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 (GC)	
Solicitation No. - N° de l'invitation EN578-191593/F	**Date** 2019-07-05
Client Reference No. - N° de référence du client 20191593	**Amendment No. - N° modif.** 006
File No. - N° de dossier 003eem.EN578-191593	**CCC No./N° CCC - FMS No./N° VME**
GETS Reference No. - N° de référence de SEAG PW-$EEM-003-35660	
Date of Original Request for Supply Arrangement **Date de demande pour un arrangement en matière d'app. originale**	2019-05-10
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2022-05-10**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
Address Enquiries to: - Adresser toutes questions à: Boyer, Tania	**Buyer Id - Id de l'acheteur** 003eem
Telephone No. - N° de téléphone (613) 858-9232 ( )	**FAX No. - N° de FAX** ( ) -
Delivery Required - Livraison exigée	
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

REQUEST FOR SUPPLY ARRANGEMENT (RFSA)
SAAS METHOD OF SUPPLY (GC CLOUD)
SOLICITATION NUMBER: EN578-191593/F
PUBLIC SERVICE AND PROCUREMENT CANADA (PSPC)

AMENDMENT 006

This Amendment 006 is raised to:

1.0 Respond to questions received regarding the RFSA, as detailed in Section 1.0, below; and
2.0 Make changes to the RFSA as detailed in Section 2.0, below.

1.0 Respond to questions regarding the RFSA:

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

QUESTIONS	ANSWERS
Q.31 Annex A – Qualification Requirements – Tier 1 M5 and Tier 2 M8 (Third Party Assurance) In previous requests from Canada to provide SOC2 Type II security certification reports they were requested to submit directly to CSE Canadian Centre for Cyber Security (CCCS) since these reports have very sensitive Security information. In addition, typically the distribution of these SOC reports is managed by the 3rd party assessor rather than by the cloud service provider and are locked with a security password so that they can only be accessed by the requestor. Would Canada please confirm if it would be acceptable to provide a link to the third party assessor's website to permit Canada to securely access this detailed report? If not, please confirm that submission of these SOC reports directly to CSE CCCS is acceptable to meet this requirement.	**A.31** Canada has considered the request. Tier 1 M5 and Tier 2 M8 entitled "(Third Party Assurance)" of the Annex A, Qualification Requirements, is modified per Section A. REQUEST FOR SUPPLY ARRANGEMENT (RFSA) DOCUMENT (i) and (ii), below.

Q.32 Annex A – Qualification Requirements - Tier 1 M6 (Supply Chain Management) Hyper-scale cloud providers rely upon a number of sub-processor providers to provide and support these services that are provided. These services providers provide a range of services from software development through to customer. Many Hyperscale Cloud providers publish public listings of their sub-processors for the hyperscale providers, and these lists are available for the Government of Canada. As a hyperscale service, it is impractical to have the list of sub-processors be assessed by the CCCS. We suggest that the Crown leverage the supply chain attestation against the NIS 800-161 standard.	**A.32** Canada has reviewed the request and the requirement shall remain the same.
Q.33 Annex A – Qualification Requirements - Tier 1 M11 (Supply Chain Risk Management) According to the internationally recognized secure software development standard, the Crown should specifically ask for SaaS providers be compliant/aligned with is ISO 27034 Information technology — Security techniques — Application security.	**A.33** Canada has reviewed the request and the requirement shall remain the same.
Q.34 Annex A – Qualification Requirements - Tier 1 M13 and Tier 2 M19 (Information Spillage) Monitoring and remediating Information Spills in a SaaS environment are a customer's responsibility. Cloud Service Providers (CSP) by default do not have access to customer data. CSP's provide self-service tools to allow customer administrators to monitor and remediate information spills in a cloud environment. This still enables compliance with IR-9 and associated control enhancements. We ask that Tier 1 M13 and Tier 2 M19 be modified to require SaaS vendors to provide self-service tools to customer administrators for use in an information spillage response. For example:	**A.34** Canada has considered the request. Tier 1 M13 and Tier 2 M19 entitled "(Information Spillage)" of the Annex A, Qualification Requirements, is modified per Section A. REQUEST FOR SUPPLY ARRANGEMENT (RFSA) DOCUMENT (iii), below.

