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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

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

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

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

Comments - Commentaires

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

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

Title - Sujet RFSA - SaaS Method of Supply	
Solicitation No. - N° de l'invitation EN578-191593/F	**Date** 2022-02-18
Client Reference No. - N° de référence du client 20191593	**Amendment No. - N° modif.** 017
File No. - N° de dossier 002ess.EN578-191593	**CCC No./N° CCC - FMS No./N° VME**
GETS Reference No. - N° de référence de SEAG PW-$EEM-003-35660	
Date of Original Request for Supply Arrangement **Date de demande pour un arrangement en matière d'app. originale**	2019-05-10
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** Eastern Daylight Saving Time EDT **on - le 2024-10-25** Heure Avancée de l'Est HAE	
Address Enquiries to: - Adresser toutes questions à: Guillot, Jacob	**Buyer Id - Id de l'acheteur** 002ess
Telephone No. - N° de téléphone (343) 552-1378 ( )	**FAX No. - N° de FAX** ( ) -
Delivery Required - Livraison exigée	
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	
Security - Sécurité This revision does not change the security requirements of the solicitation. Cette révision ne change pas les besoins en matière de sécurité de l'invitation.	

Instructions: See Herein

Instructions: Voir aux présentes

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

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

Signature **Date**

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

For the Minister - Pour le Ministre

Canada

PUBLIC SERVICE AND PROCUREMENT CANADA (PSPC)

Amendment no. 017 to Request for Supply Arrangement (RFSA)
for

SaaS Method of Supply (GC CLOUD)

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

THIS AMENDMENT 017 IS RAISED TO:	
1.0	Correct responses given to questions regarding the Request for Supply Arrangement (RFSA) addressed through previous amendments, as detailed in Section 1.0, below;
2.0	Respond to questions received regarding the RFSA, as detailed in Section 2.0, below;
3.0	Modify the RFSA, as detailed in Section 3.0, below.
4.0	Minor administrative changes that do not affect the meaning and impact of the terms and conditions made throughout.
5.0	Replace solicitation documents in their entirety to incorporate revisions made in Amendment 001 to Amendment017, as detailed in Section 5.0, below.

1.0 Correct responses given to questions regarding the RFSA address through previous amendments:

QUESTIONS	ANSWERS
IDQ.45 Do you want to see vendors go through approvals for Protected A first, to reduce effort to evolve to Protected B later (e.g. if we have additional audits for ISO/SOC2 in progress now)? Or should we just wait and do Protected B from scratch later?	**IDA.45** This is up to suppliers to decide. If you do not have solutions for protected A data, then we would recommend to wait and do protected B when you are ready, as CCCS has limited capacity to assess solutions so we do not want them to be assessing at a Protected A level if this is not useful to clients. If a vendor that has already been assessed at PA wishes to upgrade to PB, they will need to reapply in a future CCCS onboarding wave to do so.
IDQ.46 If a department wants a SaaS for unclassified requirements, is it still required to achieve approval for Protected A?	**IDA.46** Through AMD 017, Canada has added Stream 4 for unclassified SaaS solutions. For more information on the new unclassified stream, please refer to the contents of AMD 017.

2.0 Respond to questions received regarding the RFSA:

QUESTIONS	ANSWERS
Q. 140 Can the crown modify the security requirements for onboarding and assessment for Protected B SaaS providers? As an alternative to ISO 27017 and ISO 27018, can you accept ISO 27701? A significant portion of the controls overlap and can be mapped across all three.	**A. 140** ISO 27017 has a focus on security in the cloud, and ISO 27018 has a focus on privacy in the cloud. While there may be some overlap between these certifications and ISO 27701, it could not be considered as a alternative as it does not cover all provisions set out in both 27017 and 27018.
Q. 141 We have concerns about reading this definition of “Security Incident” into “incident” in Section 13.1(c) because numerous Security Incidents, i.e. “measurable anomalies,” are very likely to comprise a single data breach. As a result, under this construction, the limitation in Sec. 13.1(c) would apply to all “measurable anomalies”, greatly increasing the limitation on liability from what otherwise would apply to a single event. For this reason, we propose to define “incident” in Sec. 13.1(b) to include all Security Incidents that form a series of related events that comprise a data breach.	**A. 141** With regards to section 13.1(c) Limitation per incident, your question is about the impact that a security incident would have, however this clause is referring to a singular incident that occurs, not to the impact of such an incident. The definition for a “Security Incident” that is provided in Appendix B is sufficient.
Q. 142 With only the government mandating the clause 10.4 Price Certification, can we agree that only government customers purchase like services and agencies using this contract are compared against each other?	**A. 142** The GC has considered the request and the requirement shall remain the same. We cannot agree that when considering the “most favoured customer” only GC customers be considered. The requirement is that that the vendor compares against all customers, government or otherwise, that receive the like quantity and quality of the Services.
Q. 143 Is it sufficient enough to have all resources complete a Reliability Status check? Must there be Canadian based support personnel?	**A. 143** In regard to the inquiry regarding personnel resources, it would be dependent on the level of data they are accessing. If you have personnel resources that do not require to access the information as described in Annex J table 1 section 3, they do not need to hold a secret status. A secret status is only for individuals with privileged access rights who will be accessing Protected B information as described in Annex J.

QUESTIONS	ANSWERS
Q. 144 A few GC departments have asked where they'll be able to find us once we are approved for RFSA - SaaS Method of Supply (GC Cloud) (EN578-191593/F). Is there a list on Buy and Sell somewhere?	**A. 144** A list of active SA holders under the SaaSSA can be found here: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EEM-003-35660; specifically under the related award notices tab near the bottom of the page. Here client departments will be able to monitor and identify active SAs available for immediate use by authorized client authorities.
Q. 145 Does qualifying (being awarded an SA) for Stream 1 (Protected B) automatically qualify the organization to participate on eventual bids that only require Stream 2 (Protected A) requirements?	**A. 145** Yes, that is correct. If the vendor were to be awarded an SA after submitting a response under Stream 1, this would indicate that the vendor has met all of the conditions set forth for Protected B assessments and personnel screening as set forth in the SaaSSA. Therefore, the vendor would also meet the requirements for Unclassified and Protected A procurements.
Q. 146 in Q127/A127 there is a response of: "If the VAR does not have a role in Data Residency, then they would not be required to pass through the CCCs IT assessment for stream 3." What does that mean exactly?	**A. 146** When applying through Stream 3, it is actually the SaaS publisher that is required to onboard and be assessed by CCCS though the IT Security Assessment Program. VARs are not typically required to do so; however if they have any hand in the processing and storage of GC data, then they may be required to undergo an assessment as well.
Q. 147 There is a published list of Interested Suppliers – is this something that everyone who responds to the RFSA should be on?	**A. 147** No, it is not necessary to join the list of interested suppliers. This list in primarily intended for businesses to increase their visibility and opportunity for potential networking, however it has no impact on a vendor's assessment though the RFSA.
Q. 148 Annex I SRCL for SaaS – when do we fill this in?	**A. 148** This is the blanket SRCL that will apply to SAs awarded through the process, and any resulting contracts. Clients may have security requirements above and beyond what is represented here, in which case they will attach a specific SRCL to their resulting contract. There is no action required by the vendor with respect to Annex I.
Q. 149 Annex O seems to be new. Do we need to fill this in now or later in the process?	**A. 149** Annex O is an optional annex that has been added so that vendors may submit additional terms for GC review that would not otherwise fit within the scope of Annex D. If you have no terms beyond what is already represented in Annex D, then a submission of Annex O is not required.
Q. 150 Can activities such as a written report or verbal debrief to the client be classified as advisory services under SaaS Solutions?	**A. 150** It is not enough that the professional services be related to the SaaS solution(s) on offer, their direct purpose should be in standing up the Solution(s). When it comes to advisory services, the scope is limited to advice on how to use and configure the SaaS solution. If the professional services are not solely dedicated to supporting the SaaS use, they would not be permitted on our vehicle.
Q. 151 In order to exclude indirect damages; would Canada be willing to amend section 13.1?	**A. 151** The Limitation of Liability has been created in consultation with industry, and under the direction of TB policy. Canada is not willing to consider revisions to the Public Cloud Software as a Service Limitation of Liability at this time.
Q. 152 In Annex B Section 14 Privacy Compliance and Annex B Section 5 Auditing Compliance for Security Obligations, is the audit report required here if already available through the SOC II report?	**A. 152** Yes, as per Annex B section 5 (a) suppliers must have audits performed at least annually as per the mandatory ISO certifications. These audit(s) generate an audit report that must be made available to Canada on request, as per section 5(d). Canada may choose not to request the annual audit report; however, it must be conducted annually and made available to Canada upon request.
Q. 153 In Annex B Flow Down of Security & Privacy Obligations; will Canada provide exception to this obligation if Sub processors only process encrypted data without access to the encryption key?	**A. 153** As stated in Annex B - Flow-Down of Security & Privacy obligations states "to the extent applicable to each Supplier, Subcontractor and Sub processor" therefore although the sub processors do not have access to the encryption key, they still do have access to the

QUESTIONS	ANSWERS
	encrypted data. The obligations continue to flow downwards to the extent possible and we are not in a position to grant an exception on this requirement.
Q. 154 As per Annex B, Flow-Down of Security & Privacy Obligations, will Canada accept us to be compliant if a sub-processor already meets the security & privacy obligations with Canada in another agreement?	**A. 154** The Security & Privacy Obligations of this solicitation and its resulting SaaS Supply Arrangements may differ from the security & privacy obligations of other agreements between Canada and a supplier or its sub-processors. As such, Canada will not consider the Security & Privacy Obligations of the SaaS RFSA to be met by way of another agreement. Annex B – Security & Privacy Obligations represent ongoing obligations of Suppliers and its Subcontractor(s) and Sub-processor(s) during the period of the Supply Arrangement, rather than qualification requirements that must be demonstrated prior to the award of an SA. Annex B – Security & Privacy Obligations, specifically Flow-Down from the Security & Privacy obligations, outlines the Security and Privacy obligations that the Supplier must flow-down to it's Subcontractor(s) and Sub-processor(s). Canada will only consider a Supplier compliant with the conditions set forth within Annex B – Flow-Down of Security & Privacy Obligations if the Supplier, it's Subcontractor(s), and Sub-processor(s) meet all of the Security and Privacy obligations set forth in Annex B for the period of the Supply Arrangement.
Q. 155 In Annex F – Resulting Contract Clauses; would Canada be willing to amend section 4.1(e) Usage Grant to include the word "supported" in front of "devices and operating environments"?	**A. 155** As device(s) is already defined, Canada does not feel it is necessary to include "supported" in front of the aforementioned language.
Q. 156 In Appendix C to Annex F – Security Obligations section 1(b) Change Management; can Canada confirm that notice of improvements can done be through a support website?	**A. 156** As per the language in 1(b) "the contractor must advise Canada"; indicating that Canada should be directly informed of the changes. The onus must not fall on Canada to validate a support website for the notice of improvement(s).

3.0 Modify the RFSA as follows:

3.1 Section 1.3 of Part 1 – General Information is hereby deleted and replaced with the following:

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) **Stream 1** will include 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) **Stream 2** will include 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) **Stream 3:** will include Submissions from Value-Added Resellers of SaaS Solutions and Services. Value-Added Resellers who intend to present a Submission to qualify as a Supplier must comply with Annex A, Qualification Requirements, Tier 1 for up to Protected A and must submit certifications from the SaaS Publisher, in accordance with the SaaS Publisher Authorization Form (Form 3), to certify that the Supplier has been authorized to supply the SaaS Solution Publisher's Solution(s). **Value-Added Resellers will not be permitted to qualify under Protected B.**

(d) **Stream 4:** will include Submissions from Suppliers or Value-Added Resellers with SaaS Solutions and Services that comply with Canada's requirement for storing and processing unclassified information.

Canada began reviewing Submissions received under Stream 1, 2 and 3 on June 17, 2019, and began reviewing Submissions received under Stream 4 on February 21, 2022.

Assessments may be prioritized based on client requirements in order to best meet the needs of the Government of Canada.

3.2 Section 1.4 of Part 1 – General Information is hereby deleted and replaced with the following:

Security Requirements

There are security requirements associated with this RFSA, in particular as described in Annex A - Qualification Requirements, Annex B - Security & Privacy Obligations, Annex G – Security Requirements for Canadian Contractor, Annex H – Security Requirements for Foreign Contractor, Annex I – SRCL for SaaS, Annex J – SRCL Security Classification Guide, Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process, 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.

3.3 Section 2.6 of Part 2 – Supplier Instructions is hereby deleted and replaced with the following:

Suppliers

(a) **SaaS Publishers:** SaaS Publishers are eligible to qualify under Stream 1, 2, and 4 of this RFSA. SaaS Publishers must submit the SaaS Publisher Certification Form (Form 2) to certify their SaaS ownership rights. Cloud Service Providers (CSPs) who are also Software as a Service (SaaS) Publishers must submit SaaS Publisher Certification Form (Form 2) for their own SaaS and the SaaS Publisher Authorization Form (Form 3) for third party hosted SaaS, as applicable.

(b) **Value-Added Resellers**: Value-Added Resellers (VARs) are eligible to qualify under Stream 3 and 4 of this RFSA. VARs must submit the SaaS Publisher Authorization Form (Form 3) to demonstrate their authority to supply the SaaS to Canada.

3.4 Section 3.2 (iv) of Part 3 – Submission Preparation Instructions is hereby deleted and replaced with the following:

Substantiation of Compliance with Qualification Requirements: Unless applying under Stream 4, 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.

3.5 Section 3.2 (vii) of Part 3 – Submission Preparation Instructions is hereby deleted and replaced with the following:

Compliance with Annex B – Security & Privacy Obligations. Unless applying under Stream 4, Suppliers must comply with the obligations contained in Annex B – Security & Privacy Obligations when presenting a Submission and for the duration of their Supply Arrangement. Suppliers must demonstrate that they meet the security and privacy obligations detailed in Annex B by responding to the mandatory requirements detailed in Annex A – Qualification Requirements, Tier 1 & Tier 2 (as applicable). Suppliers may be requested to demonstrate their ongoing compliance with Annex B – Security & Privacy Obligations upon request throughout the period of any Contract issued against the Supply Arrangement.

3.6 Section 3.5 (b) and (c) of Part 3 – Submission Preparation Instructions are hereby deleted in their entirety.

3.7 Section 3.6 (e) of Part 3 – Submission Preparation Instructions is hereby deleted and replaced with the following:

CCCS Conducts Clearance Process: PSPC has an arrangement with the Canadian Centre for Cyber Security (CCCS) to process security clearances in parallel with the SaaS IT Security (ITS) Assessment, and does not control the process itself. It can be a lengthy process and Suppliers should initiate it as soon as possible. Suppliers will only be onboarded by CCCS once a Submission has been made which includes all necessary information and documents as detailed in Form 5, including acceptance of the terms and conditions of the Supply Arrangement and the Resulting Contract Clauses by way of a signed Form 1, and only during a published onboarding wave. This process is not required for Submissions under Stream 4; client departments who have a requirement to procure Solutions under Stream 4 will be responsible for conducting their own IT

Security and Supply Chain Integrity Assessments. For additional information on the SaaS ITS Assessment process, Suppliers should refer to Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process.

3.8 Section 6.3 of Part 6 – Supply Arrangement is hereby deleted and replaced with the following:

There are security requirements associated with this SA, in particular those described in security requirements, as described in Annex A - Qualification Requirements, Annex B - Security & Privacy Obligations, Annex G – Security Requirements for Canadian Contractor or Annex H – Security Requirements for Foreign Contractor, and Annex F - Resulting Contract Clauses, including its Appendices of the RFSA # EN578-191593/F. The SaaS Services and Work to be procured under this SA may also be subject to additional security requirements, depending on the clients' individual needs as detailed in the bid solicitation, contract and/or task authorization.

3.9 Section 6.5(e) of Part 6 – Supply Arrangement is hereby deleted and replaced with the following:

The quarterly reporting periods are defined as follows:

Quarter	Period	Due Date
1	April 1 to June 30	July 31 of the same year
2	July 1 to September 30	October 30 of the same year
3	October 1 to December 31	January 31 of the same year
4	January 1 to March 31	April 30 of the same year

3.10 Section 6.6 (d) of Part 6 – Supply Arrangement is hereby deleted and replaced with the following:

When submitting a request to amend Annex C, Suppliers must indicate the changes that are included in the revised Annex C, as well as any new SaaS Solutions or Services that are being added. All new Protected A and Protected B SaaS Solutions or Services will be subject to assessment by the Canadian Center for Cyber Security (CCCS).

3.11 Section 6.9 of Part 6 – Supply Arrangement is hereby deleted in its entirety, and the numbering for all subsequent sections in Part 6 are to be updated accordingly.

