limitation does not apply to the disclosure by Contractor of the trade secrets of Canada or a third party related to information technology;
3. Liens or encumbrances relating to any portion of the Work under the Contract, not including claims or encumbrances relating to intellectual property rights; and

4. Contractors breach of warranty obligations;

However, the Contractor is not liable to Canada for indirect, special or consequential damages caused by items 1 to 4 above.

(b) With respect to direct damages related to the Contractor's breach of warranty obligations, the Contractor**'**s maximum liability to Canada is the total estimated cost of the Contract (meaning the dollar amount shown on the first page of the Contract in the block titled "**Total Estimated Cost**"). All direct damages not listed above that do not relate to breach of warranty are subject to a maximum of .25 times the Total Estimated Cost or $1M, whichever is greater.

(c) If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

(d) None of the above limitations apply to damages based on loss of life or injury or claims based on infringement of intellectual property.

13. General Provisions

13.1. **Applicable Laws**. This Contract will be interpreted and governed by the laws of [PROVINCE].

13.2. **Survival**. All the parties' obligations of confidentiality, representations and warranties set out in the Contract as well as the provisions, which by the nature of the rights or obligations might reasonably be expected to survive, will survive the expiry or termination of the Contract.

13.3. **Severability**. If any provision of this Contract is declared unenforceable by an authoritative court, the remainder of this Contract will remain in force.

13.4. **Waiver**. The failure or neglect by a party to enforce any of rights under this Contract will not be deemed to be a waiver of that party's rights.

13.5 No Bribe. The Contractor warrants that no bribe, gift, benefit, or other inducement has been or will be paid, given, promised or offered directly or indirectly to any official or employee of Canada or to a member of the family of such a person, with a view to influencing the entry into the Contract or the administration of the Contract.

13.6 Contingency Fees. The Contractor represents that it has not, directly or indirectly, paid or agreed to pay and agrees that it will not, directly or indirectly, pay a contingency fee for the solicitation, negotiation or obtaining of the Contract to any person, other than an employee of the Contractor acting in the normal course of the employee's duties. In this section, "contingency fee" means any payment or other compensation that depends or is calculated based on a degree of success in soliciting, negotiating or obtaining the Contract and "person" includes any individual who is required to file a return with the registrar pursuant to section 5 of the *Lobbying Act*, 1985, c. 44 (4th Supplement).

13.7 International Sanctions.

(a) Persons in Canada, and Canadians outside of Canada, are bound by economic sanctions imposed by Canada. As a result, the Government of Canada cannot accept delivery of goods or services that originate, either directly or indirectly, from the countries or persons subject to economic sanctions.

(b) The Contractor must not supply to the Government of Canada any goods or services which are subject to economic sanctions.

(c) The Contractor must comply with changes to the regulations imposed during the period of the Contract. The Contractor must immediately advise Canada if it is unable to perform the Work as a result of the imposition of economic sanctions against a country or person or the addition of a good or service to the list of sanctioned goods or services. If the Parties cannot agree on a work around plan, the Contract will be terminated.

13.8 Integrity Provisions - Contract. The *Ineligibility and Suspension Policy* (the "Policy") and all related Directives incorporated by reference into the bid solicitation on its closing date are incorporated into, and form a binding part of the Contract. The Contractor must comply with the provisions of the Policy and Directives, which can be found on Public Works and Government Services Canada's website at *Ineligibility and Suspension Policy*.

13.9. **Code of Conduct for Procurement - Contract**. The Contractor agrees to comply with the *Code of Conduct for Procurement* and to be bound by its terms for the period of the Contract.

13.10. **Conflict of interest and Values and Ethics Codes for the Public Service**. The Contractor acknowledges that individuals who are subject to the provisions of the *Conflict of interest Act*, 2006, c. 9, s. 2, the Conflict of interest Code for Members of the House of Commons, the Values and Ethics Code for the Public Service or all other codes of values and ethics applicable within specific organizations cannot derive any direct benefit resulting from the Contract.

13.11. **Authorities**

Contracting Authority

The Contracting Authority for the Contract is:

Name:

Title:

Organization:

Address:

Telephone:

E-mail address:

The Contracting Authority must receive a copy of the Invoice for Canada's record and review.

