**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**<br>RFSA - SaaS Method of Supply (GC) | |
| **Solicitation No. - N° de l'invitation**<br>EN578-191593/F | **Date**<br>2020-04-22 |
| **Client Reference No. - N° de référence du client**<br>20191593 | **Amendment No. - N° modif.**<br>013 |
| **File No. - N° de dossier**<br>003eem.EN578-191593 | **CCC No./N° CCC - FMS No./N° VME** |
| **GETS Reference No. - N° de référence de SEAG**<br>PW-$EEM-003-35660 | |
| **Date of Original Request for Supply Arrangement**<br>**Date de demande pour un arrangement en matière d'app. originale** | 2019-05-10 |
| **Solicitation Closes - L'invitation prend fin**<br>**at - à 02:00 PM**<br>**on - le 2022-05-10** | **Time Zone**<br>**Fuseau horaire**<br>Eastern Daylight Saving Time EDT |
| **Address Enquiries to: - Adresser toutes questions à:**<br>Boyer, Tania | **Buyer Id - Id de l'acheteur**<br>003eem |
| **Telephone No. - N° de téléphone**<br>(613) 858-9232 ( ) | **FAX No. - N° de FAX**<br>( ) - |
| **Delivery Required - Livraison exigée** | |
| **Destination - of Goods, Services, and Construction:**<br>**Destination - des biens, services et construction:** | |
| **Security - Sécurité**<br>This revision does not change the security requirements of the solicitation.<br>Cette révision ne change pas les besoins en matière de sécurité de l'invitation. | |

**Instructions: See Herein**

**Instructions: Voir aux présentes**

| | | |
|---|---|---|
| **Acknowledgement copy required**<br>**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. 013 to Request for Supply Arrangement (RFSA) for

# SaaS Method of Supply (GC CLOUD)

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

| THIS AMENDMENT 013 IS RAISED TO: |
|---|
| 1.0 Respond to questions received regarding the RFSA, as detailed in Section 1.0, below. |

**1.0 Respond to questions regarding the RFSA**

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

| QUESTIONS | ANSWERS |
|---|---|
| **Q.57** Should Suppliers who onboarded into the first round of CCCS IT Security Assessment Program (the first intake window occurred between February 10 and March 6, 2020 inclusively) expect any delays in having their assessments completed due to the COVID-19 situation? | **A.57** CCCS has advised that there will be a delay of approximately one month in completing the ITS and SCI Assessments for the SaaS RFSA due to COVID-19. As a result, it is anticipated that the next onboarding process will begin in October 2020. Suppliers will be notified of the time and date of opening and closing of the second round of onboarding via buyandsell.gc.ca. |
| **Q.58** For M8 (Third Party Assurance), Tier 2 of Annex A. If a cloud service provider is ISO27001, SOC 2 Type II (Security trust principle), and Payment Card Industry Data Security Standard (PCI DSS) compliant, can the PCI certification be used in lieu of remaining trust principles of SOC 2 Type II as required by Annex A (i.e., availability, confidentiality, processing integrity), given the overlap between PCI and SOC 2 Type II controls? | **A.58** At this time the GC is not accepting any other certifications as equivalencies to those indicated as mandatory in Annex A – Qualification Requirements. |
| **Q.59** In Amendment 12, QA 54 M7 Supplier Chain Risk Management, Tier 1 the question was asked if PSPC would accept FedRAMP certification (an American-based standard Risk Management approach for Cloud Service Providers) as demonstration of compliance based on the fact that the FedRAMP program is supported by NIST, is compatible with ITSG-33 and is referenced in the Government of Canada Cloud Security Risk Management Approach and Procedures. The response PSPC provided was, "At this time the GC is not able to accept another government's assessment process as an equivalent standard".<br><br>Will PSPC please provide more detail as to why FedRAMP is not acceptable especially given the fact that the GC Cloud Security Risk Management Approach and Procedures under section 2.2 – Foundational Frameworks FedRAMP is referenced as being one of the information system security risk management standards that was used to develop the GC risk management approach. | **A.59** This level of reciprocity for another government process requires a government to government agreement which is not currently in place. Thus, the use of base level industry standards have been selected for the Canadian program. |
| **Q.60** Amendment 10, question sixteen, asks whether a VAR could qualify under this vehicle for Protected A even before the SaaS publisher is qualified for the same product. The answer states, "Yes, as matter of fact, the software publisher does not necessarily need to qualify. A VAR can hold a Supply Arrangement for a Software Publisher's products without the Software Publisher ever qualifying for a SA for those products."<br>a) Please confirm if the Software Publisher who is not responding to this RFSA but whose software is being submitted on a VAR's response must also adhere to the CCCS SaaS IT Security Assessment Program: Onboarding Process (Annex A, M5 Third Party Assurance / Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process)?<br>b) Please confirm if the Software Publisher who is not responding to this RFSA but whose software is being submitted on a VAR's response must also adhere to M7 Supply Chain Risk Management requirements. | **A.60** SaaS Publishers who are not responding to the RFSA but whose software is being submitted as part of a VAR's response must jointly participate in the onboarding with CCCS before their products can be resold by that VAR. All information for the CCCS SaaS ITS Assessment should be provided for the SaaS Publisher at the application layer and for the Cloud Service Provider for the infrastructure layer.<br><br>The VAR would only be assessed on the Supply Chain Integrity (SCI) and organizational/personnel clearances (CISD).<br><br>PSPC also confirms that CCCS requires the SaaS Publisher's certifications as detailed in the Annex A, Qualification Requirements, M5 - Third Party Assurance to complete the assessment.<br><br>For further information on the CCCS SaaS IT Security Assessment onboarding process please contact: contact@cyber.gc.ca. |