3.12 Annex A, Tier 2, M10 is hereby deleted and replaced with the following:

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 parties would include, for example, technicians who might be deployed to maintain the Commercially Available Software as a Services of the Supplier that have been proposed by the Supplier. **Please note:** Suppliers are advised that subsequent procurement Streams 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: (a) subcontractors to the Supplier; (b) subcontractors to subcontractors of the Supplier down the chain; or (c) any subsidiaries. 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 the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

3.13 Annex E – SaaS Bid Solicitation Template, Annex "X" Electronic Payment Instruments is hereby deleted and replaced with the following:

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

(a) Direct Deposit (Domestic and International);

(b) Electronic Data Interchange (EDI);

(c) Wire Transfer (International Only);

(d) Large Value Transfer System (LVTS) (Over $25M); or

(e) Acquisition Card (Visa or MasterCard), to the extent that this type of payment is made commercially available by the Contractor as a payment method;

3.14 Section 2.0 of Annex G – Security Requirements of Canadian Contractors entitled is hereby deleted and replaced with the following

The **Contractor/Sub-processor/Subcontractor** personnel requiring access to PROTECTED information, assets or sensitive 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 Contract Security Program/PWGSC.

3.15 Section 5.0 of Annex G – Security Requirements of Canadian Contractors entitled is hereby deleted and replaced with the following

The **Contractor/Sub-processor/Subcontractor** must comply with the provisions of the:

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

3.16 Table 3 of Annex J – Security Classification Guide is hereby deleted and replaced with the following:

Summary of clearance and assessment levels required:

	Designated Organizational Screening (DOS) Any Personnel with **NO** privileged roles and unrestricted logical access to GC assets within the Contractor services	**Designated Organizational Screening (DOS)** Any Personnel **WITH** privileged roles and unrestricted logical access to GC assets within the Contractor services	**Document Safeguarding Capabilities (DCS)**
Stream 1 up to Protected B (SaaS Publisher)	Reliability*	Secret	Protected B
Stream 2 up to Protected A (SaaS Publisher)	Reliability*	Secret	Protected A
Stream 3 up to Protected A (Value Added Reseller)	Reliability*	Secret	Protected A
Stream 4 Unclassified (SaaS Publisher or Value Added Reseller)	N/A	N/A	N/A

*or equivalent

3.17 Annex K - PSPC Non-Disclosure Agreement related to Supply Chain Integrity of solicitation EN578-191593/F is hereby deleted in its entirety.

3.18 Annex N – List of Approved PSPC and Client Authorities is hereby deleted in its entirety and replaced with the following:

Authorized client authorities		
Authorized client department or agency	**User agreement effective date**	**Prime contact**
Administrative Tribunals Support Service of Canada	2021-02-16	Danielle Gudbranson (danielle.gudbranson@tribunal.gc.ca)
Canada School of Public Service	2021-03-17	Anick Matthieu (anick.matthieu@csps-efpc.gc.ca)
Canadian Armed Forces – Directorate of Aerospace Procurement	2021-03-29	Donald Godbout (donald.godbout@forces.gc.ca)
Canadian Food Inspection Agency	2021-05-18	Lisa Chaykowski (lisa.chaykowski@inspection.gc.ca)
Canadian Institutes of Health Research	2021-06-21	Julie Morin (julie.morin@cihr-irsc.gc.ca)
Canadian Revenue Agency	2021-06-24	Di Chen (di.chen@cra-arc.gc.ca)
Correctional Services Canada	2021-03-12	Elizabeth Wheeler (elizabeth.wheeler@csc-scc.gc.ca)
Canadian Space Agency	2021-10-13	Jean-Denis Bisson (jean-denis.bisson@canada.ca)
Department of Finance Canada	2021-09-09	Nick Plettenberg-Dussault (nicholas.plettenberg-dussault@fin.gc.ca)
Department of National Defence, Assistant Deputy Minister (Finance)	2022-01-19	Caleb Wallace (ADMFinProcurement-ApprovisionnementSMAFin@forces.gc.ca)
Department of National Defence – ADM (HR-Civ) DGHRSD	2021-08-18	Emely Ospino (emely.ospino@forces.gc.ca)
Elections Canada	2021-01-20	Adrian Bennett (adrian.bennett@elections.ca)
Environment and Climate Change Canada	2021-02-26	Josee Francoeur (josee.francoeur@canada.ca
Fisheries and Oceans Canada	2021-12-09	Jason Picco (jason.picco@dfo-mpo.gc.ca)
Global Affairs Canada	2021-03-28	Elena DiCola (elena.dicola@international.gc.ca)
Global Affairs Canada, Platform Corporate Services, AAD	2021-11-08	Alexander Jeske (alexander.jeske@international.gc.ca)
Health Canada / Public Health Agency of Canada	2020-11-23	Jesse Arsenault (jesse.arsenault@canada.ca)
Immigration, Refugees and Citizenship Canada – Administration, Security, and Accommodations	2021-06-16	Jodie Thomas (jodie.thomas@cic.gc.ca)
Immigration, Refugees and Citizenship Canada – IT Branch	2020-11-30	Jean-Bernard Tessier (jean-bernard.tessier@cic.gc.ca)
Indigenous Services Canada, Population Health and Primary Care Directorate	2021-12-20	Stuart Malcolm (stuartleroy.malcolm@sac-isc.gc.ca)
Natural Resources Canada	2021-04-01	Leanne Callery (leanne.callery@canada.ca)
Parks Canada	2021-09-01	Pat Alguire (pat.alguire@canada.ca)
Privy Council Office	2021-12-01	Adam Rouleau (adam.rouleau@pco-bcp.gc.ca)
Public Service Commission	2021-05-20	Guillaume Gagnon (guillaume.gagnon2@canada.ca)

Public Services and Procurement Canada, Applications and Software Procurement Directorate	2020-11-10	Jacob Guillot (jacob.guillot@tpsgc-pwgsc.gc.ca)
Public Services and Procurement Canada – Departmental Acquisition Services	2021-06-08	Marlee Diamond (marlee.diamond@tpsgc-pwgsc.gc.ca)
Public Services and Procurement Canada - Human Resources Branch	2021-02-28	Vanessa Primeau (vanessa.primeau@tpsgc-pwgsc.gc.ca)
Public Services and Procurement Canada - Real Property Services Branch & Property and Facility Management Service Line & Operations and Emergency Management Directorate	2021-03-08	Martin Audette (martin.audette@tpsgc-pwgsc.gc.ca)
Royal Canadian Mounted Police	2021-05-06	Crystal Rodger (crystal.Rodger@rcmp-grc.gc.ca)
Statistics Canada	2020-11-17	Marie-Lyne Carr (marie-lyne.carr@canada.ca)
Veterans Affairs Canada	2021-02-19	Susan O'Brien (susan.obrien@canada.ca)

3.19 Form 5 - Submission Completeness Review Checklist of solicitation EN578-191593/F is hereby deleted in its entirety and replaced with the editable version under the Attachments section of the Tender Notice page: RFSA - SaaS Method of Supply (GC Cloud) (EN578-191593/F).

3.20 Form 6 - SCI Submission Template of solicitation EN578-191593/F is hereby deleted in its entirety.

3.21 Section 7.2 (c) of Annex F – Resulting Contract Clauses is hereby deleted and replaced with the following:

Total Default: If, in Canada's reasonable opinion, the Contractor's default is a total or material breach of the Contract, Canada may immediately terminate the Contract by the Notice. For clarity, Canada's opinion may be based on circumstances including but not limited to:

(i) the Contractor's non-performance of a material contract obligation;

(ii) the Contractor irrefutably appears unable to perform a material contract obligation, due to factors beyond the Contractor's control. For clarity, this includes, actual or apparent insolvency, repeated failure to produce acceptable deliverables under this or other similar contracts with Canada,

(iii) the Contractor's multiple or repeated, uncured breach of an intermediate contract obligation(s), and

(iv) the Contractor's default adversely impacting government operations.

3.22 Section 8 of Annex F – Resulting Contract Clauses entitled "Work" is hereby amended to insert the following:

All clauses related to Work apply to Work as defined in Appendix B and not to the Services.

3.23 Section 8.5 (b) of Annex F – Resulting Contract Clauses is hereby deleted and replaced with the following:

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 reasonably 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, to the extent that these services are made commercially available to other customers . There will be no charge for the services other than those charges set out in the Basis of Payment.

3.24 Section 11.6 of Annex F – Resulting Contract Clauses is hereby deleted and replaced with the following:

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

(a) Direct Deposit (Domestic International);

(b) Electronic Data Interchange (EDI);

(c) Wire Transfer (International Only);

(d) Large Value Transfer System (LVTS) (Over $25M); or

(e) Acquisition Card (Visa or Master Card), to the extent that this type of payment is made commercially available by the Contractor as payment method

3.25 Section 15 of Annex F – Resulting Contract Clauses entitled "Suspension of work" is hereby amended to capitalize "Work" in the title. The content of Section 15 including clauses (a), (b), and (c) remain unchanged.

3.26 In Appendix B – Definitions and Interpretations, delete the term "Client Data" and its definition, and replace with the following:

"Client/Customer 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.

3.27 In Appendix B – Definitions and Interpretations, insert the term "Work" and its definition, and replace with the following:

"Work"	All efforts made to produce a deliverable or to perform or provide a service that the supplier must offer under the terms of the Contract.

3.28 Section 11 (b) of Appendix C – Security Obligations is hereby deleted and replaced with the following:

If applicable, the Contractor must have a supply chain risk management approach including a Supply Chain Risk Management (SCRM) Plan that is aligned with one of the following best practices described under the Annex A – Qualification Requirements - Supply Chain Risk Management, mandatory requirement ID; M7 of Tier 1 and M11 of Tier 2:

(i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for Contractor relationships (Parts 1 to 4);

(ii) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations;

(iii) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan; or

(iv) CSA STAR controls to support CSA CCM Supply Chain Management controls.

3.29 Appendix F – SRCL for SaaS is hereby deleted and replaced with the following:

Note to Contractors: Different or additional security levels may apply to Clients using the Supply Arrangement (SA) or their Work requirements, for example, security clearances for Suppliers or Supplier resources. For all Contracts issued against a SA, Clients are required to submit their SRCL to the Contract Security Program: TPSGC.SSILVERS-ISSSRCL.PWGSC@tpsgc-pwgsc.gc.ca prior to Contract award. The Contracting Authority must reference the RFSA – SaaS Method of Supply (GC Cloud) (EN578-191593/F) when submitting their SRCL to the Contract Security Program. In the event that a Contract issued against a SA includes different or additional security levels, they will be included in Appendix F (SRCL for SaaS) and Appendix G (Security Classification Guide) to the Contract.

4.0 Minor administrative changes that do not affect the meaning and impact of the terms and conditions made throughout.

5.0 Solicitation EN578-191593/F is hereby deleted in its entirety and replaced with a new version that incorporates Amendment 001 to Amendment 017:

Please find attached in this amendment the following documents containing modifications to the RFSA solicitation documents:

1. RFSA – SaaS Method of Supply (GC Cloud) – (EN) – Amendment 017;
2. Part 6 – Supply Arrangement – (EN) – Amendment 017; and
3. Annex F – SaaS Resulting Contract Clauses – (EN) – Amendment 017.

PUBLIC SERVICES AND PROCUREMENT CANADA (PSPC)

REQUEST FOR SUPPLY ARRANGEMENT (RFSA) FOR

SOFTWARE AS A SERVICE (SAAS)

GOVERNMENT OF CANADA METHOD OF SUPPLY

(GC CLOUD)

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 the 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.

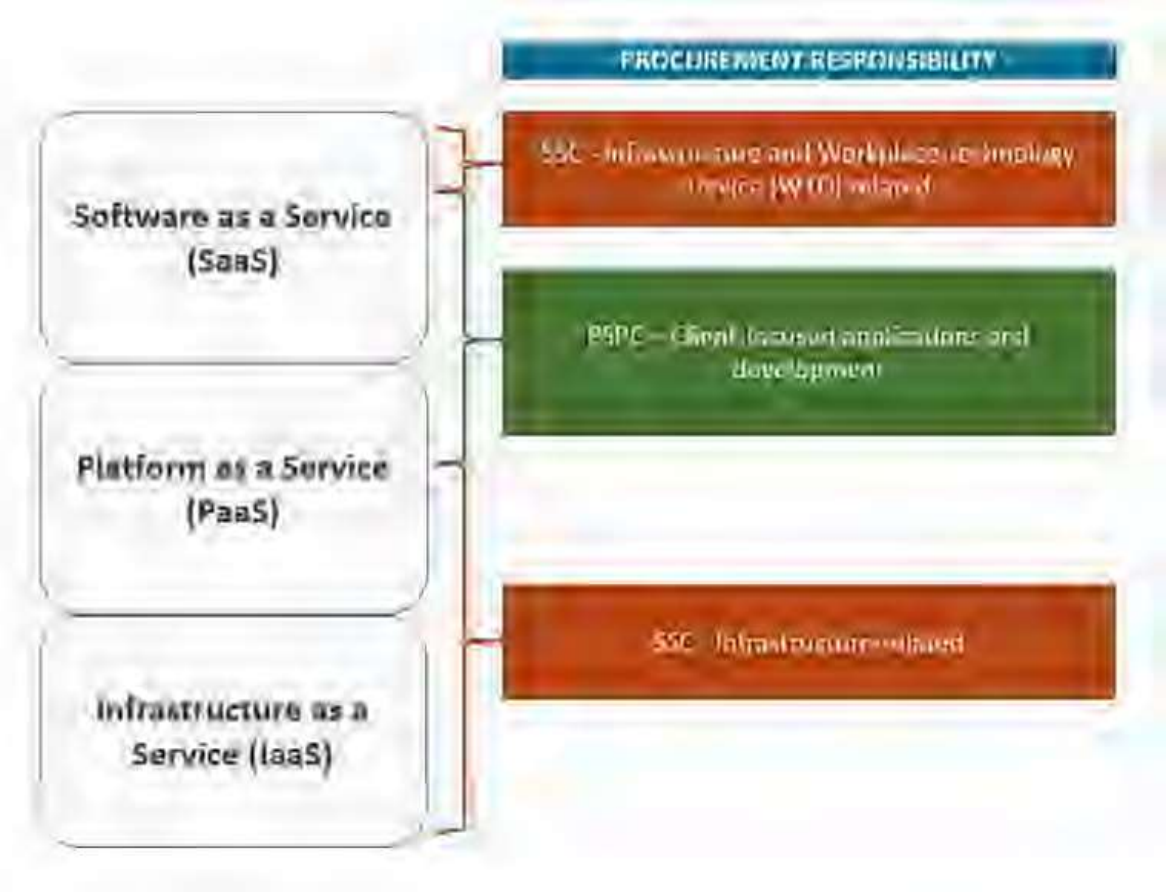
On September 7, 2018, Shared Services Canada (SSC) published an Invitation to Qualify (ITQ) as the first Stream of the procurement process for the GC Cloud Services Procurement Vehicle (https://buyandsell.gc.ca/procurement-data/tender-notice/PW-18-00841719). In parallel, PSPC issued a Request for Information (RFI) on October 29, 2018 to seek feedback from the industry on the 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 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, and 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, SaaS Solutions and Ceiling Prices, SaaS Service Level Agreement (SLA), the SaaS Bid Solicitation Template, Resulting Contract Clause, Security Requirements for Canadian Contractor, Security Requirements for Foreign Contractor, SRCL for SaaS, Security Classification Guide, PSPC Non-Disclosure Agreement related to Supply Chain Integrity, SaaS IT Security (ITS) Assessment Program onboarding process, Supply Arrangement Quarterly Reports Template, and List of Approved PSPC and Client Authorities.

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 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.

(k) Include SACC Manual clause S3037T - Applicability of COVID-19 vaccination requirements to individual solicitations if any individual solicitations under the resulting supply arrangement may be subject to the COVID-19 Vaccination Policy for Supplier Personnel.

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) **Stream 1** will include 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) **Stream 2** will include 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) **Stream 3:** will include Submissions from Value-Added Resellers of SaaS Solutions and Services. Value-Added Resellers who intend to present a Submission to qualify as a Supplier must comply with Annex A, Qualification Requirements, Tier 1 for up to Protected A and must submit certifications from the SaaS Publisher, in accordance with the SaaS Publisher Authorization Form (Form 3), to certify that the Supplier has been authorized to supply the SaaS Solution Publisher's Solution(s). **Value-Added Resellers will not be permitted to qualify under Protected B.**

(d) **Stream 4:** will include Submissions from Suppliers or Value-Added Resellers with SaaS Solutions and Services that comply with Canada's requirement for storing and processing unclassified information.

Canada began reviewing Submissions received under Stream 1, 2 and 3 on June 17, 2019, and began reviewing Submissions received under Stream 4 on February 21, 2022.

Assessments may be prioritized based on client requirements in order to best meet the needs of the Government of Canada.