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

Technical Authority

The Technical Authority for the Contract is:

Name:

Title:

Organization:

Address:

Telephone:

Facsimile:

E-mail address:

The Technical Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

Client Administrative Contact

The Client Administrative Contact is:

Name:

Title:

Organization:

Address:

Telephone:

Facsimile:

E-mail address:

The Client Administrative Contact must receive the original Invoice. All inquiries for request for payment must be made to the Client Administrative Contact.

Contractor's Representative

The Contractor's Representative is:

Name:

Title:

Telephone:

Facsimile:

E-mail address:

This Contract has been executed by the parties.

[CONTRACTOR NAME]	[CONTRACTING AUTHORITY]]
By:	By:
Name:	Name:
Title:	Title:

APPENDIX A – DELIVERABLES

1. TABLE 1 - LIST OF INITIAL DELIVERABLES

Table 1 - List of Initial Deliverables							
Item No.	**Supplier's Product Name** (Per Annex C)	**Supplier's Part No.** (Per Annex C)	**Unit of Measure** (Per Annex C)	**Period**	**Qty**	**Unit Price**	**Extended Price**
1							
...							
						Sub-Total:	$0.00

2. TABLE 2 - LIST OF OPTIONAL DELIVERABLES *(if applicable)*

Table 2 - List of Optional Deliverables						
Item No.	**Supplier's Product Name** (Per Annex C)	**Supplier's Part No.** (Per Annex C)	**Unit of Measure** (Per Annex C)	**Period**	**Qty**	**Unit Price**
1						
...						
					Sub-Total:	$0.00

APPENDIX B - DEFINITIONS AND INTERPRETATIONS

In this Contract, unless the context otherwise requires, the following terms shall have the following meanings:

“Asset” means all information technology resources used, accessed or managed by the Supplier to provision and deliver the Services described in this Agreement (including, without limitation, all technology resources at the Supplier’s Service Locations or at the Supplier’s or a Supplier Subcontractor’s data centre, networking, storage, servers, virtualization platforms, operating systems, middleware, and applications).

“Applicable Taxes” means the Goods and Services Tax (GST), the Harmonized Sales Tax (HST), and any provincial tax, by law, payable by Canada such as, the Quebec Sales Tax (QST) as of April 1, 2013.

“Average Rate” means the simple arithmetic mean of the Bank Rates in effect at 4:00 p.m. Eastern Time each day during the calendar month immediately before the calendar month in which payment is made.

“Bank Rate” means the rate of interest established from time to time by the Bank of Canada as the minimum rate at which the Bank of Canada makes short term advances to members of the Canadian Payments Association.

“Canada”, “Crown”, “Her Majesty” or “the Government” means Her Majesty the Queen in right of Canada as represented by the Minister of Public Works and Government Services and any other person duly authorized to act on behalf of that minister or, if applicable, an appropriate minister to whom the Minister of Public Works and Government Services has delegated his or her powers, duties or functions and any other person duly authorized to act on behalf of that minister.

“Canada Data” means information or data, regardless of form or format: (A) disclosed by or related to the Canada’s personnel, clients, partners, joint venture participants, licensors, vendors or suppliers; (B) disclosed by or related to End Users of the Services; or (C) collected, used or processed by, or stored for, the Services; which is directly or indirectly: (i) disclosed to the Supplier or Supplier Subcontractors by or on behalf of the Canada or End Users; (ii) to which the Supplier or any Supplier Subcontractors obtains access, intentionally or inadvertently; (iii) resident on any Asset, or on any other network, System or Hardware used or managed for Canada by the Supplier for the Services and Supplier’s services, including Supplier Infrastructure; or (iv) generated, developed, acquired or otherwise obtained by the Supplier or any Supplier Subcontractor or Sub-processor as part of or in the course of providing the Services; and includes all information derived from such information and all metadata forming part of or associated with such information. For greater certainty, “Canada Data” includes all information and data stored in or processed through the Services, Assets, or Supplier Infrastructure.