(1) The Supplier must provide Canada with a document that outlines the process to respond to an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Submission; or (ii) another best practice of Leading Service Providers approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for the customer administrator to identify the specific Information Asset that is involved in an Asset's or System's contamination; (b) A process for the customer administrator to isolate and eradicate a contaminated Asset or System; and (c) A process for the customer administrator to identify Assets or Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. Tier 1 M13 and Tier 2 M19 Information Spillage (requirement 2) Given Information Spillage response is a customer responsibility, we ask that requirement (2) "The Supplier must provide an up-to-date information spillage process to Canada on an annual basis" be removed.	
Q.35 Annex A – Qualification Requirements - Tier 2 M13 (Privacy by Design) This requirement needs to be revised as the standard which has been cited doesn't refer to application development nor privacy. The appropriate ISO standard is ISO 27034. ISO 27034 is Information technology -- Security techniques -- Application security. It addresses the Security Development Lifecycle items that the Government of Canada has asked for in the PBMM. ISO 27032 refers to cyberspace security which is not the applicable standard in this case.	**A.35** Canada has considered the request. Tier 2 M13 entitled "(Privacy by Design)" of the Annex A, Qualification Requirements, is modified per Section A. REQUEST FOR SUPPLY ARRANGEMENT (RFSA) DOCUMENT (iv), below.

Q.36 Annex B - Security & Privacy Obligations- Section 5 "(Auditing Compliance for Security Obligations) Cloud providers are unable to comply with this requirement as they do not provide implementation plans and progress on remediation measures to customers. Given that this will also impact third party SaaS providers deployed on global hyper-scale cloud provider platforms, we feel this will have a significant negative impact on the Crown's objectives of providing a rich catalogue of services to the Government Canada. We ask that Annex B, Section 5.2 be removed in its entirety.	**A.36** Canada has considered the request. Section 5 entitled "(Auditing Compliance for Security Obligations)" of the Annex B, Security & Privacy Obligations, is modified per Section A. REQUEST FOR SUPPLY ARRANGEMENT (RFSA) DOCUMENT, Section (v), below.
Q.37 Annex B - Security & Privacy Obligations – Section 7 (Network and Communications Security) Section 7 (b) Does not provide a definition of the Crown's view of microservices. Microservices may refer to a variety of processes along a continuum from those adjacent in the same virtual machine, to those distributed across a public network in a different data center. In addition customers can may choose to configure their customer deployed services to not use encryption (for example, for backwards compatibility customers may, even though not recommended, choose to use deprecated protocols such at HTTP. As a general rule, Hyperscale cloud providers encrypt data in transit between servers where they are wholly in control the communications. Therefore, we are asking the Government of Canada to remove this requirement.	**A.37** Canada has considered the request. Section 7 entitled "(Network and Communications Security)" of the Annex B, Security & Privacy Obligations, is modified per Section A. REQUEST FOR SUPPLY ARRANGEMENT (RFSA) DOCUMENT, Section (vi), below.

Q.38 Annex F - Software as a Service Resulting Contract Clauses Pursuant to Article 4.1 c) Indemnification of the Resulting Contract Clause, Canada requires that the Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any intellectual property infringement claim by a third party based on Canada's use of the Solution. Although the Contractor agrees in principle with the above it wishes to specify that such provision should be modified in order to clarify that the Contractor agrees to defend Canada if a 3rd party claims that the Contractor's SaaS services or deliverables provided to Canada infringe any intellectual property right and to pay all costs, damages and legal fees that a court finally awards, provided that Canada: a) promptly notifies the Contractor in writing of the claim; and b) co-operates with the Contractor in, and allows the Contractor full participation in, the defence and related settlement negotiations; and c) obtains the Contractor's prior approval to any agreement resulting from settlement negotiations held with the third party. In light of the above and given that this provision is related to the limitation of liability clause that PSPC and SSC are developing with the IT industry, this provision should be deleted and replaced when the new Limitation of Liability clause (including the related Intellectual Property Right Infringement provision) as soon as it becomes available (see Note under Article 12 of the Resulting Contract Clauses).	**A.38** Canada has considered the request. Section 4.1 Solution Services (c) entitled "(Indemnification)" of the Annex F, Resulting Contract Clauses, is modified per Section B. ANNEX F - RESULTING CONTRACT CLAUSES DOCUMENT, Section (i), below.