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, Annex G – Security Requirements for Canadian Contractor, Annex H – Security Requirements for Foreign Contractor, Annex I – SRCL for SaaS, Annex J – SRCL Security Classification Guide, Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process, 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 are 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 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 Submission;
(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 Submission;
(v) failure of the Supplier to properly identify the Submission;
(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.

(d) **Submission of Confidential Information.** Suppliers are asked to mark all confidential information included in their Submission as confidential. The confidential information must be clearly identified by marking each page containing such information as "Confidential" and by highlighting all confidential information therein.

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 FCP for employment equity, the bid solicitation and resulting contract templates would include such specific requirements. Further information on the 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 Supply Arrangement (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 qualify under Stream 1, 2, and 4 of this RFSA. SaaS Publishers must submit the SaaS Publisher Certification Form (Form 2) to certify their SaaS ownership rights. Cloud Service Providers (CSPs) who are also Software as a Service (SaaS) Publishers must submit SaaS Publisher Certification Form (Form 2) for their own SaaS and the SaaS Publisher Authorization Form (Form 3) for third party hosted SaaS, as applicable.

(b) **Value-Added Resellers**: Value-Added Resellers (VARs) are eligible to qualify under Stream 3 and 4 of this RFSA. VARs must submit the SaaS Publisher Authorization Form (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 Requirements
Section V: Security Clearance Requirements

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 Request for Supply Arrangement (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. By presenting a Submission, the Supplier agrees to accept the terms and conditions of the Supply Arrangement, including the Resulting Contract Clauses, as per Form 1. Submissions that do not include a signed Form 1 will not be assessed by CCCS until the GC has received a signed copy of Form 1.

(ii) **SaaS Publisher as Supplier Form**: Form 2 (if applicable) – If the Software as a Service (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**: Unless applying under Stream 4, 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 (SLA):** Suppliers must submit their published service level agreements (SLA), to be included in Annex D – SaaS Solution Service Level Agreements (SLA). Any terms contained in Annex D – SaaS Solution SLA which include pricing information, such as (but not limited to) those that attempt to impose financial conditions, pricing terms, or compliance penalties, shall be deemed stricken and are of no force or effect.

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 identify the SaaS Solution and corresponding SLA.

Only terms and conditions in the SLA related to service levels and service delivery will apply. Any terms and conditions of the SLA not related to service levels and service delivery, as detailed below, will be deemed stricken and will not apply.

Terms and conditions related to service levels and service delivery under the SLAs must include the following:

A. Period during which the Contractor will provide warranty and support;
B. Support services availability;
C. Contact and procedure information for accessing support;
D. Errors – severity level definitions;
E. Procedures for resolution of problems;
F. Response times;
G. Procedures on how and when all telephone, fax or email communications will be responded to;
H. Escalation path and procedures;
I. Downtime definition, scheduled and unscheduled;
J. Available disaster recovery system;
K. Service credits – triggers and calculation; and,
L. Maintenance entitlements (e.g. patches, updates, major/minor releases, etc.).

(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.

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

(vii) **Compliance with Annex B – Security & Privacy Obligations.** Unless applying under Stream 4, Suppliers must comply with the obligations contained in Annex B – Security & Privacy Obligations when presenting a Submission and for the duration of their Supply Arrangement. Suppliers must

demonstrate that they meet the security and privacy obligations detailed in Annex B by responding to the mandatory requirements detailed in Annex A – Qualification Requirements, Tier 1 & Tier 2 (as applicable). Suppliers may be requested to demonstrate their ongoing compliance with Annex B – Security & Privacy Obligations upon request throughout the period of any Contract issued against the Supply Arrangement.

(viii) **Software Usage Rights (SUR):** Suppliers may submit additional software usage rights terms not addressed within Annex F – Resulting Contract Clauses to be included in Annex O – SaaS Software Usage Rights (SUR). Any terms contained in Annex O – SaaS SUR which include pricing information, such as (but not limited to) those that attempt to impose financial conditions, pricing terms, or compliance penalties, shall be deemed stricken and are of no force or effect.

Proposed supplemental terms service must be limited to standard terms typically provided to commercial customers who provision the SaaS Solution.

SURs 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 SUR documents, the Supplier must clearly identify the SaaS Solution and corresponding SUR.

If Canada determines that any proposed software usage rights term is unacceptable to Canada, Canada will provide the Supplier with an opportunity to remove that provision form its submission, or to propose alternate language for consideration by Canada. Whether or not any proposed additional software usage rights terms are accepted and incorporated into any resulting Supply is solely within the discretion of Canada.

Terms and conditions included in the related to software usage rights under the SURs may include, but are not necessarily limited to, the following:

A. Defining authorized users;
B. Access and use rights;
C. Access and use restrictions;
D. Use verification/audit rights;
E. Warranty disclaimers;
F. Indemnification in the case of customer misuse;
G. Customer obligations/responsibilities.

3.3 Section II: Financial Submission

(a) In the Financial Submission, Suppliers must submit a list of proposed SaaS Solutions and related Professional Services (as described in subsection (b) below), with their ceiling prices and applicable percentage discount against their commercial pricing. Suppliers must choose one of the following options for submitting their SaaS Solutions and Professional Services ceiling prices in Annex C - SaaS Solutions and Professional Services Ceiling Prices:

(i) Option 1: Suppliers provide a link to their commercially-available SaaS catalogue and indicate the percentage discount offered to Canada; or,

(ii) Option 2: Supplier complete the table in Annex C - SaaS Solutions and Professional Services Ceiling Prices listing their ceiling prices for SaaS Solutions and Professional Services.

Where a link is provided to an online catalogue in accordance with option 1, Canada reserves the right to request that the Supplier include in their online catalogue all of the information requested in sub-

section (d) below. Where a table is provided in accordance with option 2, Canada reserves the right to request that Suppliers make this information available via an online catalogue in the future. Any pricing information included elsewhere in the Supplier's Submission, including in Annex D – SaaS Solution Service Level Agreements and Annex O – Software Usage Rights, shall be deemed stricken and is of no force or effect.

(b) Professional Services to be acquired through the RFSA are limited to the following: Quick Start Guide ("QSG") training and services, implementation services, training services, data cleansing, migration and transition services, and advisory services. However, where a link is provide to an online catalogue in accordance with option 1, Suppliers are not required to create a custom catalogue for the RFSA.

(c) **Refresh Period** – Supply Arrangement holders are permitted to update their SaaS Solutions and Professional Services ceiling prices on an ongoing basis.

(i) Suppliers are permitted to submit a new Annex C – SaaS Solutions and Professional Services Ceiling Prices no more frequently than once per month;

(ii) Where a link is provided to an online catalogue in Annex C – SaaS Solutions and Professional Services Ceiling Prices, Suppliers shall be permitted to update their online catalogue as often as necessary providing they notify the Supply Arrangement prior to the release of a new version; and,

(iii) All SaaS Solutions and Professional Services ceiling prices are subject to review and price support may be requested by the Supply Arrangement Authority at any time during the period of the SA. All new SaaS Solutions or Services will be subject to assessment by the Canadian Center for Cyber Security (CCCS). No amendment to Annex C – SaaS Solutions and Professional Services Ceiling Prices will be issued unless and until Canada has reviewed and accepted any new SaaS Solutions and Services Supply Chain Security Information (SCSI).

(d) 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. The following should be addressed in the Supplier's **SaaS Solutions and Professional Services Ceiling Prices**:

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

(ii) **SaaS Solution's or Professional Services Name:** Suppliers must provide the commercial name that the SaaS Publisher uses to identify the SaaS Solution or Professional Services 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 Professional Services 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 or Professional Services Ceiling Prices (such as “per user”, “per entity”, “per diem” etc.) under which the SaaS Solutions and Professional Services 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 and Professional Services are available, designated as “EN” for English, “FR” for French, or “EN, FR” for both;

(ix) **SaaS Solution Product Description:** Suppliers may enter a brief description of the SaaS Solution.

(x) **SaaS Solution Information:** Suppliers may provide a web site URL containing information on the SaaS Solution or Professional Services.

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

(e) **Price support**: 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;

(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 Requirements

Suppliers must meet the Supply Chain Integrity (SCI) requirements outlined in Annex A – Qualification Requirements, M6 and M7, Tier 1 for up to Protected A and M10 and M11, Tier 2 for up to Protected B (Supply Chain Management) of the RFSA. The requirements must be met before a Supply Arrangement is awarded.

3.6 Section V: Security Clearance Requirements

(a) **Security Clearance Requirements**: The Supplier must meet the security clearance requirements described in the requirements outlined in Annex A – Qualification Requirements, M4, Tier 1 for up to Protected A and M7, Tier 2 for up to Protected B (Personnel Security) of the RFSA. The requirements must be met before a Supply Arrangement is awarded.

(b) **Contractor/Sub-processor/Subcontractor:** Contractor/Sub-processor/Subcontractor must meet the security requirements outlined in Annex G – Security Requirements for Canadian Contractor, Annex H – Security Requirements for Foreign Contractor, Annex I – SRCL for SaaS and Annex J – Security Classification Guide, as applicable.

(c) **Timing**: Suppliers should take steps to obtain the required security clearance promptly. The security clearance requirements should be met before the award of a Supply Arrangement. Any delay in the award of a Supply Arrangement to allow the Supplier to obtain the required clearance will be at the sole discretion of PSPC.

(d) **Joint Venture Supplier:** Unless otherwise specified in the solicitation, in the case of a joint venture Supplier, each member of the joint venture must meet the security requirements, outlined in (b) above.

(e) **CCCS Conducts Clearance Process**: PSPC has an arrangement with the Canadian Centre for Cyber Security (CCCS) to process security clearances in parallel with the SaaS IT Security (ITS) Assessment, and does not control the process itself. It can be a lengthy process and Suppliers should initiate it as soon as possible. Suppliers will only be onboarded by CCCS once a Submission has been made which includes all necessary information and documents as detailed in Form 5, including acceptance of the terms and conditions of the Supply Arrangement and the Resulting Contract Clauses by way of a signed Form 1, and only during a published onboarding wave. This process is not required for Submissions under Stream 4; client departments who have a requirement to procure Solutions under Stream 4 will be responsible for conducting their own IT Security and Supply Chain Integrity Assessments. For additional information on the SaaS ITS Assessment process, Suppliers should refer to Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process.

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 Request for Supply Arrangement (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 Supply Arrangement (SA).

(d) **Right of Canada:**

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

(ii) 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) or Annex O – Software Usage Rights (SUR). No SA will be awarded unless and until Canada has approved all such terms and conditions;

4.2 Technical and Financial Evaluation

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) Annex C - SaaS Solutions and Professional Services Ceiling Prices as per Article 3.3 (a), (b), (c) and (d); and
(ii) Price support as per Article 3.3 (e).

4.2.3 Mandatory Security Evaluation

The mandatory security requirements are as follows:

(i) Organization and personnel clearances (as per Annex G – Security Requirements for Canadian Contractor, Annex H – Security Requirements for Foreign Contractor, Annex I – SRCL for SaaS and Annex J – SRCL Security Classification Guide for the RFSA, as applicable);

(ii) Supply Chain Integrity assessment (as per 4.3); and,

(iii) SaaS IT Security (ITS) Assessment.

4.3 Supply Chain Integrity Process

(a) SCI is examined during the SaaS ITS Assessment. SCI assessments are another level of assurance to confirm that implemented security controls are less likely to be maliciously undermined by threat actors through supply chain attacks.

(b) For SaaS providers, the SCI process initiated by Shared Services Canada (SSC) is used. In this process, the SaaS provider gives a list of the software, hardware, contractors, and suppliers that are used to deliver the service offering. The provider also updates the Government of Canada (GC) periodically to note any changes to the initial list. If the GC determines that the list of software, hardware, contractors, and suppliers is extensive, SCI safeguards may be required.

(c) **SCI Process:** PSPC has an arrangement with the Canadian Centre for Cyber Security (CCCS) to process the SCI assessment in parallel with the IT Security Assessment, and as such PSPC does not control the process. Suppliers will only be onboarded by CCCS once a Submission has been accepted by PSPC, and only during published onboarding waves. For additional information on the SaaS ITS Assessment process, Suppliers should refer to Annex L: SaaS IT Security (ITS) Assessment Program: Onboarding Process.

(d) For additional information on security requirements, Bidders should refer to: contact@cyber.gc.ca.

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 Supply Arrangement (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 Request for Supply Arrangement (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

The Supply Arrangement is 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 through a SaaS product catalogue (herein after referred to as the SaaS Catalogue).

6.2 Disclosure and Publication of Supply Arrangement

(a) It is a condition of the Supply Arrangement (SA) that Canada has the right to disclose and publish the entire contents of the SA, including ceiling price information, on the government Intranet. Canada will attempt to limit access to price lists to the government Intranet but cannot guarantee the confidentiality of information stored on any network device such as the Internet, an extranet, a virtual private network (VPN), an inter-network, or such other means as may become possible from time to time so that there could be "universal access rights" from any location, whether their means of access is secure, wireless, mobile or by any other means available.

(b) The Supplier further agrees that it will have no right of claim against Canada, the Minister, Clients, employees, agents or servants, or any of them, in relation to disclosure of the information contained in the SA as a result of establishing the SaaSSA catalogue, and will indemnify Canada, the Minister, Clients, employees, agents or servants, and any of them, against any action, suit, demand, right or claim asserted by anyone as a result of such disclosure.

(c) Canada will not be liable for any errors, inconsistencies or omissions in any such published information. If the Supplier identifies any errors, inconsistencies or omissions, the Supplier agrees to notify the Supply Arrangement Authority immediately.

6.3 Security Requirements

There are security requirements associated with this SA, in particular those described in security requirements, as described in Annex A - Qualification Requirements, Annex B - Security & Privacy Obligations, Annex G – Security Requirements for Canadian Contractor or Annex H – Security Requirements for Foreign Contractor, and Annex F - Resulting Contract Clauses, including its Appendices of the RFSA # EN578-191593/F. The SaaS Services and Work to be procured under this SA may also be subject to additional security requirements, depending on the clients' individual needs as detailed in the bid solicitation, contract and/or task authorization.

6.4 Standard Clauses and Conditions

All clauses and conditions identified in this Supply Arrangement 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).

6.4.1 General Conditions

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

6.5 Supply Arrangement Reporting

(a) 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.

(b) The report must be in the format provided in attached Annex M to the Supply Arrangement - Supply Arrangement Quarterly Reports Template. A writable copy of Annex M - Supply Arrangement Quarterly Reports Template is available on the Software Acquisition and Reference Centre (SARC) website at: https://www.tpsgc-pwgsc.gc.ca/app-acq/cral-sarc/saas-eng.html, and under the "Attachments" section at: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EEM-003-35660.

(c) If information is not available, the reason for omission must be indicated. If no contracts are issued during a specific period the Supplier must provide a "NIL" report.

(d) The data must be submitted to the Supply Arrangement Authority on a quarterly basis according to the reporting periods defined below. The Supply Arrangement Quarterly Reports must be submitted to the Supply Arrangement Authority via email to TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca, or made available for download, no later than 30 calendar days after the end of each reporting period.

(e) The quarterly reporting periods are defined as follows:

Quarter	Period	Due Date
1	April 1 to June 30	July 31 of the same year
2	July 1 to September 30	October 30 of the same year
3	October 1 to December 31	January 31 of the same year
4	January 1 to March 31	April 30 of the same year

(f) Failure to provide fully completed reports in accordance with the above instructions may result in the suspension or cancellation of the SA, the removal of the Supplier from the list of qualified Suppliers and/or the application of a vendor performance corrective measure.

6.6 Updating Annex C - SaaS Solutions and Professional Services Ceiling Prices

(a) The Supplier will be permitted to update Annex C - SaaS Solutions and Professional Services Ceiling Prices on an ongoing basis.

(b) Where the Supplier has included in their Submission a copy of the table included in Annex C – SaaS Solutions and Professional Services Ceiling Prices, the Supplier may submit a new version of the table no more frequently than once per month.

(c) Where the Supplier has included a link to their online catalogue, Suppliers shall be permitted to update their catalogue as often as necessary providing they notify the Supply Arrangement Authority prior to the release of a new version.

(d) When submitting a request to amend Annex C, Suppliers must indicate the changes that are included in the revised Annex C, as well as any new SaaS Solutions or Services that are being added. All new Protected A and Protected B SaaS Solutions or Services will be subject to assessment by the Canadian Center for Cyber Security (CCCS).

(e) By submitting a request to amend Annex C, the Supplier is certifying that the change(s) in the amendment request is/are the only change(s) made to the updated Supplier's Annex C - SaaS Solutions and Professional Services Ceiling Prices. If any changes other than the ones identified in the Supplier's amendment request are made to the Annex C - SaaS Solutions and Professional Services Ceiling Prices, the Supplier understands that the Government of Canada may adjust these unidentified changes back at any time or suspend the SA.