“Client” means the department or agency for which the Work and/or Services are performed under the Contract. In such respect, Client may refer to any Government Department, Departmental Corporation or Agency, or other Crown entity described in the Financial Administration Act (as amended from time to time), and any other party for which the Department of Public Works and Government Services may be authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act

“Client Data” means (i) any data provided to the Contractor by Client or at its direction in connection with the Solution and (ii) all content that the Contractor develops and delivers to Client, and that Client accepts, in accordance with this Contract.

“Cloud Computing” means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and

services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

“Cloud Infrastructure” means the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer. [NIST]

“Cloud Service Provider (“CSP”)” means the entity that owns, operates and maintains the physical infrastructure on which a Solution is hosted and from which a Solution is distributed. A CSP may also be SaaSP if they host and distribute their own and third-party solutions. “Commercially Available” means a product and/or service available to the public to obtain for use or consumption and requires no special modification or maintenance over its life cycle.

“Contract” means the Articles of Contract, any general conditions, any supplemental general conditions, annexes, appendices and any other document specified or referred to as forming part of the Contract, all as amended by agreement of the Parties from time to time.

“Contracting Authority” means the person designated by that title in the Contract, or by notice to the Contractor, to act as Canada's representative to manage the Contract.

“Contractor” means the entity named in the Contract to provide the Services and/or the Work to Canada

“Contract Price” means the amount stated in the Contract to be payable to the Contractor for the Work, exclusive of Applicable Taxes.

“Cost” means cost determined according to Contract Cost Principles 1031-2 as revised to the date of the bid solicitation or, if there was no bid solicitation, the date of the Contract.

“Date of payment” means the date of the negotiable instrument drawn by the Receiver General for Canada to pay any amount under the Contract.

“Deliverable” or “Deliverables”, when used generically, refers to any discrete part of the Work to be performed for Canada.

“Device” means equipment having a physical central processor unit (CPU), mass storage and input output devices such as keyboard and monitor and includes servers, desktops, workstations, notebooks, laptops, personal digital assistants and mobile computing equipment.

“Error” means any instruction or statement contained in or absent from the Solution, which, by its presence or absence, prevents the Solution from operating in accordance with the Specifications.

“Federal Government Working Day” is defined as Monday to Friday, 8:00 am to 4:00 pm Eastern Time, excluding statutory holidays observed by Canada.

“IaaS“ or “Infrastructure as a Service” means “(t)he capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).”

“IaaS Infrastructure” means Infrastructure managed by the Contractor and provided as a Service (e.g. Data Center, Networking, Storage, Servers, Virtualization platform). This also includes the Systems, Hardware and Software that are used to manage, operate and provision an IaaS Infrastructure.

“Information Assets” means any individual data element of such Canada Data.

“Information Spillage” means incidents where an Information Asset is inadvertently placed on an Asset or System that is not authorized to process it (e.g. ITSG-33, IR-9).

“PaaS” or ”Platform as a Service” means “(t)he capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. [NIST]

“PaaS Infrastructure” means the platform infrastructure managed by the Contractor and provided as a Service (e.g. Data Center, Networking, Storage, Servers, Virtualization platform, O/S, Middleware, and Runtime). This also includes the Systems, Hardware and Software that are used to manage, operate and provision the PaaS Infrastructure.

“Party” means Canada, the Contractor, or any other signatory to the Contract and “Parties” means all of them.

“Public Cloud” means the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

“Public Services and Procurement Canada” or “Public Works and Government Services Canada” means the Department of Public Works and Government Services as established under the Department of Public Works and Government Services Act.

“Overdue” means the time when an amount is unpaid on the first day following the day on which it is due and payable according to the Contract.

“Personal Information” means information that is about an identifiable individual and recorded in any form, as defined in section 3 of the Privacy Act. Examples include, but is not limited to the information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual. Definition from Government of Canada Justice Laws Website : https://laws-lois.justice.gc.ca/eng/acts/P-21/section-3.html

“Processor” means a natural or legal person, public authority, agency or other body that processes Personal Information on behalf of, and in accordance with the instructions of, Canada.

“Product Manufacturer” means the entity which assembles the component parts to manufacture a Product.

“Public Cloud” means the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

“Public Cloud Services” means a shared pool of configurable Cloud Computing service models made available to users as a rapid, on demand, elastic self service via the Internet from a Cloud Service Provider's servers as opposed to being provided from a company's own on-premises servers, but does

not include managed services, training, private or on-premise cloud services, or professional or consulting services that exceed standard public commercially available support services.