Q.39 Annex F - Software as a Service Resulting Contract Clauses Pursuant to Article 5.6 No Infringement of the Resulting Contract Clause, Canada requires that the Contractor warrants that nothing in the Solution, or in Canada's use of the Solution, will infringe or constitute a misappropriation of the intellectual property or other rights of a third party. Contractor cannot provide such a warranty, however, it can agree to defend Canada in the event of a 3rd party claim for intellectual property infringement. As result, Article 5.6 should be deleted. In addition, given that this provision is related to the limitation of liability that PSPC and SSC are developing with the IT industry, this provision should be replaced when the new Limitation of Liability clause (including the related Intellectual Property Right Infringement provision) as soon as it becomes available (see Note under Article 12 of the Resulting Contract Clauses).	**A.39** Canada requires that Suppliers submit SaaS Publisher and Authorization Forms to certify that, at the time the Supply Arrangement is issued, the Supplier has the requisite authority from any third party IP rights owners. However, Suppliers will be permitted to update their SaaS Catalogue on an ongoing basis and will evolve their commercial offering, and while Canada requires Suppliers to maintain such authority over any deliverables, Canada also requires that suppliers warrant: 1. Having and maintaining all authority to perform the Contract; 2. That SaaS Solution is not known to infringe any third party rights; and, 3. That the Supplier's grant to Canada to access and use a SaaS Solution does not infringe any third party rights. Finally, Canada will continue to require Suppliers to indemnify Canada for any infringement claim against Canada, based on the access and use granted by Suppliers, pursuant to the Contract. Canada recognizes that suppliers cannot control a third party claim being made, but requires suppliers to protect Canada from such claims that result from a Supplier's delivery. Therefore, Section 5.6 entitled "(No Infringement)" is modified per Section B. ANNEX F - RESULTING CONTRACT CLAUSES DOCUMENT, Section (ii), below.
Q.40 Annex A – Qualification Requirements – Tier 1 M3 (Data Centre Facilities) The Supplier requires that Canada either amends or clarifies the following items: (i) sub-paragraph e) requires two forms of identification; given existing policies applicable to commercial cloud offerings,	**A.40** Canada has reviewed the request and the requirement shall remain the same. (i) To clarify the sub-paragraph e) of Tier 1 M3 entitled "(Data Centre Facilities)" of Annex A – Qualification Requirements, the supplier is required to provide at least two (1 foundational and 1 supporting) identification

Supplier requests that only one form of identification be required; and (ii) sub-paragraph i), please clarify the reference to "telework sites"; what does Canada mean by "work from home" and in that case, does Canada expect to be able to inspect an employee's home?	documents, consistent with the TBS Standard on Security Screening. (ii) To clarify the sub sub-paragraph i) of Tier 1 M3 entitled "(Data Centre Facilities)" of Annex A – Qualification Requirements "telework sites"; refers to remote locations where the work is done away from the office. An employee might work from home, from a coffee shop, or from anywhere that is not a regular office. "Work from home" refers to the employee's home. In that case, employees required to have access to protected or classified information from their home, will be subject to a home inspection by Canada. Inspection is mandatory for all physical locations where sensitive government-owned information is kept in hard/soft copy and stored in the employee's home, as applicable. To ensure that the location meets the security requirements, the supplier will have to identify all addresses in which safeguarding information document and/or system informatics are stored.
Q.41 We'd like to point you to the questions in the SSC Cloud RFP related to supply chain integrity. Based on the vendor community concerns below, would the Crown please reconsider the SCSI requirements and modify the Integrity process associated with this RFSA to use industry recognized certifications? Additionally, this would provide consistency between SSC and PSPC.	**A.41** Canada has reviewed the request and the requirement shall remain the same.
Q.42 The Privacy Obligations in Appendix D impose a potential liability on Suppliers and does not provide sufficient information to allow Suppliers to analyze their impacts:	**A.42** Canada has considered the request. (i) Section 1.0 entitled "Auditing Compliance" of the Appendix D, Privacy Obligations, is deleted per Section B. ANNEX F - RESULTING CONTRACT CLAUSES DOCUMENT, Section (iii), below.

