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 DAMA - Logiciels-services SaaS	
Solicitation No. - N° de l'invitation EN578-191593/F	**Date** 2020-04-22
Client Reference No. - N° de référence du client 20191593	**Amendment No. - N° modif.** 013
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

SERVICES PUBLICS ET APPROVISIONNEMENT CANADA (SPAC)

Modification nº 013 à la demande d'arrangement en matière d'approvisionnement (DAMA) pour

une méthode d'approvisionnement de logiciels-services (Infonuagique GC)

Nº de l'invitation sur le site d'Achatsetventes : EN578-191593/F

LA MODIFICATION N^{O} 013 VISE À :
1.0 Répondre aux questions reçues au sujet de la DAMA, qui sont reportées à la section 1.0 ci-dessous.

1.0 Réponses aux questions reçues au sujet de la DAMA

Remarque : les questions peuvent avoir été modifiées ou résumées.

QUESTIONS	RÉPONSES
Q.57 Les fournisseurs qui se sont joints à la première ronde du programme d'évaluation de la sécurité des TI du CCC (la première période d'intégration allant du 10 février au 6 mars 2020 inclusivement) doivent-ils s'attendre à des retards dans leur évaluation en raison de la pandémie de COVID-19?	**R.57** Le CCC a annoncé qu'il y aura un retard d'environ un mois pour faire les évaluations de la sécurité des TI et de la SCI pour la DAMA relative aux logiciels-services en raison de la COVID-19. En conséquence, il est prévu que le prochain processus d'intégration commence en octobre 2020. Les fournisseurs seront avisés de la date et de l'heure de début et de fin de la deuxième ronde d'intégration sur Achatsetventes.gc.ca.
Q.58 Concernant O8 (Assurance d'une tierce partie) au palier 2 dans l'annexe A, si un fournisseur de services infonuagiques est conforme aux normes ISO27001, SOC 2 de type II (principe de confiance de sécurité) et Payment Card Industry Data Security Standard (PCI DSS), la certification PCI peut-elle être utilisée au lieu des principes de confiance restants (disponibilité, intégrité du traitement et confidentialité) de SOC 2 de type II, comme requis par l'annexe A, étant donné le chevauchement des contrôles PCI et SOC 2 de type II?	**R.58** Pour le moment, le GC n'accepte aucune autre certification comme équivalente à celles mentionnées comme obligatoires à l'annexe A – Exigences de qualification.
Q.59 Dans la modification 12, à la question 54, au sujet du critère O7 Gestion des risques de la chaîne d'approvisionnement, palier 1, il a été demandé si SPAC accepterait la certification FedRAMP (une norme américaine pour la gestion des risques par les fournisseurs de services infonuagiques) comme démonstration de conformité puisque le programme FedRAMP est appuyé par le NIST, est compatible avec ITSG-33 et est cité dans le document *Approche et procédures de gestion du risque en matière de sécurité de l'informatique en nuage* du gouvernement du Canada. SPAC a répondu : « À l'heure actuelle, le gouvernement du Canada n'est pas en mesure d'accepter le processus d'évaluation d'un autre gouvernement comme norme équivalente ». SPAC peut-il expliquer plus en détail pourquoi la certification FedRAMP n'est pas acceptable, surtout en considérant que le document *Approche et procédures de gestion du risque en matière de sécurité de l'informatique en nuage* du GC, à la section 2.2 – Cadres de fondement, dit que FedRAMP est une des normes en gestion du risque en matière de sécurité des systèmes d'information qui a été utilisée pour développer l'approche de gestion des risques du GC?	**R.59** Ce niveau de réciprocité pour un processus d'un autre gouvernement exige une entente intergouvernementale qui n'existe pas actuellement. Par conséquent, des normes de base de l'industrie ont été choisies pour le programme canadien.
Q.60 Dans la modification 10, la question 16 demande si un revendeur de produits modifiés (RPM) pourrait, dans le cadre de cet instrument, bénéficier du niveau Protégé A avant même que l'éditeur du logiciel ne soit reconnu pour le même produit. La réponse affirme : « Oui, absolument. En fait, l'éditeur de logiciels ne doit pas nécessairement remplir les conditions requises. Un RPM peut détenir un arrangement en matière d'approvisionnement (AMA) pour les produits d'un	**R.60** Les éditeurs de logiciels-services qui ne répondent pas à cette DAMA, mais dont le logiciel est proposé dans la réponse d'un RPM, doivent participer conjointement à l'intégration avec le CCC avant que leurs produits puissent être revendus par un RPM. Toute l'information pour l'évaluation de la sécurité des TI en logiciels-services du CCC devrait être fournie par l'éditeur de logiciels-services pour la couche