“Quick Start” Services – means a defined package of services possibly including essential training on best practices, Architecture, Deployment, Operational Design Integration, scalability, or use of the Solution. Also sometimes referred to as a Jump Start Package or Quick Start Guide.

“Record” means any hard copy document or any data in a machine-readable format containing Personal Information or Canada data

“Security Event Log” means any event, notification or alert that a device, systems or software is technically capable of producing in relation to its status, functions and activities. Security Events Logs are not limited to security devices, but are applicable to all devices, systems and software that are technically capable of producing event logs that can be used in security investigations, auditing and monitoring. Examples of Systems that can produce security event logs are, but not limited to: firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, network, authentication services, directory services, DHCP, DNS, hardware platforms, virtualization platforms, servers, operating systems , web servers, databases, applications , application/layer 7 firewalls.

“Security Incident” means any observable or measurable anomaly occurring with respect to an Asset, which results, or which may result, in: (A) a violation of the Canada’s Security Policies, a Specific Security Measure, the Supplier’s or Supplier Subcontractor’s security policies or procedures, or any requirement of these Security Obligations or the Privacy Obligations; or (B) the unauthorized access to, modification of, or exfiltration of any Authorized Personnel’s credentials, Users’ credentials, or Information Asset.

“Service Level Agreement (SLA)” means an agreement between the Supplier and Canada that defines the level of service expected from the Supplier.

“Service Location(s)” means any facility, site or other physical location owned, leased, provisioned or otherwise occupied by the Supplier or any Supplier Sub-processor from which the Supplier or any Supplier Sub-processor provides any Public Cloud Services.

“Services” means

i) granting usage rights to the software application(s) (“Solutions”)

ii) providing Solution Documentation;

iii) maintaining, upgrading, and updating the Solution(s);

iv) managing incidents and defects to ensure the Solution(s) operate at the applicable service levels; and,

v) providing incidental and additionally required information technology infrastructure services required to deliver the Solution.

“Software as a Service” or “SaaS” means the service model through which the capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. [NIST]

“SaaS Publisher” (“SaaSP”)” means the entity that owns, operates, maintains and distributes SaaS Solutions.

“Solution Availability” means the percentage of minutes in a month that the Solution is operational.

“Solution Documentation” means all of the manuals, handbooks, user guides and other human-readable material to be provided by the Contractor to Canada under the Contract for use with the Solution.

“SaaS Solution or “Solution” means the software application delivered through a SaaS distribution model in which an Application Service Provider or Cloud Service Provider makes centrally hosted software applications available to customers over the Internet, providing access to and use of a fully maintained, automatically upgraded, up-to-date Solution, technical support services, as well as physically and electronically secure information technology infrastructure, all included in the subscription service.

“Specifications” means the description of the essential, functional or technical requirements of the Services in Annex D, Service Level Agreement, including the procedures for determining whether the requirements have been met.

“Submission” means the documents that the Supplier submits in response to the RFSA.

“Sub-processor” means any natural or legal person, public authority, agency or other body which processes personal information on behalf of a data controller.

“Supplier” means the person or entity (or, in the case of a joint venture, the persons or entities) presenting a Submission in response to this Request for Supply Arrangement (RFSA) issued by Canada. It does not include the parent, subsidiaries or other affiliates of the Supplier, or its subcontractors.

“Usage rights” means granting access to and use of a Solution, also sometimes known as a subscription license.

“User” means any individual, or system process acting on behalf of an individual, authorized by the Canada to access the Services.

“Value-Added Reseller” or “VAR” means a Supplier who is an affiliate, partner, value-added reseller or other channel distributor of SaaS. VAR does not include a Software Publisher, an SaaSP, or a CSP who is also an SaaSP.

“Workplace Technology Devices” means desktops, mobile workstations such as laptops and tablets, smartphones, phones, and peripherals and accessories such as monitors, keyboards, computer mouse, audio devices and external and internal storage devices such as USB flash drives, memory cards, external hard drives and writable CD or DVD.

APPENDIX C – SECURITY OBLIGATIONS

Security Obligations

The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to Sub-processors, to the extent applicable to each Contractor Sub-processor, given the nature of the Public Cloud Services provided by it to the Contractor.