(f) All SaaS Solutions and Professional Services ceiling prices are subject to review and price support may be requested by the Supply Arrangement Authority at any time during the period of the SA. If requested price support justifications are not completed and submitted as requested, the Supply Arrangement Authority will provide the Supplier with a time frame within which to meet the requirement. Failure to comply with the request of the Supply Arrangement Authority and meet the requirements within that time period will void the modification request or create delay in processing Supplier's request(s).

(g) Canada reserves the right to reject a request to update Annex C - SaaS Solutions and Professional Services Ceiling Prices as a result of any associated security assessments or price verification. If Canada and the Supplier cannot reach an agreement regarding the requested modifications, the Supplier may elect to remove such products from Annex C - SaaS Solutions and Professional Services Ceiling Prices.

6.7 Updating Annex D – Service Level Agreements (SLA)

(a) The Supplier is 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 the Supplier wishes to add a new SaaS Solution to the Supply Arrangement, the SLA must be resubmitted to the Supply Arrangement Authority for acceptance prior to the SLA(s) being incorporated into the Supply Arrangement.

(b) 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.

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

6.8 Updating Annex O – Software Usage Rights (SUR)

a) The Supplier is permitted to update their SUR on an ongoing basis, providing that the changes to the SUR are acceptable to Canada. Where the Supplier wishes to add a new SaaS Solution to the Supply Arrangement, the SUR must be resubmitted to the Supply Arrangement Authority for acceptance prior to the SUR being incorporated into the Supply Arrangement.

b) Any terms or conditions of the SUR 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 O – SaaS Software Usage Rights (SUR). No terms

purporting to abridge or extend the time to commence an action for breach, tort, or other action are of any effect.

c) Canada reserves the right to reject or negotiate any of the terms and conditions proposed by the Supplier and submitted under Annex O – SaaS Software Usage Rights (SUR). No amendment to Annex O will be awarded unless and until Canada has approved all such terms and conditions.

6.9 Condition to Remain a Qualified Supplier

(a) The Supplier acknowledges that it is a condition of the SA that:

(i) the Supplier (and its Approved Agents and Cloud Service Providers, as applicable) must continue to meet all the qualification requirements described in the RFSA during the Supply Arrangement period; and,

(ii) all certifications made in the Supplier's Submission must be true at the time of the submission and must remain true throughout the Supply Arrangement Period. The Supplier acknowledges that Canada is entitled to verify these certifications throughout the Supply Arrangement Period.

(b) Canada may verify compliance with these conditions at any time during the Supply Arrangement Period and failure to meet any of these conditions constitutes grounds for the suspension of this SA.

(c) Canada may require a Supplier to validate its qualification at any time. For example, the Supply Arrangement Authority may require a Supplier to provide evidence that:

(i) it continues to have the financial capability;

(ii) the Joint Venture membership (if applicable) remains as stated in the SA; and/or,

(iii) it continues to meet the certification requirements for the Set-Aside Program for Aboriginal Businesses (if applicable).

(d) The Supplier must immediately notify the Supply Arrangement Authority if it no longer meets any of the mandatory qualification requirements of this SA.

(e) Where the Supplier no longer meets any of the individual requirements for qualification, the Supply Arrangement Authority may, at its discretion:

(i) suspend the SA in its entirety until the Supplier has demonstrated that it meets the requirements for which it has been found deficient, during which time the Supplier will not be eligible for contracts and solicitations issued under this procurement vehicle; or

(ii) cancel the SA in its entirety, in which case the Supplier may present a new Submission at any time.

6.10 Suspension or Cancellation of a Supply Arrangement

(a) Canada, at its sole discretion, may suspend or cancel the SA if:

(i) Late deliveries occur;

(ii) Complete and accurate Quarterly Usage Reports are not submitted within the required time frames;

(iii) Contracts are accepted from unauthorized parties (those not listed under Annex N - List of Approved PWGSC and Client Authorities);

(iv) The product list includes unauthorized goods (such as hardware, appliances, or Infrastructure/Platform as a Service), or services (such as professional services other than Quick Start Guide services, training, implementation, data cleansing, migration and transition services or advisory services);

(v) Violations of any of the specific terms and conditions detailed in the SA occur;

(vi) Contract(s) awarded against the SA have been terminated for default;

(vii) Canada has imposed measures on the Supplier under the PSPC Vendor Performance Policy (or such similar policy as may be in place from time to time);

(viii) Canada has documented at least three instances of Contract poor performance. An instance of poor performance may include, but is not limited to, late or failed delivery of reports or goods, lack of timely notification given to the Supply Arrangement Authority of changes in the Supplier's Supply Arrangement Representative, security status, and/or non-compliance with invoicing procedures; or

(ix) Information is provided to Clients by the Supplier that conflicts with any aspect of the terms and conditions, pricing, or availability of SaaS Solutions or Services currently listed in the SA.

(b) Removal or Suspension of the Supplier's SA does not affect the right of Canada to pursue other remedies or measures that may be available.

(c) The Supplier acknowledges that Canada has the right to publish information regarding the status of the Supplier's SA, including information related to the suspension, cancellation or withdrawal of Approved Value-Added Reseller(s), if applicable.

6.11 Supplier promotional or marketing literature

The Supplier must notify Canada in advance of any intent to make public an announcement related to the issuance of a SA or the award of Contract(s). Canada reserves the right to request that the Supplier modify any information being provided in a public announcement.

6.12 Period of the Supply Arrangement

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

6.13 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.

6.14 Authorities

6.14.1 Supply Arrangement Authority

The Supply Arrangement Authority is:

Name: Elizabeth Quenville
Title: Supply Team Leader

Public Works and Government Services Canada
Acquisitions Branch
Applications and Software Procurement Directorate

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

Telephone: 873-354-7516
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.

6.14.2 Supplier's Representative

Fill in or delete, as applicable.

6.14.3 Supply Chain Security Authority

The Supply Chain Security Authority for the Contract is:
Name: CCCS SCI team
E-mail address: SCI@cyber.gc.ca

The Supply Chain Security Authority is the CCCS 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.

6.14.4 Privacy Officer

As per Annex B – Security and Privacy Obligations, the Supplier must provide Canada with information that identifies an individual as a Privacy Officer to act as the Contractor's representative for all matters related to the Personal Information and the Records.

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

6.15 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. A List of all approved PSPC and Client authorities are included under Annex N.

6.16 Priority of Documents

If there is a discrepancy between the wordings 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 and Privacy Obligations
(e) Annex E, Bid Solicitation Template;
(f) Annex F, Resulting Contract Clauses;
(g) Annex G, Security Requirements for Canadian Contractor;
(h) Annex H, Security Requirements for Foreign Contractor;
(i) Annex I, SRCL of SaaS;
(j) Annex J, Security Classifications Guide;
(k) Annex K, PSPC Non-Disclosure Agreement related to Supply Chain Integrity;
(l) Annex L, SaaS IT Security (ITS) Assessment Program: Onboarding Process;
(m) Annex M – Supply Arrangement Quarterly Reports Template;
(n) Annex N – List of Approved PWGSC and Client Authorities; and
(o) 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)*.
(p) Annex C, SaaS Solutions and Professional Services Ceiling Prices
(q) Annex D, SaaS Service Level Agreements (SLA)
(r) Annex O, Software Usage Rights (SUR)

6.17 Certifications and Additional Information

6.17.1 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 including those that would continue beyond the period of the SA.

6.18 Applicable Laws

The 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 Public Services and Procurement Canada (PSPC) contracting officers who have been given the authority by PSPC to use the Supply Arrangement (SA) can issue resulting contracts using their existing delegated contract approval and signing authorities.

7.2 Contractor Selection

(a) **Requirements valued at less than $40,000.00 CAD (GST/HST/QST included)**

(i) **Sole Source:** For requirements under **$40,000.00** CAD (applicable taxes included), Canada may choose, at its sole discretion, to direct contracts to a Supplier or to issue contracts following Bid Solicitations.

(b) **Requirements valued at $40,000.00 CAD (applicable taxes included) or greater**

(i) For requirements above **$40,000.00 CAD** (applicable taxes included) where there is only one source of supply, the Client must provide valid sole source limited tendering certification in accordance with the Government Contracting Regulations.

(ii) If only one source of supply exists for the required Software as a Service (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.

(iii) **Bid Solicitation:** For requirements valued at **$40,000.00 CAD** or above, if multiple SaaS Solutions are available from the Government of Canada (GC) SaaS Catalogue that can meet Canada's technical requirements, Canada will issue a bid solicitation to all Supply Arrangement holders who offer a Solution that meets the Client's technical requirements under their Supply Arrangement. 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 Procurement Strategy for Aboriginal Businesses (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.

Note that the splitting of requirements, (i.e. the dividing of a requirement into several lower dollar value requirements) to avoid a higher approval authority is contrary to contracting policy.

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 GETS (www.buyandsell.gc.ca) and may be 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

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.

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).**

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

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
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 (and any Supplier Sub-processors, as applicable) and Canada.	In the document, the Supplier must include, at a minimum, the parties' roles and responsibilities for: (a) Account management; (b) Boundary protection; (c) Asset and information system backup; (d) Incident management; (e) System monitoring; and (f) Vulnerability management.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
M2	**Data Protection**	The physical locations of the Commercially Available Public Software as a Service[1] (which may contain Canada's data) 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 Public Services and Procurement Canada (PSPC) website: http://www.tpsgc-pwgsc.gc.ca/esc-	The Supplier must provide documentation that demonstrates how the proposed Commercially Available Public Software as a Service submitted meets the mandatory requirements outlined in Data Protection Requirement. 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 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 included in the Submission. 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.

[1] For the purposes of this Annex A, Commercially Available Public Software as a Service means a Solution which is available commercially to other customers. As part of their subscription to use the solution, the Supplier undertakes to make available to Canada all the functions and functionalities included in the commercially available version of the solution, as well as the auxiliary IT infrastructure services and requirements necessary for the provision of the solution, all of which is included in the subscription price.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		src/international-eng.html and as updated from time to time.	
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;	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 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		(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 Government of Canada (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.	Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation included in the Submission. 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.
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.	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:

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		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 in writing 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 of, 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 on the reliability of Software as a Services hosting GC assets and data.	(a) system documentation or technical documentation outlining and detailing the security measures including policies, processes 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 for Personnel Security requirements 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 included in the Submission. 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.
M5	**Third Party Assurance**	The Software as a Service (SaaS) must be designed and developed to ensure the security of their proposed Commercially Available Public Software as a Service, including, implementing	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

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		information security policies, procedures, and security controls. Suppliers that have already completed the security assessment by providing to the Canadian Center for Cyber Security (CCCS) their certifications and audit reports, and have already entered into a Non-Disclosure Agreement (NDA) with them, must send their certifications and audit reports directly to CCCS client services at contact@cyber.gc.ca in order to meet this requirement. For suppliers that have not completed the security assessment, the onboarding process will commence once the Submission complies with the requirements of the Request for Supply Arrangements, meets all mandatory technical and financial evaluation criteria, and provides all of the mandatory certifications in order to be declared responsive. PSPC will then refer the Supplier to CCCS client services to begin the onboarding process to the IT Assessment and to enter into an NDA with them in order to receive a copy of the onboarding submission form and any additional information required to meet this requirement.	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 and audit reports for the proposed Service to demonstrate compliance: (a) 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 (b) 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: 1. Be valid as of the Submission date; 2. Identify the legal business name of the proposed Supplier, and applicable Supplier Sub-processor, including Cloud Service Providers (CSPs); 3. Identify the current certification date and/or status; 4. identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report; 5. 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

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
			such as data centre hosting, the subservice organization's assessment report must be included; and 6. 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; and • Certifications must be valid and within the 12 months prior to the start of a contract.
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 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. For SaaS, the Contractor must demonstrate that the IaaS/PaaS leveraged by the Services ensures: (a) Supplier Sub-processors have been assessed by the CCCS Program; and (b) Supplier meet the security obligations for Sub-Processors and/or Subcontractors outlined by the Supplier, for the life of the contract.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		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 Streams may require the Supplier to notify Canada regularly when there are updates to the list of third party suppliers.	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.
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 must demonstrate compliance by providing at least one of the following four 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 organization's defined security safeguards are 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

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
			proposed Commercially Available Public Software as a Service will reduce and mitigate supply chain risks; or 4. CSA STAR controls to support CSA CCM Supply Chain Management controls.
M8	**Privileged Access Management**	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrate how the Software as a Service is able to meet the following 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	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 Privileged Access Management requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		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 Communication Security Establishment's (CSE's) ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3h); (f) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3); (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;	

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		(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 (Up to and including Protected A Data)
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 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3); (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 Federation of Identity requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
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 Security (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 Endpoint Protection requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
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 Secure Development requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
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 Government of Canada (GC) services and take reasonable measures to: (a) Implement multi-factor authentication mechanisms for authentication of remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3h); (b) Employ CSE Approved Cryptographic Algorithms 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 Supplier Remote Management requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
M13	**Information Spillage**	**Information Spillage** 1. The Supplier must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, 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 data elements that is involved in a System's contamination; (b) A process to isolate and eradicate a contaminated System; and (c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination; (d) The supplier will confirm a point of contact, proper procedures and an agreed upon secure form of communication to provide assistance where practicable for customer administrators. 2. Upon request of Canada, the Supplier must provide a document that describes the Supplier's Information Spillage Response 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 Information Spillage requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
M14	**Cryptographic Protection**	**Cryptographic Protection** The Supplier must provide Canada with a document that outlines the process it follows to respond to 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, Transport Layer Security (TLS), software modules, Public Key Infrastructure (PKI), and authentication tokens, where applicable), in accordance with CSE approved cryptographic algorithms, cryptographic key sizes, and crypto periods; (b) Use cryptographic algorithms, 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	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 Cryptographic Protection requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		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.	
M15	**Data Segregation**	The Supplier must 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's 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 substantiation required for Data Segregation requirements 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.

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).**

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

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
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 (and any Supplier Sub-processors, as applicable) and Canada.	In the document, the Supplier must include, at a minimum, the parties' roles and responsibilities for: (a) Account management; (b) Boundary protection; (c) Asset and information system backup; (d) Incident management; (e) System monitoring; and (f) 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 Government of Canada (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. To be considered compliant, the provided documentation must include: (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. The substantiation required for Master / Root Account Management requirements cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
			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 included in the Submission. 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.
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,	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 Protection Isolation requirements 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		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.	Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation included in the Submission. 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.
M4	**Data Segregation**	The Supplier must 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's 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 substantiation required for Data Segregation requirements 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
M5	**Data Protection**	The Supplier of the proposed Commercially Available Software as a Services must have the ability for 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 Streams may require the Supplier of the proposed Commercially Available Software as a Service to notify Canada when	The Supplier must demonstrate compliance by providing documentation outlining the 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 Data Protection requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		there are updates to the list of physical locations which may contain Canada's data.	
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 security controls and the practices in the Directive on Security Management (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C). 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 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	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 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 included in the Submission. Suppliers must indicate where in their 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 (Up to and including Protected B Data)
		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.	
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	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Personnel Security Requirements.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		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 in writing 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 of, 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	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 for Personnel Security requirements 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 included in the Submission. 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 (Up to and including Protected B Data)
		and/or effect on the reliability of cloud services hosting GC assets and data.	
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	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 and audit reports 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 and 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;

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		by CCCS; and (ii) a copy of the most recent summary report provided by CCCS. This will accelerate the qualification process and at the same time doesn't require the Supplier to demonstrate the compliance. Suppliers that have already completed the security assessment by providing to CCCS their certifications and audit reports and have already entered into a Non-Disclosure Agreement (NDA) with them, must send their certifications and audit reports directly to CCCS client services at contact@cyber.gc.ca in order to meet this requirement. For suppliers that have not completed the security assessment, the onboarding process will commence once the Submission complies with the requirements of the Request for Supply Arrangements, meets all mandatory technical and financial evaluation criteria, and provides all of the mandatory certifications in order to be declared responsive. Public Services and Procurement Canada (PSPC) will then refer the Supplier to CCCS client services to begin the onboarding process to the IT Assessment and to enter into an NDA with them in order to receive a copy of the onboarding submission form and any additional information required to meet this requirement.	(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 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 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
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 under Section 4 entitled "Obligations Cloud Service Provider (CSP) IT Security Assessment Program" of Annex B - Security & Privacy Obligations. 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 include: (a) GC Security Control Profile for Cloud-Based GC IT Services, and (b) Industry Certification in Third-Party Assurance detailed under Tier 2 M8.
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	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: (a) subcontractors to the Supplier; (b) subcontractors to subcontractors of the Supplier down the chain; or (c) any subsidiaries.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		that could provide Canada with the proposed Commercially Available Software as a Service, is not considered to be a third party. Third parties would include, for example, technicians who might be deployed to maintain the Commercially Available Software as a Services of the Supplier that have been proposed by the Supplier. **Please note:** Suppliers are advised that subsequent procurement Streams may require the Supplier to notify Canada regularly when there are updates to the list of third-party suppliers.	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 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 (Up to and including Protected B Data)
M11	**Supply Chain Risk Management**	The Supplier of the proposed Commercially Available Software as a Service 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; or 4. CSA STAR controls to support CSA CCM Supply Chain Management controls. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
			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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
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 Streams 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's 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 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 (Up to and including Protected B Data)
M13	**Privacy by Design**	The Supplier must demonstrate that it implements privacy by design as part of its software development lifecycle, and in accordance with 'Secure Development' as identified below. <u>Secure Development</u> 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 27034, (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. Upon request of Canada, the Supplier must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
M14	**Privileged Access Management**	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrates how the Software as a Service is able to meet the following security requirements of 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	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 Privileged Access Management requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3h); (f) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with Communication Security Establishment's (CSE's) ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3h); (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;	

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		(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 authenticator 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 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3h); (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 Federation of Identity requirements 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 included in the Submission. 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.