| QUESTIONS | ANSWERS |
|---|---|
| **Q.61** Amendment 12, Question and Answer 53 regarding M5 (Third Party Assurance) Tier 1 asks whether PSPC will accept the Cloud Security Alliance CAIQ self-assessment as an alternative to the Cloud Security Alliance CCM self-assessment? The response provided was "For Tier 1, up to Protected A, GC is ready to accept the CCM Level 1 self-assessment responses. For Tier 2, up to Protected B, GC requires the CCM Level 2 assessment performed by a certified 3rd party auditor in order to assess in detail the available report." We are seeking further clarification on this response:<br><br>Does this mean that PSPC will accept a completed CSA CAIQ questionnaire to meet this requirement? If so, are Software Publishers to also register in the CSA STAR Registry or is just the completed CSA CAIQ questionnaire sufficient? If a completed CSA CAIQ questionnaire is not acceptable please specific information on what would satisfy this requirement for Tier 1, up to Protected A. | **A.61** Self assessments require the questionnaire and associated report from an accredited auditor. A completed questionnaire as done by a third party auditor is what is required. Completion of one of the ISO or SOC certifications would be accepted. |
| **Q.62** In lieu of the Cloud Security Alliance Self-Assessment referenced in Annex A, Requirement M5 - Third Party Assurance for Tier 1, would you be willing to accept any of the following: - ISO 27001 - ISO 27017 - ISO 27018 - - PCI-DSS - - SOC 1 (SSAE16/ISAE 3402, previously SAS 70) - - SOC 2 & SOC 3. | **A.62** As per Annex A – Qualification Requirements, M5 - Third Party Assurance for Tier 1 (up to Protected A), compliance must be demonstrated by providing one or more of the following industry certifications identified below, and validated through independent third party assessments.<br><br>The Supplier must provide the following industry certifications for the proposed Service to demonstrate compliance:<br><br>(a) One of the following:<br><br>(i) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; or<br>(ii) AICPA Service Organization Control (SOC) 2 Type II<br>AND<br><br>(b) Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version.<br><br>Each provided certification and assessment report must:<br><br>1. Be valid as of the Submission date;<br>2. Identify the legal business name of the proposed Supplier, and applicable Supplier Sub-processor, including CSP;<br>3. Identify the current certification date and/or status;<br>4. Identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report.<br>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 such as data centre hosting, the subservice organization's assessment report must be included; and<br>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.<br><br>Please note:<br>• Certifications must be provided for all portions of the proposed Service identified;<br>• Certifications must be accompanied by assessment reports; and |

| QUESTIONS | ANSWERS |
|---|---|
| | • Certifications must be valid and within the 12 months prior to the start of a contract.<br><br>At this time the GC is not accepting any other certifications as equivalencies to those indicated as mandatory in Annex A – Qualification Requirements. |