1. **Change Management.**

(a) The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Obligations as needed to comply with the security practices of industry standards.

(b) The Contractor must advise Canada of all improvements that affect the Services in this Contract, including technological, administrative or other types of improvements. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

2. Acknowledgements. The parties acknowledge that:

(a) All Assets and Information Assets are subject to these Security Obligations.

(b) Notwithstanding any other provision of the Contract, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Assets and Information Assets.

3. **Data Transfer and Retrieval.**

The Contractor must, upon request by Canada:

(a) Extract all online, nearline, and offline information assets, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a Canada code repository, and network configurations such that the Client can use these instructions to migrate from one environment to another environment; and

(b) Securely transfer all Information Assets, including metadata, in a machine-readable and usable format acceptable to Canada, in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx).

4. **Data Disposition and Returning Records to Canada.**

(1) The Contractor must, upon request by Canada, securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Information Assets and ensure that previously stored data cannot be addressed by others customers after it is released. This includes all copies of Information Assets that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following: (i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Clearing and Declassifying Electronic Data Storage Devices (CSE ITSG-06).

(2) The Contractor must, upon request by Canada, provide evidence that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from the Canada instance.

6. **Continuous Monitoring**.

(1) The Contractor must continually manage, monitor, and maintain the security posture of all Assets, Supplier Infrastructure and Service Locations throughout the period of the Contract, and ensure that the Public Cloud Services provided to Canada are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:

(a) Actively and continuously monitor threats and vulnerabilities to its Assets, Supplier Infrastructure, Service Locations, or Information Assets;

(b) Undertake best efforts to prevent attacks through security measures such as denial of service protections;

(c) Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;

(d) Identify unauthorized use and access of any Public Cloud Services, data and components relevant to Canada's IaaS, PaaS or SaaS Solution;

(e) Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Public Cloud Services or libraries that the Solution make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

(f) Respond, contain, and recover from threats and attacks against the Contractor Services; and

(g) Where required, take proactive countermeasures, including taking both pre-emptive and responsive actions, to mitigate threats.

(2) The Contractor's Public Cloud Services must allow for GC application data (for IaaS, PaaS and SaaS) and GC network traffic (for IaaS and PaaS) of cloud hosted GC services to be copied and forwarded to a predetermined location (in the cloud or on GC premises).

(3) The Contractor's Public Cloud Services must allow Canada to deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for Canada's Solution at the Canada managed host and network layer, for Canada managed components only.

7. Notifications.

(1) The Contractor must provide:

(a) Timely notification of any interruption that is expected to impact service availability and performance (as agreed to by the parties and included in the SOW and/or SLA);

(b) Regular updates on the status of returning the Solution to an operating state according to the agreed upon SLAs and system availability requirements, both as advance alerts and post-implementation alerts; and

(c) Information system security alerts, advisories, and directives via email for vulnerabilities that pose a threat to the Solution

8. Security Incident Response

(1) If the Contractor becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data or Personal Information while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay (i) notify Canada of the Security Incident; (ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(2) The Contractor must alert and promptly notify the Client (via phone and email) of any compromise, breach or of any evidence such as (i) a Security Incident, (ii) a security multifunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information Asset, or (v) another irregular activity identified by the Contractor, that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days), and will be made without undue delay, in any event, within 24 hours.

(3) The Contractor must collaborate with Canada on the containment, eradication, and recovery of Security Incidents in accordance with the Contractor's Security Incident response process and in alignment with the GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html). This includes:

(a) Allowing only designated representatives of Canada to have the ability to:
   i. request and receive information associated with the Security Incident and any compromised Information Assets (including user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;
   ii. track the status of a reported information security event or Security Incident.

(b) Supporting Canada's investigative efforts in the case of any compromise of the users or data in the Solution that is identified.

(4) The Contractor must:

(a) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data or the service; and

(b) Track, or enable Canada to track, disclosures of Assets and Information Assets, including what data has been disclosed, to whom, and at what time.