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 Security (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 Endpoint Protection requirements 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 included in the Submission. 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.

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 Secure Development requirements 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 included in the Submission. 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.

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 authentication of remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3h); (b) Employ CSE Approved Cryptographic Algorithms 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 Supplier Remote Management requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
M19	**Information Spillage**	**Information Spillage** (1) The Supplier must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, 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 data elements that are involved in a System's contamination; (b) A process to isolate and eradicate a contaminated System; and (c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. (d) The supplier will confirm a point of contact, proper procedures, and an agreed upon secure form of communication to provide assistance where practicable for customer administrators. (2) Upon request of Canada, the Supplier must provide a document that describes the Supplier's Information Spillage Response 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 Information Spillage requirements 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 included in the Submission. 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.

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 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, Transport Layer Security (TLS), software modules, Public Key Infrastructure (PKI), and authentication tokens, where applicable), in accordance with CSE approved cryptographic algorithms, cryptographic key sizes, and crypto periods; (b) Use cryptographic algorithms, 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 either an approved or an allowed mode to	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 Cryptographic Protection requirements 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 included in the Submission. 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.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2
		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.	

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 (SA), 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 Subcontractors and Sub-processors, to the extent applicable to each Supplier Subcontractor and 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 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; and (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

The Supplier must conduct the security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting Canada's Data as follows:

(a) As per the mandatory ISO certifications, 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;

(c) Each audit will be performed by independent, third party auditors 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; and

(d) Each audit will result in the generation of an audit report that must be made available to Canada. The audit report must clearly disclose any material findings by the third party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

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 its Sub-processor to supplement the certification and audit reports described in Section 5 (Third Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications.

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; and,

(b) Provide a means via API for applications to provision services, and extract reporting, billing and financial data pertaining to the cloud services consumed by the Client.

(c) 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 and providing the ability for the GC to meet the GC's standards on API (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html).

For Software as a Service (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 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 Transportation Layer Security (TLS) 1.2, or subsequent versions;
(b) Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in Communication Security Establishment's (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);
(c) Use correctly configured certificates within the TLS connections in accordance with CSE guidance; and
(d) 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 used to deliver the SaaS Solution to the Government of Canada (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 of 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 centers' geographical locations in Canada where the capability is available.

10. Logging and Auditing (Tier 1 and 2)

(a) The Supplier must implement log generation and management practices and controls for all Service components that store or process Assets and Information Assets 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.

(b) 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:

(i) 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;

(ii) 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;

(iii) 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 Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or SaaS Service provided to it by the Supplier or a Supplier Sub-processor; and

(iv) 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)

(a) 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/government/system/digital-government/online-security-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.

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

(i) 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.

(ii) 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

(a) In the event Canada needs to conduct privacy audits, inspections and/or review any additional information (e.g., documentation, data protection description, and data) 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.

(b) 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).

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

(i) Where a standard or framework provides for audits, an audit of such control standard or

framework will be initiated at least annually;

(ii) 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

(iii) Each audit will be performed by qualified, independent, third party privacy auditors 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.

(d) 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.

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

13. Protecting Information Assets

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

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

(i) 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;

(ii) 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.

(b) 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, the 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

The Supplier must 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 Privacy Officer must be a resident of Canada. 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 professional Services Ceiling Prices

Option 1: Suppliers provide a link to their commercially-available Software as a Service (SaaS) catalogue and indicate the percentage discount offered to Canada.

URL:

OR

Option 2: Suppliers complete the table below.

TABLE 1 - PRODUCT LIST AND CEILING PRICES												
Item NO.	**SaaS Publisher's Part No. (A)**	**SaaS Solution's Name (B)**	**SaaS Publisher's Name (C)**	**Cloud Service Provider's Name (D)**	**Ceiling Prices for SaaS Solutions (E)**	**Ceiling Prices for Optional Professional Services (F)**	**Unit of Measure (G)**	**Applicable Percentage Discount (H)**	**Language (s) available (I)**	**SaaS Solution Product Description (J)**	**SaaS Solution Information (K)**	**Keywords/tags (L)**
	(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)	(enter ceiling price for professional services per per diem rates, hours, or package in Canadian Dollars for each category: Quick Start Guide ("QSG"), training and services, implementation services, training services, data cleansing, migration and transition services, and advisory 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 for the Supply Arrangement (SA))	(enter the language of the SaaS Solution, English and/or French)	(enter a brief description of the SaaS Solution – if applicable)	(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 and conditions in the SLA, detailed under 3.2 Section I: Technical Submission, (c) (v), related to service levels and service delivery will apply. Any terms and conditions of the SLA not related to service levels and service delivery will be deemed stricken and will not apply. 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 Government of Canada (GC) Software as a Service (SaaS) Supply Arrangement (SA) with the Public Services and Procurement Canada (PSPC) file number EN578-191593/*XXX*/EEM. All terms and conditions of the SA 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 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

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.

The 2003 standard instructions is amended as follows:

- 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 PSPC Bid Receiving Unit (BRU) 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 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 _____ (*insert number of days*) days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

2.6 Applicability of COVID-19 vaccination requirements to individual solicitations

The requirement covered by the bid solicitation of any resulting supply arrangement may be subject to a vaccination requirement pursuant to the COVID-19 Vaccination Policy for Supplier Personnel.

PART 3 - BID PREPARATION INSTRUCTIONS

3.0 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, as amended above. 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. Prices must not be indicated in any other section of the bid. The Technical Bid and the Certifications may be included on the same USB Key.

3.1 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.

3.2 Section II: Financial Bid

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

3.2.2 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.

3.2.3 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.

3.2.4 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.

4.2.2 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/corporate/portfolio/labour/programs/employment-equity/federal-contractors.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 titled "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 3.2.2, 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):

( ) Direct Deposit (Domestic and International);

( ) Electronic Data Interchange (EDI);

( ) Wire Transfer (International Only);

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

( ) Acquisition Card (Visa or MasterCard), to the extent that this type of payment is made commercially available by the Contractor as a payment method.

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).

(See Attached at the end of the RFSA)

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

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

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

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

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

ANNEX G – Security Requirements for Canadian Contractor

1. The **Contractor/Sub-processor/Subcontractor** must, at all times during the performance of the Contract/Supply Arrangement, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding Capability (DSC) at the level of PROTECTED A or B (as applicable), issued by the Contract Security Program , **Public Services and Procurement Canada (PSPC), also referred to as PWGSC.**

2. The **Contractor/Sub-processor/Subcontractor** personnel requiring access to PROTECTED information, assets or sensitive 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 Contract Security Program/PWGSC.

3. The **Contractor/Sub-processor/Subcontractor** 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 the Contract Security Program/PWGSC.

5. The **Contractor/Sub-processor/Subcontractor** must comply with the provisions of the:
   (a) Security Requirements Check List (SRCL) and security guide (if applicable),
   (b) Contract Security Manual (Latest Edition);
   (c) ISS website: Security requirements for contracting with the Government of Canada, located at https://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html

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

ANNEX H – Security Requirements for Foreign Contractor

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

The Designated Security Authority for Canada (Canadian DSA) is the Contract Security Program, Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming **Contractor/Sub-processor/Subcontractor** compliance with the security requirements of this contract for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor/Sub-processor/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 the Cloud Solutions, in addition to the Security and Privacy Requirements, detailed in Appendix C & Appendix D, respectively. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

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

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

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

   (b) The Foreign recipient **Contractor/Sub-processor/Subcontractor** must not begin the work, services or performance until the Canadian 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/Sub-processor/Subcontractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

   (c) The Foreign recipient **Contractor/Sub-processor/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/Sub-processor's/Subcontractor's** Chief Executive Officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which

would enable them to adversely affect the organization's policies or practices in the performance of the contract.

(d) The Foreign recipient **Contractor/Sub-processor/Subcontractor** must not grant access to **CANADA PROTECTED** information/assets, except to its personnel who have been screened 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 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:

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

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

c. The Foreign recipient **Contractor/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

d. 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/PERSONAL** information/assets, provided to the foreign recipient **Contractor/Sub-processor/Subcontractor** or produced by the Foreign recipient **Contractor/Sub-processor/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, and 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, and the Contracting Authority (in collaboration with the Canadian DSA).

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

6. The Foreign recipient **Contractor/Sub-processor/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/Sub-processor/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.

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

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

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

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

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

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

13. The Foreign recipient **Contractor/Sub-processor/Subcontractor** requiring access to **CANADA PROTECTED** information/assets or Canadian restricted sites, under this contract, must submit a Request for Site Access to the Departmental Security Officer of the Department/Organization for which the Services and/or Work are performed under the Contract**.**

14. The Foreign recipient **Contractor/Sub-processor/Subcontractor** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED B** information until authorization to do so has been confirmed by the Canadian DSA.

15. The Foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that all the databases including the backup database used by organizations to provide the services described in the proposed Cloud Solutions, containing any **CANADA PROTECTED B** Information, related to the Services and/or Work, are located within Canada.

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

17. All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

18. All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

19. The Foreign recipient **Contractor/Sub-processor/Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex I.

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

Protection and Security of Data Stored in Databases

1. The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that all the databases used by organizations to provide the services described in the proposed Cloud Solutions containing any **CANADA PROTECTED B** Information, related to the Services and/or Work, are located in Canada.
2. The foreign recipient **Contractor/Sub-processor/Subcontractor** must control access to all databases on which any data relating to the **contract/subcontract** is stored so that only individuals with the appropriate security screening are able to access the database, either by using a password or other form of access control (such as biometric controls).
3. The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that all databases on which any data relating to the **contract/subcontract** is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases.
4. The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that all data relating to the **contract/subcontract** is processed only in Canada or in another country approved by the Contracting Authority under subsection 1.
5. The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection 1.
6. Despite any section of the General Conditions relating to subcontracting, the foreign recipient **Contractor/Sub-processor/Subcontractor** must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the contract unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.

Personal Information

Interpretation

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

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

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

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

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

Ownership of Personal Information and Records

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

Use of Personal Information

The foreign recipient **Contractor/Sub-processor/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**.

Collection of Personal Information

1. If the foreign recipient **Contractor/Sub-processor/Subcontractor** must collect Personal Information from a third party to perform the Services and/or Work, the foreign recipient **Contractor/Sub-processor/Subcontractor** must only collect Personal Information that is required to perform the Services and/or Work. The foreign recipient **Contractor/Sub-processor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor/Sub-processor/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/Sub-processor/Subcontractor**.
2. The foreign recipient **Contractor/Sub-processor/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.
3. If requested by the Contracting Authority, the foreign recipient **Contractor/Sub-processor/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/Sub-processor/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.

4. At the time it requests Personal Information from any individual, if the foreign recipient **Contractor/Sub-processor/Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of their Personal Information, the foreign recipient **Contractor/Sub-processor/Subcontractor** must ask the Designated Security Authority for Canada for instructions.

Maintaining the Accuracy, Privacy and Integrity of Personal Information

The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor/Sub-processor/Subcontractor** must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor/Sub-processor/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/Sub-processor'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/Sub-processor/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/Sub-processor/Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor/Sub-processor/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/Sub-processor/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 their 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/Sub-processor/Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Sub-processor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the **Contractor/Sub-processor/Subcontractor** 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/Sub-processor/Subcontractor** and Canada at any time; and

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

Safeguarding Personal Information

The foreign recipient **Contractor/Sub-processor/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/Sub-processor/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.

Quarterly Reporting Obligations

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

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

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

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

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

Threat and Risk Assessment

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

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

b. a list of the types of Personal Information used by the foreign recipient **Contractor/Sub-processor/Subcontractor** in connection with the Services and/or Work;

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

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

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

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

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

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

Audit and Compliance

Canada may audit the foreign recipient **Contractor's/Sub-processor's/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.

Statutory Obligations

1. The foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/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/Sub-processor/Subcontractor** believes that any obligations in the **contract/subcontract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor/Sub-processor/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/Sub-processor/Subcontractor** believes it conflicts.

Disposing of Records and Returning Records to Canada

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

Legal Requirement to Disclose Personal Information

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

Complaints

Canada and the foreign recipient **Contractor/Sub-processor/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.

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 sub-processors, subcontractors, agents, or representatives, or any of their employees.

SECRET CLEARANCE

Secret clearance will be required for any **Contractor/Sub-processor/Subcontractor** personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the **Contractor/Sub-processor/Subcontractor** data centers, any sensitive system and security incident data.

The contractor and/or any and all sub-processors and subcontractors must be from a country with which Canada has an international bilateral industrial security instrument, or will have such an instrument with Canada by the end of the bidding period. 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.

1. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of **their respective National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the National legislation, regulations and policies of the supplier's country/the Canadian DSA.**

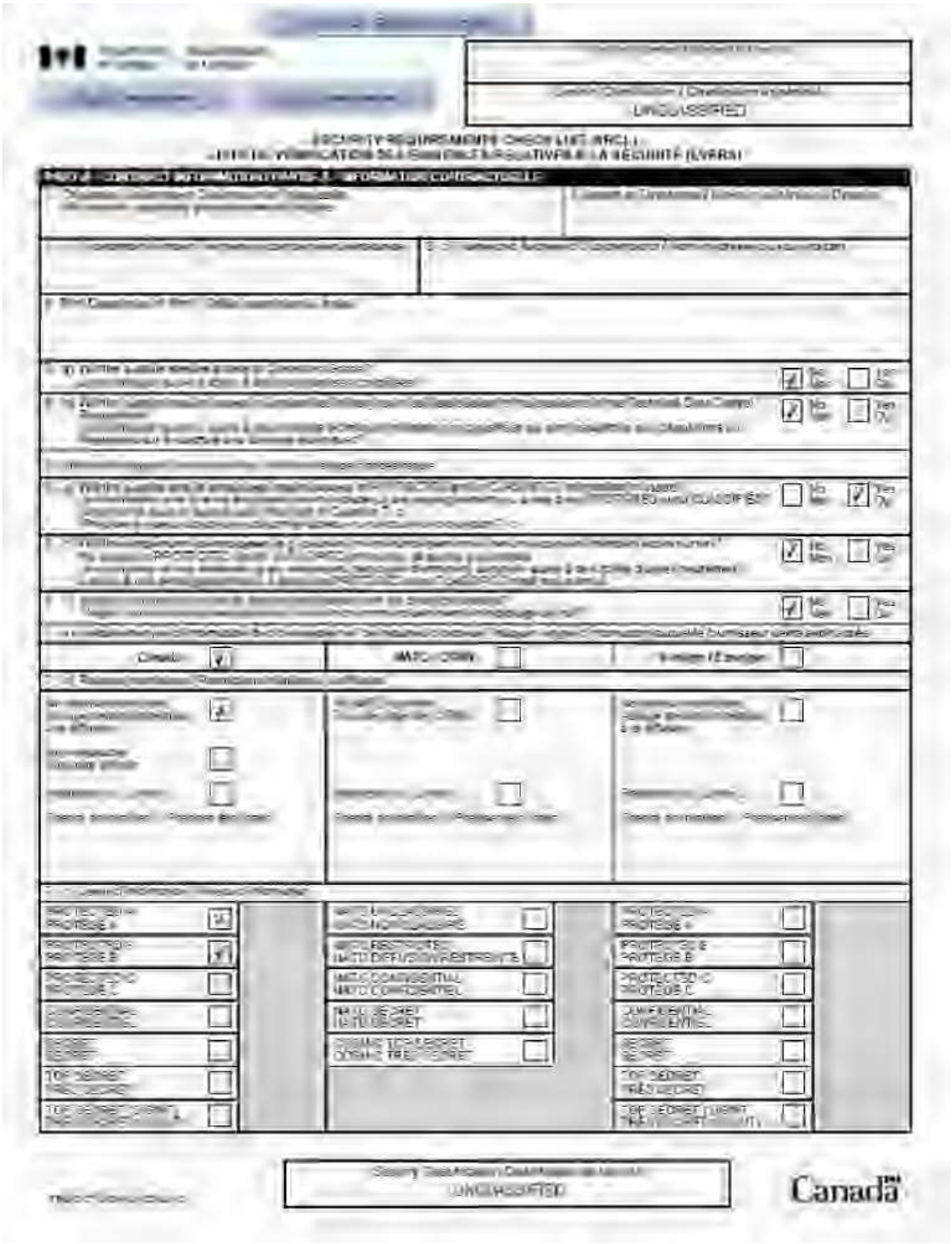
2. The Foreign recipient **Contractor/Sub-processor/Subcontractor** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED/CLASSIFIED** information/assets until the National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country** has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Contractor Sub-processor/Subcontractor**, these tasks may be performed up to the level of **SECRET.**