(i) Can Canada advise under what circumstances would the Contracting Authority require the Supplier to conduct a privacy audit? (ii) Can Canada advice qualifications (AICPA, CPA Canada, or ISO?) are required by the third party privacy auditor?	(ii) In accordance with Section 5 of "Annex B - Security & Privacy Obligations", As per the mandatory ISO certifications, an audit of such control standard or framework will be initiated at least annually; 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 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. 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.
Q.43 Appendix F (formerly Appendix E) - SECURITY REQUIREMENTS FOR FOREIGN CONTRACTOR We request that Canada confirms that this Appendix F does not apply to a Canadian supplier even if it uses subcontractors and sub-processors located outside of Canada.	**A.43** Canada confirms that Appendix F (formerly Appendix E) – Security Requirement for Foreign Contractor <u>does apply to foreign sub-processors and/or sub-processors</u> located outside of Canada. Canadian supplier using foreign subcontractors and/or sub-processors must must comply with Appendix F - Security Requirement for Foreign Contractor.

2.0 The following clauses and conditions are revised and incorporated into the RFSA:

A. REQUEST FOR SUPPLY ARRANGEMENT (RFSA) DOCUMENT.

(i) **DELETE Requirement of "Tier 1 M5" in its entirety and REPLACE with:**

Requirement
The Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Public Software as a Service, including, implementing information security policies, procedures, and security controls. For 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. 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.

(ii) **DELETE Requirement of "Tier 2 M8" in its entirety and REPLACE with:**

Requirement
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.

Requirement
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-serviceprovider-information-technology-security-assessment-processitsm50100). Any Supplier that has participated in the process must provide documentation to confirm that they have completed the on-boarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS. This will accelerate the qualification process and at the same doesn't require the Supplier to demonstrate the compliance. For 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. 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.

(iii) **DELETE Requirement of "Tier 1 M13 and Tier 2 M19" in its entirety and REPLACE with:**

Requirement
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

Requirement
(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. "

(iv) **<u>DELETE Requirement of "Tier 2 M13" in its entirety and REPLACE with:</u>**

Requirement
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: 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 27034, (iii) ITSG-33, (iv) SAFECode, or (iv) 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.

(v) **<u>DELETE "Section 5" of Annex B - Security & Privacy Obligations in its entirety and REPLACE with:</u>**

5. Auditing Compliance

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

(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.

(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.

(vi) **DELETE "Section 7" of Annex B - Security & Privacy Obligations in its entirety and REPLACE with:**

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 TLS 1.2, or subsequent versions;

(b) Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in 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.

(vii) **DELETE Required to demonstrate compliance of "Tier 2 M9" in its entirety and REPLACE with:**

Required to demonstrate compliance for Tier 2
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 a included; GC Security Control Profile for Cloud-Based GC IT Services , and Industry Certification in Third-Party Assurance detailed under Tier 2 M8.

B. ANNEX F - RESULTING CONTRACT CLAUSES DOCUMENT.

(i) **DELETE Section "4.1 Solution Services (c)" in its entirety and REPLACE with:**

(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,

1. the Supplier must immediately do one of the following:

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

   b) 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;

   c) 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.

   d) 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. "

(ii) **DELETE Section "5.6 No Infringement." in its entirety and REPLACE with:**

" 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. "

(iii) **DELETE Section "1.0 Auditing Compliance" of Appendix D – Privacy Obligations in its entirety.**

(iv) **DELETE Section "7.5 Right to Terminate" in its entirety and REPLACE with:**

7.5 " Rights & Remedies

7.5.1 Rights are Cumulative

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

7.5.2 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 Breach**: 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 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.

7.5.3 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 Contract. The Notice will identify the effective date of termination, the affected Work or Services (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.

b. **Services.**

i. For subscription Services paid monthly in advance, Canada will forego its right to claim the unliquidated portion of an advance payment at the date of the termination; and

ii. For Services on annual subscriptions or with defined Contract Periods, with annual advance payments, Canada will forego its right to claim that part of the portion of an advance payment that is unliquidated at the last day of the month following date of the termination.

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."

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