9. E-Discovery and Legal Holds

The Contractor must (and must, to the extent applicable given the nature of the subcontracted Public Cloud Services provided by each Contractor Sub-processor, require Contractor Sub-processors to) take reasonable measures to ensure the Solution provides e-discovery and legal hold features for the Security Event Logs in order to enable Canada to conduct timely and effective security investigations and meet legal court requests for legal holds.

10. Security Assessment Testing

The Contractor must have a process that allows Canada to conduct a non-disruptive and non-destructive vulnerability scan or penetration test of Canada's portion of the Solution components within the Contractor environment.

11. Sub-processors

(1) 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.

(2) 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. The Contractor must assist Canada with verification of sub-processors within 10 working days.

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.

APPENDIX D – PRIVACY OBLIGATIONS

1.0. Auditing Compliance

(1) In the event Canada needs to conduct security audits, inspections and/or review any additional information (e.g., documentation, data protection description, data architecture and security descriptions) pursuant to Section 12.1, both Parties agree to negotiate a solution in good faith and consider both the rationale for Canada's request and the Contractor's processes and protocols.

(2) Within 30 days of request from the Contracting Authority, the Contractor must engage a third party to conduct a privacy audit or provide evidence to confirm that it does not generate, collect, use, store or disclose any additional personal information as defined by Canada, other than Client data as defined by the Contractor and does not specifically have Personal Information in Support Data (collected in logs (e.g., telemetry data such as email message headers and content).

2.0 Data Ownership and Privacy Requests

(1) Client Data including all Personal Information (PI) will be used or otherwise processed only to provide the Services, including purposes compatible with providing the Services. The Contractor must not use or otherwise process Canada Data or derive information from it for any advertising or similar commercial purposes. As between the parties, the Client retains all right, title and interest in and to Client Data. The Contractor acquires no rights in Canada Data, other than the rights Client grants to the Contractor to provide the Solution to the Customer.

(2) All data the Contractor stores, hosts or processes on behalf of Canada remains the property of Canada. When requested by the Contracting Authority, the Contractor must provide Personal Information records within five Federal Government Working Days (or seven Federal Government Working Days if it must be retrieved from offsite backup/replication) in a Word or Excel document.

4.0 Assist in Delivery of Canada's Privacy Impact Assessment

(1) Upon request of the Technical Authority, the Contractor must support Canada in creating a privacy impact assessment in accordance with the Treasury Board Directive on Privacy Impact Assessment (https://www.statcan.gc.ca/eng/about/pia/dcpia) by assisting the Canada with the supporting documentation including a foundational PIA for Canada provided by the Contractor. The Contractor agrees to provide this support within ten working days of a request or within a mutually agreed upon timeframe depending on the complexity of the request by the Canada.

5.0 Privacy Breach

(1) The Contractor must alert and promptly notify the Technical Authority (via phone and email) of any compromise, breach or of any evidence that leads the Contractor to reasonably believe that risk of compromise, or a breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365

days), and within the service level commitments detailed in the applicable Annex D – Service Level Agreement.

(2) If the Contractor becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data or Personal Information while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay:

i. notify Canada of the Security Incident;
ii. investigate the Security Incident and provide Canada with detailed information about the Security Incident; and
iii. take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(3) The Contractor must:

(c) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data; and

(d) Tracks, or enables Canada to track, disclosures of Canada Data, including what data has been disclosed, to whom, and at what time.

THE FOLLOWING SECURITY REQUIREMENTS ARE OPTIONAL (TO BE USED WHERE THE CONTRACTOR WILL HAVE ACCESS TO PROTECTED INFORMATION)

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

(a) Appendix D – Security Requirements for Canadian Contractor

(b) Appendix E – Security Requirements for Foreign Contractor

Appendix D – 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.

Appendix E – 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), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming **Contractor/Subcontractor** compliance with the security requirements for foreign suppliers. 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. 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.
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:
    i. The Foreign recipient **Contractor/Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.
    ii. 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.
    iii. 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.
        (a) 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

3. 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.

4. **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).

5. 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.

6. 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.

7. 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.

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

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

10. 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.

11. 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.

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**.

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) 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.

(2) 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.

(3) 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.

13. Maintaining the Accuracy, Privacy and Integrity of Personal Information

(1) 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:

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

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

(c) 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);

(d) 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;

(e) 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;

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

(g) include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor/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;

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

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

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

12.10 Safeguarding Personal Information

(1) 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:

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

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

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

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

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

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

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

12.11 Statutory Obligations

(1) 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.