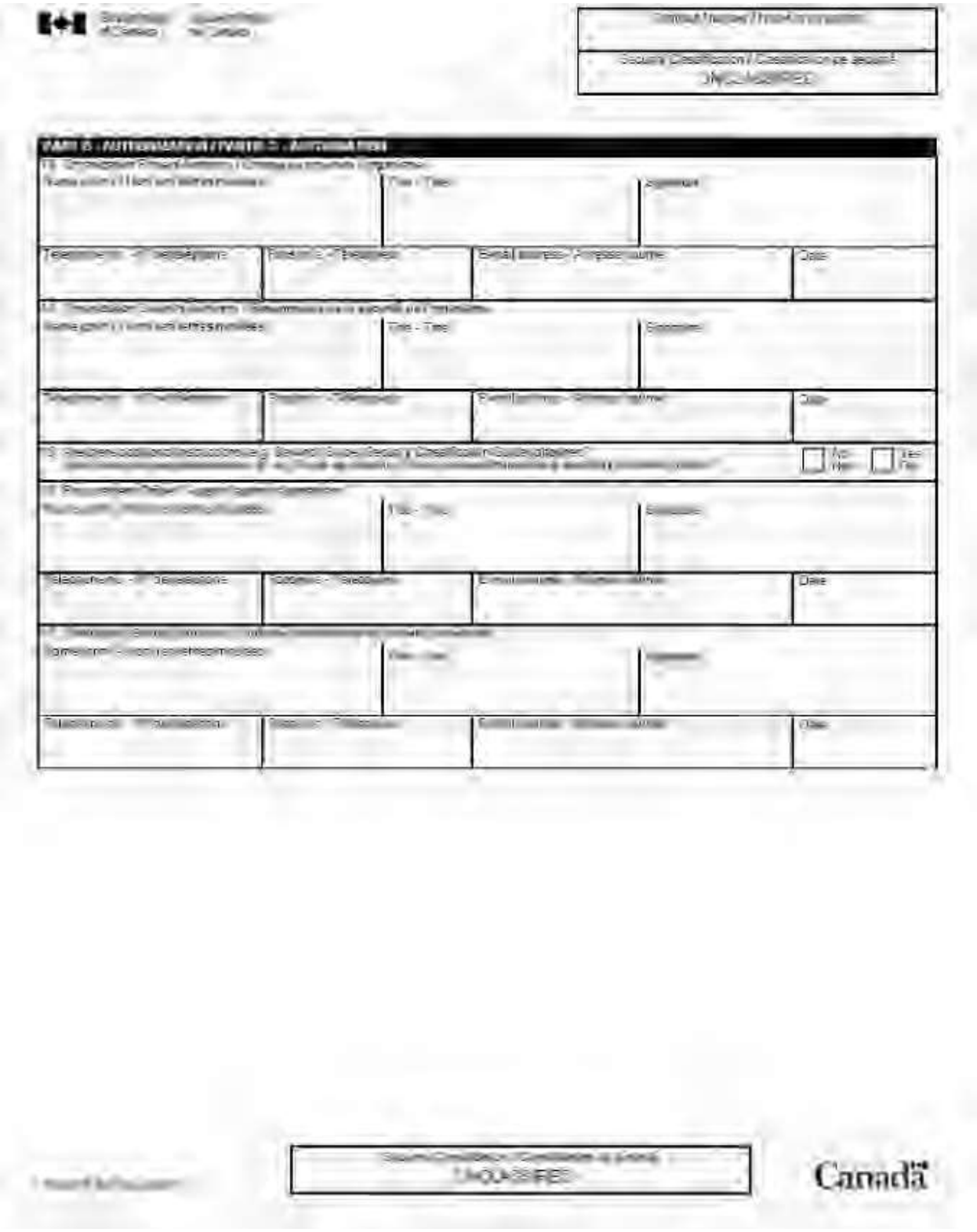
3. The Foreign recipient **Contractor/Sub-processor/Subcontractor** shall not use the **CANADA PROTECTED/CLASSIFIED** information/assets for any purpose other than for the performance of the **Contractor / Sub-processor/Subcontractor** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

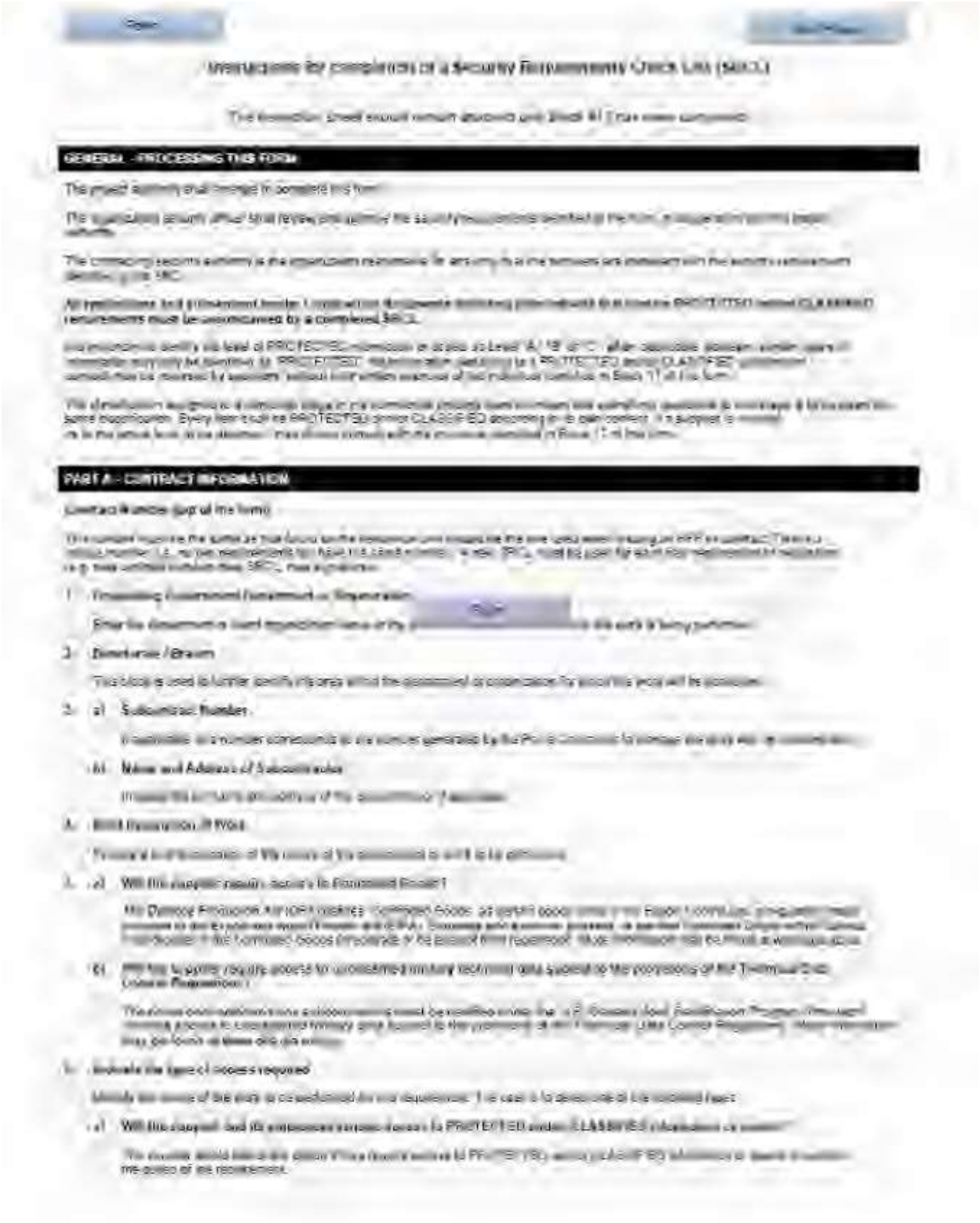
4. The Foreign recipient **Contractor/Sub-processor/Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED/CLASSIFIED** information/assets pursuant to this **Contractor/Sub-processor/Subcontractor** has been compromised.

5. The Foreign recipient **Contractor/Sub-processor/Subcontractor** shall not disclose **CANADA PROTECTED/CLASSIFIED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent shall be sought through the {recipient's National Security Authority/Designated Security Authority (NSA/DSA)/Canadian DSA}.

6. The Foreign recipient **Contractor/Sub-processor/Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex I.

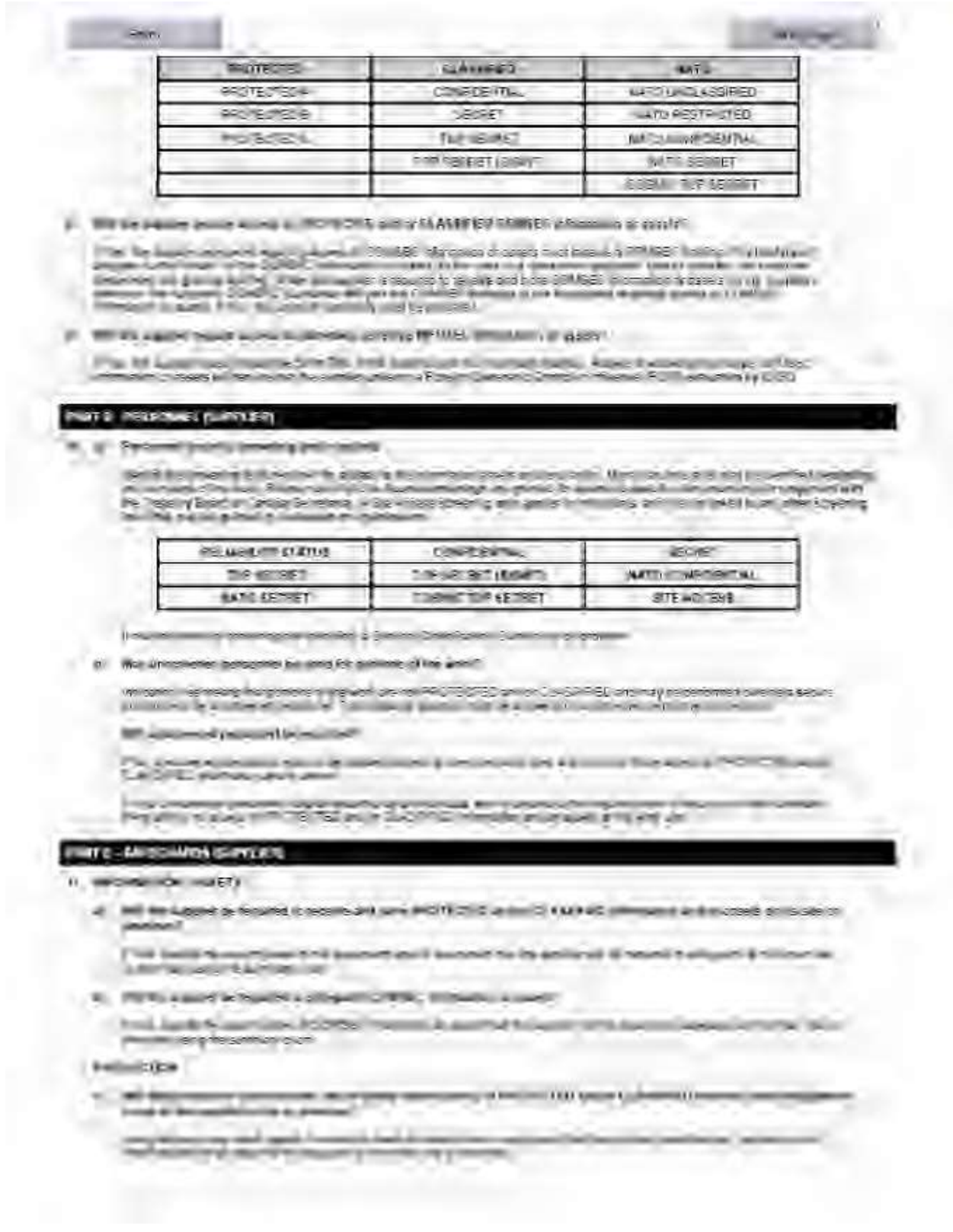

UNCLASSIFIED
UNCLASSIFIED
Canada





Page **112** of **144**

RFSA



INFORMATION TECHNOLOGY (IT)

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

[illegible]

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

[illegible] PROTECTED B level)

SUMMARY CHART

[illegible]

[illegible]

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

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

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

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

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

PART D - AUTHORIZATION

13. **Organization Project Authority**

[illegible]

14. **Organization Security Authority**

[illegible]

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

[illegible]

16. **Procurement Officer**

[illegible]

17. **Contracting Security Authority**

[illegible]

SRCL – Security Classifications Guide

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

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

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

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

Track	Role	Responsibilities	Access to	Location (other than meetings)	Personnel Clearance Requirements (working assumption)
Quick Start Guide ("QSG") Training and Services Package	Consultant	Defining the project plan, designing and deploying the solution, training on product functionality	• No access to physical systems (hands on keyboards); • May attend meetings where protected system configuration data is displayed and/or discussed; • No access to user data	Onsite - N/A Remote – Yes*	Reliability or equivalent
Advisory Services	Delivery Executive, Program Manager or Project Manager	Governance / project management of the engagement	• No access to physical systems (hands on keyboards); • May attend meetings where protected system configuration data is displayed and/or discussed; • No access to user data	Onsite - N/A Remote – Yes*	Reliability or equivalent
Implementation Services	Project Manager, Consultant	Project planning, data preparation and migration, installation and configuration, conduct workshops	• Access to Systems; • May attend meetings where protected system configuration data is displayed and/or discussed; • Access/Potential Access to data	Onsite - N/A Remote – Yes*	Secret or equivalent
Training Services	Consultant	Leading workshops, creation of documents (service maps, monitoring, etc.)	• No access to physical systems (hands on keyboards); • May attend meetings where protected system configuration data is displayed and/or discussed; • No access to user data	Onsite - N/A Remote – Yes*	Reliability or equivalent

Data Cleansing, Migration and Transition Services	Data Cleansing Services Consultant	Technical oversight of engagement, general guidance, document and deliverables review	• Access to Systems; • Access/Potential Access to data; • Access to GC documentation as required to complete data cleansing	Onsite - (if required by Client) Remote – Yes*	Secret or equivalent
	Migration Services Consultant	Migration of data. Post-migration support to assist Service Desks	• Access to Systems; • Access/Potential Access to data; • Access to GC documentation as required to complete migrations	Onsite - (if required by Client) Remote – Yes*	Secret or equivalent
	Transition Services Consultant	**Remediation Phase** - Working side-by-side with clients to remediate issues **Enable Phase** - Working side-by-side with clients to deploy SaaS solution	• Access to Systems; • Access to GC documentation as required to assist in the remediation and enablement; • Potential access to user data	Onsite - (if required by Client) Remote – Yes*	Secret or equivalent

*Foreign Recipient Contractors/Sub-processors/Sub-contractors must not allow work on or access to Canada Protected Information from a residence located outside of Canada.

Summary of clearance and assessment levels required:

	Designated Organizational Screening (DOS) Any Personnel with **NO** privileged roles and unrestricted logical access to GC assets within the Contractor services	**Designated Organizational Screening (DOS)** Any Personnel **WITH** privileged roles and unrestricted logical access to GC assets within the Contractor services	**Document Safeguarding Capabilities (DCS)**
Stream 1 up to Protected B (SaaS Publisher)	Reliability*	Secret	Protected B
Stream 2 up to Protected A (SaaS Publisher)	Reliability*	Secret	Protected A
Stream 3 up to Protected A (Value Added Reseller)	Reliability*	Secret	Protected A
Stream 4 Unclassified (SaaS Publisher or Value Added Reseller)	N/A	N/A	N/A

*or equivalent

ANNEX K

(Intentionally blank)

ANNEX L – SAAS IT Security (ITS) Assessment Program: Onboarding Process

1. Making a Submission to the Software as a Service (SaaS) IT Security (ITS) Assessment Program

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

(i) Prepare a Submission which complies with the requirements of the Request for Supply Arrangement (RFSA), meets all mandatory technical and financial requirements evaluation criteria, and provides all of the mandatory certifications and forms required in order to be declared responsive. The Canadian Center for Cyber Security (CCCS) reserves the right to put an IP Security Assessment on hold if a Supplier has not presented a responsive Submission to the Contracting Authority at the time of onboarding.

(ii) Contact the CCCS Contact Centre: contact@cyber.gc.ca or 613-949-7048 or 1-833-CYBER-88 during a predetermined onboarding Wave.

- Wave 1 – 9 a.m. EST February 10, 2020 to 2 p.m. EST March 6, 2020
- Wave 2 – 9 a.m. EST on January 18, 2021 to 2 p.m. EST on February 12, 2021
- Wave 3 – To be determined

(iii) Prepare to enter into a bilateral Non-Disclosure Agreement (NDA) with the CCCS.

(iv) Provide all documentation for the assessment to the CCCS Contact Centre. When providing documents, Pretty Good Privacy (PGP) encryption program credentials should be used to encrypt the documents. See section 2 – PGP Key for a copy of the PGP key. All documentation required by CCCS must be provided prior to the closing of the onboarding Wave to ensure successful onboarding.

2. PGP Key

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

3. Contacts and Assistance

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

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

ANNEX M – SUPPLY ARRANGEMENT QUARTERLY REPORTS TEMPLATE

No.	Contract No.	Contract Amd. No.	Contract or Contract Amd. Award Date	Contract Expiry Date	Name of Authorized Signing Authority *(as per Annex N)*	Department of Contracting Authority	Name of Client Department	Part No.	Product Name	Qty	Contract Unit Price	Total Price	Value-Added Reseller
1													
2													
3													
4													
5													

Quarterly Reports must be submitted to the Supply Arrangement Authority via email to TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca by each quarter's due date as specified in Part 6, section 6.5, Supply Arrangement Reporting.

Definitions / Instructions:

No.: Suppliers are required to report each line item separately

Contract No.: The Contract number is unique to each Contract and is listed on page 1 of each Contract

Contract Amd. No.: The number of the contract amendment, if applicable

Contract or Contract Amd. Award Date: Enter the date on page one of either the contract or the contract amendment as applicable

Contract Expiry Date: Enter the contract expiry date, found in the terms and conditions of the contract, not including optional periods

Name of Authorized Signing Authority: Enter the name of the Contracting Authority (i.e. name of the person who signed the Contract)

Department of Contracting Authority: Enter the name of the department of the contracting authority

Name of Client Department: Enter the name of the client department, indicated in the Technical Authority clause of the Contract

Part No.: Enter the Manufacturer's Part Number from Annex C - SaaS Solutions and Professional Services Ceiling Prices

Product Name: Enter the Product Name from the issued contract

Qty: Enter the quantity for each item

Contract Unit Price: Enter the Unit Price, not including GST/HST/QST

Total Price: Enter the Total Price, not including GST/HST/QST

Value-Added Reseller: Enter the Reseller assigned to fulfill the contract, if applicable

ANNEX N – LIST OF APPROVED PSPC AND CLIENT AUTHORITIES

Authorized client authorities		
Authorized client department or agency	**User agreement effective date**	**Prime contact**
Administrative Tribunals Support Service of Canada	2021-02-16	Danielle Gudbranson (danielle.gudbranson@tribunal.gc.ca)
Canada School of Public Service	2021-03-17	Anick Matthieu (anick.matthieu@csps-efpc.gc.ca)
Canadian Armed Forces – Directorate of Aerospace Procurement	2021-03-29	Donald Godbout (donald.godbout@forces.gc.ca)
Canadian Food Inspection Agency	2021-05-18	Lisa Chaykowski (lisa.chaykowski@inspection.gc.ca)
Canadian Institutes of Health Research	2021-06-21	Julie Morin (julie.morin@cihr-irsc.gc.ca)
Canadian Revenue Agency	2021-06-24	Di Chen (di.chen@cra-arc.gc.ca)
Correctional Services Canada	2021-03-12	Elizabeth Wheeler (elizabeth.wheeler@csc-scc.gc.ca)
Canadian Space Agency	2021-10-13	Jean-Denis Bisson (jean-denis.bisson@canada.ca)
Department of Finance Canada	2021-09-09	Nick Plettenberg-Dussault (nicholas.plettenberg-dussault@fin.gc.ca)
Department of National Defence, Assistant Deputy Minister (Finance)	2022-01-19	Caleb Wallace (ADMFinProcurement-ApprovisionnementSMAFin@forces.gc.ca)
Department of National Defence – ADM (HR-Civ) DGHRSD	2021-08-18	Emely Ospino (emely.ospino@forces.gc.ca)
Elections Canada	2021-01-20	Adrian Bennett (adrian.bennett@elections.ca)
Environment and Climate Change Canada	2021-02-26	Josee Francoeur (josee.francoeur@canada.ca)

Fisheries and Oceans Canada	2021-12-09	Jason Picco (jason.picco@dfo-mpo.gc.ca)
Global Affairs Canada	2021-03-28	Elena DiCola (elena.dicola@international.gc.ca)
Global Affairs Canada, Platform Corporate Services, AAD	2021-11-08	Alexander Jeske (alexander.jeske@international.gc.ca)
Health Canada / Public Health Agency of Canada	2020-11-23	Jesse Arsenault (jesse.arsenault@canada.ca)
Immigration, Refugees and Citizenship Canada – Administration, Security, and Accommodations	2021-06-16	Jodie Thomas (jodie.thomas@cic.gc.ca)
Immigration, Refugees and Citizenship Canada – IT Branch	2020-11-30	Jean-Bernard Tessier (jean-bernard.tessier@cic.gc.ca)
Indigenous Services Canada, Population Health and Primary Care Directorate	2021-12-20	Stuart Malcolm (stuartleroy.malcolm@sac-isc.gc.ca)
Natural Resources Canada	2021-04-01	Leanne Callery (leanne.callery@canada.ca)
Parks Canada	2021-09-01	Pat Alguire (pat.alguire@canada.ca)
Privy Council Office	2021-12-01	Adam Rouleau (adam.rouleau@pco-bcp.gc.ca)
Public Service Commission	2021-05-20	Guillaume Gagnon (guillaume.gagnon2@canada.ca)
Public Services and Procurement Canada, Applications and Software Procurement Directorate	2020-11-10	Jacob Guillot (jacob.guillot@tpsgc-pwgsc.gc.ca)
Public Services and Procurement Canada – Departmental Acquisition Services	2021-06-08	Marlee Diamond (marlee.diamond@tpsgc-pwgsc.gc.ca)
Public Services and Procurement Canada - Human Resources Branch	2021-02-28	Vanessa Primeau (vanessa.primeau@tpsgc-pwgsc.gc.ca)
Public Services and Procurement Canada - Real Property Services Branch & Property and Facility Management Service Line & Operations and Emergency Management Directorate	2021-03-08	Martin Audette (martin.audette@tpsgc-pwgsc.gc.ca)

Royal Canadian Mounted Police	2021-05-06	Crystal Rodger (crystal.Rodger@rcmp-grc.gc.ca)
Statistics Canada	2020-11-17	Marie-Lyne Carr (marie-lyne.carr@canada.ca)
Veterans Affairs Canada	2021-02-19	Susan O'Brien (susan.obrien@canada.ca)

ANNEX O – Software Usage Rights (SUR)

Only terms and conditions in the SUR, detailed under 3.2 Section I: Technical Submission, (c) (viii), related to software usage rights will apply. Any terms and conditions of the SUR not related to software usage rights will be deemed stricken and will not apply. Suppliers may submit their SURs by way of URLs. Suppliers are permitted to update their SURs on an ongoing basis, providing that the changes to the SUR do not represent are acceptable to Canada. Where a Supplier wishes to add a new SaaS Solution to their Supply Arrangement, the SUR(s) must be resubmitted to the Supply Arrangement Authority for acceptance prior to the SUR(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 O – SaaS Software Usage Rights (SUR).

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

Form 1 – Request For Supply Arrangement (RFSA) 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 (FTE) 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.] ***Facility Security Clearance - Secret*** ***Designated Organizational Screening – Reliability Status*** ***Document Safeguarding Capabilities – Protected A / Protected B***	FSC:_____ DOS:_____ DSC:_____	
Aboriginal Businesses [Suppliers are requested to indicate 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 (Office of Small and Medium Enterprises (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 Software as a Service (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 Solutions 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 Software as a Service (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 Supply Arrangement (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 _____

Request for Supply Arrangement (RFSA) Number _____

Form 3 – SaaS Publisher Authorization Form

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

This confirms that the Software as a Service (SaaS) Publisher identified below understands and acknowledges that the Supplier named below has submitted a Submission in response to the Request for Supply Arrangement (RFSA) dated _____, reference number _____ issued by Public Services and Procurement Canada (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 Supply Arrangement (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/policy-and-guidelines/supply-manual/section/9#annex-9.4).
(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 _____

Request for Supply Arrangement (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 Requirements

Forms:

1) Submission Submission Form (RFSA Form 1)

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

ANNEXES:

Annex A – Qualification Requirements *(Mandatory for Streams 1, 2, and 3)* ☐

Annex C – SaaS Solutions and Ceiling Prices ☐

a) ☐ Must be submitted using the format outlined in Annex C or submitted via a web-site link.
b) ☐ **Item No**. included for each product.
c) ☐ **SaaS Publisher's Part No.** *(the part number the Software as a Service (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)** *(the Supplier must identify the existing CSP whose Commercially Available Cloud Services will be used to supply to Canada the proposed SaaS)*

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

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

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

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

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

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

Annex D – SaaS Solution Service Level Agreement(s)

Service Level Agreement (SLA):

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

Name of Authorized Signatory of Supplier: _____

Signature of Authorized Signatory of Supplier: _____

ANNEX F – SOFTWARE AS A SERVICE (SAAS)
RESULTING CONTRACT CLAUSES

TO THE REQUEST FOR SUPPLY ARRANGEMENT (RFSA) FOR

SOFTWARE AS A SERVICE (SAAS)

GOVERNMENT OF CANADA METHOD OF SUPPLY

(GC CLOUD)

TABLE OF CONTENTS

Software as a Service Solution (SaaS)

Resulting Contract Terms

***Note to Contractors**: 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 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 prices no greater than those 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 *(Optional clause to be used when professional services are required)* **Professional Services.** The Contractor agrees to provide the following Professional Services, as and when requested by Canada, using the Task Authorization process:

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

(b) implementation services;

(c) training services;

(d) data cleansing, migration and transition services; and

(e) 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 (Section 2.1 – 2.5 OR Section 2.1 a – f), as applicable to the corresponding Unit of Measure submitted by the Contractor in the applicable Annex C 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.

2.5 **Change in Consumption.** The Contractor grants to Canada the irrevocable option to increase or decrease their consumption of the SaaS products or services detailed in Appendix A at the time of contract renewal. Where Canada's consumption of a specific SaaS products or services is decreased, the Contractor agrees that no penalty shall apply as a result.

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 prices no greater than those 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.*

The Contractor agrees to provide a notification functionality or a 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 at least 60 days in advance of the expiry of the subscription services or Contract Period.

(d) ***Grace Period.*** *The Contractor agrees to provide Canada with an optional grace period of 4 weeks to terminate the Contract Period, in the event that Canada fails to stop its usage of the Service on or before the end of the defined Contract Period. At any time before the expiry of the grace period, and notwithstanding any auto-renewal clause elsewhere in the Contract, the Contracting Authority may terminate the Contract by providing written notice to the Contractor of Canada's decision to terminate the Contract. Upon delivery of the notice, the termination will take effect immediately or, at the time specified in the termination notice. Canada will be released from further obligation under the Contract after the termination date, and will be specifically released from any extended term resulting from an auto-renewal clause. The Contractor will apply no penalty or additional fees in these circumstances.*

(e) ***Canada's Responsibility.*** *Notwithstanding the provision of the grace period, Canada remains responsible to monitor its obligations under the Contract, including fees, renewal and expiry dates, consumption, usage, payment, termination and renewals.*

(f) ***Change in Consumption:*** *The Contractor grants to Canada the irrevocable option to increase or decrease their consumption of the SaaS products or services detailed in Appendix A. Where Canada's consumption of a specific SaaS products or services is decreased, the Contractor agrees that no penalty shall apply as a result.*

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 be responsible for 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 with terms that are materially 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. The 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 core 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. The Contractor agrees to immediately repay the portion of any advance payment for the Services that is unliquidated at the date of the termination to Canada.

4. Services

4.1Solution 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.** If anyone claims that as a result of Canada's access or use of the SaaS Services, Canada is infringing its intellectual property rights, Canada will promptly notify the Supplier in writing about the claim. In the above circumstances, or if anyone claims that the Supplier is infringing its intellectual property rights in relation to the subject SaaS Solution of this Contract.

The Supplier must immediately do one of the following:

(i) take all necessary steps to acquire the rights to be able to continue to provide Canada the Solution Services in accordance with the Contract;

(ii) modify or replace the allegedly infringing part of or the whole SaaS Solution, and continue to provide Canada the Solution Services in accordance with the Contract;

(iii) if the above options are not viable, the Supplier agrees to provide written notice of the claim to Canada, and propose an alternate "Replacement" SaaS Solution as a new or interim basis of the Solution Services under this Contract. The Supplier agrees to provide the new or interim Solution Services at the same price as the subject Solution Services, for the duration of the Contract Period, regardless of the Supplier's commercial price for the Replacement SaaS Solution, or whether the Replacement SaaS Solution has greater functionality. Additionally, the Supplier agrees to provide training at no additional cost if required by Canada for its use of the Replacement SaaS Solution; or

(iv) provide written notice to Canada to terminate the Contract, including the name of the claimant, the nature of the claim, the Supplier's purported authority to the allegedly infringing part of the SaaS Solution and a confirmation of the Supplier's inability to continue to provide Canada the Solution Services in accordance with the Contract. For this termination right, the Supplier agrees to provide Canada extended access to any GC data used or stored through the SaaS Solution for recovery or migration, and agrees to fully refund any part of the Contract Price that Canada has already paid in previous 12 months, or from the date of infringement, whichever is earlier.

If the Supplier fails to comply with this section within a reasonable amount of time, the Supplier agrees to reimburse Canada for all the costs Canada may incur to resolve the infringement claim, including the procurement of new Solution Services.

(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**. Subject to the quantities identified in Appendix A, 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) 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, subject to the quantities identified in Appendix A,

(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.

(k) **Data Retrieval:** The Contractor agrees to make Canada's data available for a minimum of 45 days after the end of the Contract to allow the Client sufficient time to migrate their data to a new environment, at no additional cost to Canada.

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, **to the best of its knowledge**, nothing in the Solution, or in Canada's use of the Solution, **does or 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 Right to License. The Contractor guarantees that it has the right to license the Software as a Service and full power and authority to grant to Canada all the rights granted under the Contract. The Contractor also guarantees that all necessary consents to that grant have been obtained. Canada agrees that its only remedy and the Contractor's entire obligations in relation to a breach of this guarantee are the remedies and obligations set out in the section 4.1(c) "Indemnification" contained in the in Annex F of the Articles of Agreement.

6.5 Defective Documentation. If at any time during the Contract Period, Canada advises the Contractor of a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor must correct the defect or non-conformance 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. Rights & Remedies

7.1 Rights are Cumulative:

All rights and remedies provided in the Contract or by law are cumulative, not exclusive.

7.2 Termination for Default

(a) **Notice of Default:** The Contracting Authority may serve the Contractor with written Notice of Termination for Default of part or all of the Contract. The Notice will identify the breach, the relevant circumstances, any proposed cure period, the affected Work or Services (if partial termination), any action plan requirement, any required Transition or Migration Services, and the effective date of termination. The Notice will also identify whether Canada reserves any additional damages claim.

(b) **Contractor Compliance:** The Contractor must comply with the requirements of the Notice.

(c) **Total Default**: If, in Canada's reasonable opinion, the Contractor's default is a total or material breach of the Contract, Canada may immediately terminate the Contract by the Notice. For clarity, Canada's opinion may be based on circumstances including but not limited to:

(i) the Contractor's non-performance of a material contract obligation;

(ii) the Contractor irrefutably appears unable to perform a material contract obligation, due to factors beyond the Contractor's control. For clarity, this includes, actual or apparent insolvency, repeated failure to produce acceptable deliverables under this or other similar contracts with Canada,

(iii) the Contractor's multiple or repeated, uncured breach of an intermediate contract obligation(s), and

(iv) the Contractor's default adversely impacting government operations.

(d) **Other Default:**

(i) If the Contractor defaults are not Total Defaults, Canada will identify a Cure Period during which the Contractor must remedy the default and may require an action plan.