(2) 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.

12.12 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.

12.13 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.

12.14 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.

12.15 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.

APPENDIX G – SUPPLY CHAIN INTEGRITY PROCESS

1. On-going Supply Chain Integrity Process

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

1.1.1.1 an IT Product List;

1.1.1.2 a list of subcontractors; and

1.1.1.3 network diagram(s).

This SCSI is included as Appendix G. The Parties also acknowledge that security is a critical consideration for Canada with respect to this Contract and that on-going assessment of SCSI will be required throughout the Contract Period. This Article governs that process.

1.1.2 Assessment of New SCSI: During the Contract Period, the Contractor may need to modify the SCSI information contained in Appendix G . In that regard:

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

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

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

1.1.2.4 Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is provided by the Contractor or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of any proposed new SCSI.

1.1.3 Identification of New Security Vulnerabilities in SCSI already assessed by Canada:

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

1.1.3.2 The Contractor acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified and, that being the case, new security vulnerabilities may be identified in SCSI that have

already been the subject of an SCSI assessment and assessed without security concerns by Canada, either during the procurement process or later during the Contract Period.

1.1.4 Addressing Security Concerns:

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

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

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

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

c) implement the mitigation plan approved by Canada.

This process applies both to new Products and to Products that were already assessed pursuant to the Supply Chain Integrity Process assessment by Canada, but for which new security vulnerabilities have since been identified.

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

1.1.5 Cost Implications:

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

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

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

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

d) the normal useful life of the Product;

e) any “end of life” or other announcements from the manufacturer of the Product indicating that the Product is or will no longer be supported;

f) the normal useful life of the proposed replacement Product;

g) the time remaining in the Contract Period;

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

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

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

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

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

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

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

1.1.6 General:

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

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

1.1.6.3 Any service levels that are not met due to a transition to a new Product or subcontractor required by Canada pursuant to this Article will not trigger a Service Credit, nor will a

failure in this regard be taken into consideration for overall metric calculations, provided that the Contractor implements the necessary changes in accordance with the migration plan approved by Canada or proceeds immediately to implement Canada's requirements if Canada has determined that the threat to national security is both serious and imminent.

1.1.6.4 If the Contractor becomes aware that any subcontractor is deploying Products subject to security concerns in relation to the Services and/or Work, the Contractor must immediately notify both the Contracting Authority and the Technical Authority and the Contractor must enforce the terms of its contract with its subcontractor. The Contractor acknowledges its obligations pursuant to General Conditions 2035, Subsection 8(3).

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

2. Subcontracting

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

2.1.1.1 the name of the subcontractor;

2.1.1.2 the portion of the Services and/or Work to be performed by the subcontractor;

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

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

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

2.1.1.6 any other information required by the Contracting Authority.

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

3. Change of Control

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

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

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

b) the entities have now or in the two years before the request for the infor*mation had a fid*uciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

c) the entities otherwise do not deal with one another at arm's length, or ea*ch of them does* not deal at arm's length with the same third party.

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

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

3.1.1.4 other information

related to ownership and control that may be requested by Canada.If requested by the Contracting Authority, the Contractor must provide this information regarding its subcontractors as well. However, if a subcontractor considers this information to be confidential, the Contractor may meet its obligation by having the subcontractor submit the information directly to the Contracting Authority. Regardless of whether the information is submitted by the Contractor or a subcontractor, Canada agrees to handle this information in accordance with Subsection 22(3) of General Conditions 2035 (General Conditions – Higher Complexity – Services), provided the information has been marked as either confidential or proprietary.

3.1.2 The Contractor must notify the Contracting Authority in writing of:

3.1.2.1 any change of control in the Contractor itself;

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

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

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

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

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

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

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

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

Competitive procurement starts with prerequisite National Security Exemption	L'approvisionnement concurrentiel commence par l'exemption relative à la sécurité nationale préalable
Bidder provide Supply Chain Security Information (SCSI) to Contracting Authority	Le soumissionnaire fournit l'information sur la sécurité de la chaîne d'approvisionnement (ISCA) à l'autorité contractante.
Cyber and IT Security (CITS) reviews SCSI in consultation with Security Partners	La Cybersécurité et sécurité de la technologie de l'information (CSTI) examine l'ISCA conjointement avec les partenaires en matière de sécurité.
Bidder has 10 calendar days to resubmit revised SCSI with mitigation applied	Le soumissionnaire a 10 jours civils pour présenter à nouveau l'ISCA révisée comprenant les mesures d'atténuation utilisées.
Decision by CITS	La CSTI rend sa décision.
Yes	Oui
Bidder receives approval letter to continue to next phase of procurement	Le soumissionnaire reçoit la lettre d'approbation lui permettant de passer à l'étape suivante de l'approvisionnement.
Competitive procurement completes with resulting contract	L'approvisionnement concurrentiel se termine par l'attribution du contrat.
Cross check of lists provided for SCI at implementation	Comparaison des listes fournies pour l'ICA lors de la mise en œuvre.
No	Non
1st Rejection: Debrief session with Bidder to identify mitigations	1er refus : séance de compte rendu avec le soumissionnaire pour déterminer les mesures d'atténuation.
2nd Rejection: Bidder does not qualify	2e refus : le soumissionnaire est exclu du processus.

On-going SCI auditing from the moment the contract has been awarded until it ends.	Vérification continue de l'ICA à partir du moment où le contrat est attribué jusqu'à la fin du contrat.
Contractor provides revised SCSI on regular basis	L'entrepreneur fournit de l'ISCA révisée régulièrement.
CITS reviews SCSI in consultation with Security Partners	La CSTI examine l'ISCA conjointement avec les partenaires en matière de sécurité.
Contractor has to resubmit revised SCSI with mitigation applied	L'entrepreneur doit présenter à nouveau l'ISCA révisée comprenant les mesures d'atténuation utilisées.
Decision by CITS	La CSTI rend sa décision.
Yes	Oui
Contractor receives Approval	L'entrepreneur reçoit l'approbation
Non	Non
Debrief session with Contractor	Séance de compte rendu avec l'entrepreneur
Internal threat evaluation can lead to the review of specific equipment or services	L'évaluation des menaces internes peut mener à l'examen de matériel ou de services précis.

Contractor has to resubmit revised SCSI with mitigation applied	L'entrepreneur doit présenter à nouveau l'ISCA révisée comprenant les mesures d'atténuation utilisées.
CITS in consultation with Security Partners monitors threats or security audits	La CSTI, conjointement avec les partenaires en matière de sécurité, surveille les menaces ou les vérifications de sécurité.
Threat identified?	A-t-on décelé une menace?
Yes	Oui
Debrief session with Contractor	Séance de compte rendu avec l'entrepreneur

APPENDIX H – TASK AUTHORIZATION FORM

TASK AUTHORIZATION (TA)				
Contractor:		**Contract Number:**		
Commitment: #		**Financial Coding:**		
Task Number (Amendment):		**Issue Date:**		**Response Require By:**
1. Statement of Work (Work Activities, Certifications and Deliverables)				
2. Period of Service:	**From** (Date)	To be determined	**To** (Date)	To be determined
3. Work Location:				
4. Travel Requirements:				
5. Language Requirement:				
6. Other Conditions/Constraints:				
7. Level of Security Clearance required for the Contractor Personnel:				
8. Contractor's Response:				

Category and Name of Proposed Resource	PWGSC Security File Number	Rate	Estimated # of Days	Total Cost
			Estimated Cost	
			Applicable Taxes	
			Total Labour Cost	

TASK AUTHORIZATION (TA)	
Total Travel & Living Cost	
Firm Price	

Contractor's Signature

Name, Title and Signature of Individual Authorized to sign on behalf of the **Contractor** (type or print) _____	Signature: _____ Date: _____

Approval – Signing Authority

Signatures (Client)	**Signatures (PWGSC)**
Name, Title and Signature of Individual Authorized to sign: Technical Authority: _____ Date: _____	Contracting Authority: _____ Date: _____

You are requested to sell to her Majesty the Queen in Right of Canada, in accordance with the terms and conditions set out herein, referred to herein, or attached hereto, the services listed herein and in any attached sheets at the price set out thereof.