(ii) If, in response to the Notice, the Contractor indicates its inability or unwillingness to cure the default, Canada may terminate the Contract for default immediately.

(iii) If the Contract (including any individual Task Authorization) specifies that a specific default will be subject to no cure period, Canada may terminate the Contract for default immediately without providing any opportunity to cure the default.

(e) Canada is not required to notify the Contractor of any or every default. The Parties agree Canada may choose to not use this formal notification process or may choose to extend time to the Contractor, and neither will be construed as Canada waiving any rights or acquiescing in the Contractor's default.

(f) If Canada terminates the Contract for default, Canada will only pay for completed Work or Services delivered and accepted, prior to the termination date. Canada will not pay any amount exceeding the value of the Work or Services accepted. The contractor agrees to immediately repay the portion of any advance payment that is unliquidated at the date of the termination to Canada.

7.3 Termination for Convenience

(a) **Notice of Termination:** The Contracting Authority may serve the Contractor with written Notice of Termination for Convenience of part or all of the Work. The Notice will identify the effective date of termination, the affected Work (if partial termination), and any required Transition or Migration Services. The Contractor must comply with the requirements of the Notice, including continuing to perform or deliver Services or Work not affected by the termination.

(b) The Contractor agrees to immediately repay the portion of any advance payment that is unliquidated at the date of the termination to Canada.

(c) If, under (a), Canada terminates:

a. **Work.** Canada will pay the Contractor reasonable costs incidental to the termination of the Work incurred by the Contractor, specifically excluding costs related to severance of employees, unless the Contractor establishes those costs arise from statutory obligations.

(d) The parties agree that these amounts represent a genuine estimate of liquidated damages that would result to the Contractor for early termination of the Contract, and not a penalty.

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

All clauses related to Work apply to Work as defined in Appendix B and not to the Services

8.1 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.

8.2 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.

8.3 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 subsections (i) and (ii).

8.4 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 of 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.

(e) **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 the Work received up to the effective date of the termination.

8.5 Professional Services: Transition Services

(a) **Migration.** The Contractor acknowledges that due to 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 reasonably 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, to the extent that these services are made commercially available to other customers. There will be no charge for the services other than those charges set out in the Basis of Payment.

8.6 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(s) or location(s) 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.

9. 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.

9.1 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.

9.2 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.

9.3 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.

9.4 Periodic 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.

9.5 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.

10. 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 C or the winning bid.

10.1 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.

10.2 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 TA, 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 TA, 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.

10.3 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.

10.4 Price Certification. The Contractor certifies that the price quoted is not in excess of the lowest price charged anyone else, including the Contractor's most favoured customer, for the like quality and quantity of the goods, services or both.

11. Payments

11.1 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;

(iv) deduction for holdback, if applicable; and

(v) 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.

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

11.3 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.

11.4 Method of Payment

(a) Canada will make payment to the Contractor for the Services either in advance or in arrears, in accordance with Annex C SaaS Solutions and Ceiling Pricesor 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 11.3 once the dispute is resolved.

11.5 Limitation of Expenditure.

(a) 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.

(Note to Contracting Authority: The following clause may be used where the cloud services are consumption based (rather than a defined subscription period), in order to help ensure that clients do not exceed the quantity/costs identified in Appendix A.)

(b) Canada's total liability to the Contractor under the Contract must not exceed $ _____. Customs duties are _____ (*insert "included", "excluded" or "subject to exemption"*) and Applicable Taxes are extra.

(c) 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 agree to notify the Contracting Authority and Technical Authority in writing for the following reasons, whichever comes first:

(i) when it is 75% committed, or
(ii) four months before the expiry of the subscription services or contract period, or
(iii) as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

(d) If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

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

(a) Direct Deposit (Domestic and International);

(b) Electronic Data Interchange (EDI);

(c) Wire Transfer (International Only);

(d) Large Value Transfer System (LVTS) (Over $25M); or

(e) Acquisition Card (Visa or MasterCard), to the extent that this type of payment is made commercially available by the Contractor as a payment method.

12. 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.

13. Limitation of Liability

13.1 First Party Liability:

(a) **Contract Performance:** The Contractor is fully liable for all damages to Canada, arising from the Contractor's performance or failure to perform the Contract.

(b) **Data Breach:** The Contractor is fully liable for all damages to Canada resulting from its breach of security or confidentiality obligations resulting in unauthorized access to or unauthorized disclosure of records or data or information owned by Canada or a third party.

(c) **Limitation Per Incident:** Subject to the following section, irrespective of the basis or the nature of the claim, the Contractor's total liability per incident will not exceed the cumulative value of the Contract invoices for 12 months preceding the incident.

(d) **No Limitation**: The above limitation of Contractor liability does not apply to:

(i) wilful misconduct or deliberate acts of wrongdoing, and

(ii) any breach of warranty obligations.

13.2 Third Party Liability: Regardless whether the third party claims against Canada, the Contractor or both, each Party agrees that it will accept full liability for damages that it causes to the third party in connection with the Contract. The apportionment of liability will be the amount set out by agreement of the Parties or determined by a court. The Parties agree to reimburse each other for any payment to a third party in respect of damages caused by the other, and the other Party agrees to promptly reimburse for its share of the liability.

14. Compliance with on-site measures, standing orders, policies, and rules

The Contractor must comply and ensure that its employees and subcontractors comply with all security measures, standing orders, policies or other rules in force at the site where the Work is performed.

15. Suspension of the Work

(a) The Contracting Authority may at any time, by written notice, order the Contractor to suspend or stop the Work or part of the Work under the Contract for a period of up to 180 days. The Contractor must immediately comply with any such order in a way that minimizes the cost of doing so. While such an order is in effect, the Contractor must not remove any part of the Work from any premises without first obtaining the written consent of the Contracting Authority. Within these 180 days, the Contracting Authority must either cancel the order or terminate the Contract, in whole or in part, under section(s) 7.2 or 7.3 of Annex F – Resulting Contract Clauses.

(b) When an order is made under subsection (a), unless the Contracting Authority terminates the Contract by reason of default by the Contractor or the Contractor abandons the Contract, the Contractor will be entitled to be paid its additional costs incurred as a result of the suspension plus a fair and reasonable profit.

(c) When an order made under subsection (a) is cancelled, the Contractor must resume work in accordance with the Contract as soon as practicable. If the suspension has affected the Contractor's ability to meet any delivery date under the Contract, the date for performing the part of the Work affected by the suspension will be extended for a period equal to the period of suspension plus a period, if any, that in the opinion of the Contracting Authority, following consultation with the Contractor, is necessary for the Contractor to resume the Work. Any equitable adjustments will be made as necessary to any affected conditions of the Contract.

16. General Provisions

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

16.2 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.

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

16.4 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.

16.5 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.

16.6 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).

16.7 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.

16.8 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*.

16.9 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.

16.10 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.

16.11 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:

Grant of Agent Authority *(if applicable)*

The Contractor advises Canada, and Canada acknowledges that the Contractor intends to appoint one of its Authorized Partners as its Authorized Agent ("Authorized Agent") to fulfill certain contractual obligations on behalf of the Contractor during the Contract, as defined in the Scope section below.

The Contractor appoints its Authorized Partner, ***(to be completed at Contract Award)*** as its Authorized Agent under the Contract.

The Authorized Agent Contact is:

Name:

Title:

Telephone:

Facsimile:

E-mail address:

The Contractor agrees to provide 30-days advance written notice to the Contracting Authority of any of the following:

(i) its replacement of any Authorized Partner as Authorized Agent,

(ii) any change to the scope of power delegated to the Authorized Agent, and

(iii) the termination of the Authorized Agent.

The Contractor agrees, upon request by the Contracting Authority, to immediately remove or replace the Authorized Agent. Removal or replacement of the Authorized Agent is in addition to any other remedy Canada may invoke. A breach by an Authorized Agent is a breach by the Contractor itself.

16.12 Scope of Agent Authority

(Note to Contracting Authority: The following clause is only to be included where the Contractor grants an authorized agent to fulfill certain contractual obligations and can otherwise be deleted if not applicable)

The Contractor declares that the named Authorized Agent is authorized to transact business on the Contractor's behalf in matters relating to the supply of the goods and services under the Contract, limited to negotiating prices, providing billing information, invoicing, providing consumption reporting services, and receiving payment.

The Contractor agrees that, upon proof of payment, any payment made by Canada to the Authorized Agent will be considered payment to the Contractor itself. This agency relationship (through which the Authorized Agent performs contractual obligations on behalf of the Contractor) does not amend, diminish or modify any of the responsibilities of the Contractor under the Contract. The Contractor agrees and understands that it is solely responsible for ensuring that all of its Authorized Agents comply with the applicable terms and conditions of the Contract. If the Authorized Agent fails to comply with the applicable terms and conditions, the Contractor must, upon written notification from the Contracting Authority, immediately complete and fulfill those obligations at no additional cost to Canada.

This Contract has been executed by the parties.

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

APPENDIX A – DELIVERABLES (estimated requirements)

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**	**Extended 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:

TERMS	DEFINITIONS
"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 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 Canada or the 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 (v) 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/Customer 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.
"Contract"	Means the articles of the 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.
"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.

"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.
"End User"	The term "end user" refers to the consumer of a good or service.
"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 the 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 the 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.
"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 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 are 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: (a) managed services; (b) Training services , (c) private or on premise cloud services; and (d) professional or consulting services that exceed standard public commercially available support services.

"Quick Start"	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 that 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, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), hardware platforms, virtualization platforms, servers, operating systems , web servers, databases, applications, or 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 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: (a) granting usage rights to the software application(s) ("Solutions"); (b) providing Solution Documentation; (c) maintaining, upgrading, and updating the Solution(s); (d) managing incidents and defects to ensure the Solution(s) operate at the applicable service levels; and (e) 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 Infrastructure"	Infrastructure managed by the supplier (or a supplier's subcontractor) in order to offer a SaaS service (e.g. data center, networking, storage, servers, virtualization platform, operating system, middleware, Runtime, data, applications). It also includes the systems, hardware and software used to manage, operate and deliver SaaS infrastructure.
"SaaS Publisher" ("SaaSP")"	Means the entity that owns, operates, maintains and distributes SaaS Solutions.
"Solution Program"	Computing, firmware, routine, code, instruction, script, macro, application programming or other interface, tool, definition of document display, object library, software tool or other instruction or set of instructions to follow for hardware or other software, whether in source code or in object code, expressed in a single or in all languages, including integrated program-human interfaces, SQL and other query languages, HTML and other computer markup languages.
"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 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, and Annex O, Software Usage Rights, including the procedures for determining whether the requirements have been met.
"Submission"	Means the documents that the Supplier submits in response to the Request for Supply Arrangement (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 RFSA issued by

	Canada. It does not include the parent, subsidiaries or other affiliates of the Supplier, or its subcontractors.
"System"	Any combination of hardware and software, including any communications line or network device used to provide the link between this combination of hardware and software related to the services.
"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 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, a SaaS, or a CSP who is also a SaaS.
"Work"	All efforts made to produce a deliverable or to perform or provide a service that the supplier must offer under the terms of the Contract
"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

(a) 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 accessed 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).

(b) 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.

5. Continuous Monitoring

(a) 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:

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

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

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

(iv) Identify unauthorized use and access of any Public Cloud Services, data and components relevant to Canada's Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) Solution;

(v) 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 makes use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

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

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

(b) The Contractor's Public Cloud Services must allow for Government of Canada (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).

(c) 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.

6. Notifications

(a) The Contractor must provide:

(i) Timely notification of any interruption that is expected to impact service availability and performance (as agreed to by the parties and included in the Statement of Requirements (SOR) and/or Service Level Agreement (SLA));

(ii) 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

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

7. Security Incident Response

(a) 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.

(b) 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.

(c) 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/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html). This includes:

(i) Allowing only designated representatives of Canada to have the ability to:

1. 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 Intrusion Detection System (IDS)/Intrusion Protection System (IPS)/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;
2. track the status of a reported information security event or Security Incident.

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

(d) The Contractor must:

(i) 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

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

8. 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.

9. Security Assessment Testing

(a) The Contractor must have a process 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. This includes the ability to conduct regular internal and external scanning related to the GC tenancy, and when there are significant changes to the main platform, to identify any potential system vulnerabilities related to the GC tenancy by performing:

(i) vulnerability scans;

(ii) web application scans, and

(iii) penetration tests.

(b) The Contractor must develop a plan of action and milestones for the Solution to document any planned remedial actions to correct weaknesses or deficiencies to the main platform in order to reduce or eliminate known vulnerabilities in the system, or those that could be related to operation of the GC tenancy.

(c) Upon request of Canada, the Contractor must provide the results of the testing of the overall platform and the plan of action and milestones documentation for planning and any review purposes.

10. Sub-processors

(a) The Contractor must provide a list of Sub-processors that could be used in providing Canada with the Cloud 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 country (or countries) where the Sub-processor would perform the activities required to support the Cloud Services.

(b) The Contractor must provide a list of Sub-processors within ten days of the Contract award date. The Contractor must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processors with access to Customer Data or Personal Data.

11. Supply Chain Risk Management

(a) The Contractor must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide SaaS. This includes, but is not limited to, designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain.

(b) If applicable, the Contractor must have a supply chain risk management approach including a Supply Chain Risk Management (SCRM) Plan that is aligned with one of the following best practices described under the Annex A – Qualification Requirements - Supply Chain Risk Management, mandatory requirement ID; M7 of Tier 1 and M11 of Tier 2:

(i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for Contractor relationships (Parts 1 to 4);
(ii) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
(iii) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan; or
(iv) CSA STAR controls to support CSA CCM Supply Chain Management controls.

(c) Within 90 days of contract award, the Contractor must:

(i) Provide an update that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime;

OR

(ii) Provide Canada with a copy of the SRCM Plan on an annual basis, or upon request of Canada.

In the situation where the Contractor is a SaaS Publisher using a GC-approved IaaS Provider that already complies with Section 11 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS Publisher using a GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed

in the GC-approved IaaS Provider environment for a supply chain integrity (SCI) review. This SCI review will be conducted no sooner than every three years.

12. On-going Supply Chain Integrity Process

(a) The Parties acknowledge that security is a critical consideration for Canada with respect to this Contract and that on-going assessment of SaaS will be required throughout the Contract Period.

(b) The Parties acknowledge that Canada reserves the right to review the native SaaS of any Contractor in whole or in part at any time for supply chain integrity concerns. This acknowledgement does not obligate the Contractor to support the SCI review.

(c) Throughout the Contract Period, the Contractor must provide to Canada information relating to any data breach of the Contractor's network of which it knows, that results in either (a) any unlawful access to Canada's content stored on Contractor's equipment or facilities, or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure or alteration of Canada's content in relation to change of ownership, to the SaaS under this Contract, that would compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications of Canada.

13. Change of Control

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

(b) 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 30 calendar days of receiving Canada's determination, arrange for another subcontractor, acceptable to Canada, to deliver the portion of the Cloud Services being delivered by the existing subcontractor (or the Contractor must deliver this portion of the Cloud Services 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 120 calendar days of receiving the original notice from the Contractor regarding the change of control.

(c) 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 and the resulting termination, and Canada will

only be responsible for paying for those services received up to the effective date of the termination.

(d) 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 Contact pursuant to this Article where the Contractor or subcontractor continues, at all times, to be controlled, directly or indirectly, by the same ultimate owner.

APPENDIX D – PRIVACY OBLIGATIONS

1. Data Ownership and Privacy Requests

(a) 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.

(b) 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 readable document.

2. Assist in Delivery of Canada's Privacy Impact Assessment (PIA)

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.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308) by assisting 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.

3. Privacy Breach

(a) 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 – SaaS Service Level Agreement.

(b) 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.

(c) The Contractor must:

(i) 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

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

APPENDIX E – 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)

See attached the statement of work and the required certificates.

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) Name, Title and Signature of Individual Authorized to sign: Technical Authority: _____ Date: _____	**Signatures (PWGSC)** 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.	

APPENDIX F – SRCL FOR SAAS

(Insert if applicable)

Note to Contractors: Different or additional security levels may apply to Clients using the Supply Arrangement (SA) or their Work requirements, for example, security clearances for Suppliers or Supplier resources. For all Contracts issued against a SA, Clients are required to submit their SRCL to the Contract Security Program: TPSGC.SSILVERS-ISSSRCL.PWGSC@tpsgc-pwgsc.gc.ca prior to Contract award. The Contracting Authority must reference the RFSA – SaaS Method of Supply (GC Cloud) (EN578-191593/F) when submitting their SRCL to the Contract Security Program. In the event that a Contract issued against a SA includes different or additional security levels, they will be included in Appendix F (SRCL for SaaS) and Appendix G (Security Classification Guide) to the Contract.

APPENDIX G – SECURITY CLASSIFICATION GUIDE

(Insert if applicable)

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