QUESTIONS	RÉPONSES
éditeur de logiciels sans que ce dernier se qualifie pour un AMA pour ces produits. » a) Veuillez préciser si l'éditeur de logiciels qui ne répond pas à cette DAMA, mais dont le logiciel est proposé dans la réponse d'un RPM, doit aussi adhérer au programme d'évaluation de la sécurité des TI en logiciels-services du CCC : processus d'intégration (Annexe A, O5 Assurance d'une tierce partie/Annexe L – Programme d'évaluation de la sécurité des TI en logiciels-services : processus d'intégration). b) Veuillez préciser si l'éditeur de logiciels qui ne répond pas à cette DAMA, mais dont le logiciel est proposé dans la réponse d'un RPM, doit aussi se conformer aux exigences du critère O7 Gestion des risques de la chaîne d'approvisionnement.	application et par le fournisseur de services infonuagiques pour la couche d'infrastructure. Le RPM serait seulement évalué sur l'intégrité de la chaîne d'approvisionnement (SCI) et sur les habilitations de sécurité pour l'organisation et le personnel délivrées par la DSIC. SPAC confirme aussi que le CCC exige les certifications de l'éditeur de logiciels, comme précisé à l'annexe A, Exigences de qualification, O5 Assurance d'une tierce partie, pour achever l'évaluation. Pour obtenir plus d'information sur le processus d'intégration au programme d'évaluation de la sécurité des TI en logiciels-services du CCC, veuillez écrire à l'adresse suivante : contact@cyber.gc.ca.
Q.61 Dans la modification 12, au sujet du critère O5 Assurance d'une tierce partie, niveau 1, la question 53 demande si SPAC acceptera l'autoévaluation CAIQ de la Cloud Security Alliance comme solution de rechange à l'autoévaluation CCM de la Cloud Security Alliance. La réponse est la suivante : « Pour le niveau 1, jusqu'au niveau de sécurité Protégé A, le gouvernement du Canada est prêt à accepter les réponses d'autoévaluation du niveau 1 de l'outil CCM. En ce qui concerne le niveau 2, jusqu'au niveau de sécurité Protégé B, le gouvernement du Canada exige qu'une évaluation CCM de niveau 2 soit effectuée par un vérificateur tiers certifié en vue d'évaluer en détail le rapport. » Nous demandons une clarification de cette réponse : Cela signifie-t-il que SPAC acceptera un questionnaire rempli d'autoévaluation CAIQ de la CSA comme preuve de satisfaction de cette exigence? Si c'est le cas, les éditeurs de logiciels doivent-ils aussi s'inscrire au registre STAR de la CSA ou le questionnaire rempli d'autoévaluation CAIQ est-il suffisant? Si ce questionnaire n'est pas acceptable, veuillez précisez ce qui répondrait à cette exigence pour le niveau 1 jusqu'à Protégé A.	**R.61** Les autoévaluations exigent le questionnaire et le rapport connexe d'un vérificateur tiers certifié. Un questionnaire rempli par un vérificateur tiers certifié est requis. L'obtention d'une des certifications ISO ou SOC serait acceptée.
Q.62 Au lieu de l'autoévaluation offerte par la Cloud Security Alliance mentionnée à l'annexe A, critère O5 — Assurance d'une tierce partie au niveau 1, accepteriez-vous l'une des certifications suivantes : ISO 27001, ISO 27017, ISO 27018, PCI-DSS, SOC 1 (SSAE16/ISAE 3402, auparavant SAS 70), SOC 2 et SOC 3?	**R.62** Selon l'annexe A – Exigences de qualification, O5 Assurance d'une tierce partie au niveau 1 (jusqu'à Protégé A), la conformité doit être démontrée en fournissant l'une ou plusieurs des certifications industrielles suivantes, validées par des évaluations indépendantes par des tiers. Le fournisseur doit présenter les certifications suivantes de l'industrie afin de démontrer la conformité du service proposé : (a) l'une des suivantes : (i) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, ou (ii) contrôle de l'organisation des services (SOC) de l'AICPA – rapports des SOC 2 de type II; ET (b) une autoévaluation de ses services par rapport à la version 3.01 (ou une version ultérieure) de la

QUESTIONS	RÉPONSES
	matrice des contrôles infonuagiques (MC) de la Cloud Security Alliance (CSA). Chaque rapport de certification et d'évaluation fourni doit : 1. être valide à la date de soumission; 2. indiquer la dénomination sociale du fournisseur proposé et du sous-traitant du fournisseur, s'il y a lieu, y compris le fournisseur de services infonuagiques; 3. indiquer la date ou l'état de la certification actuelle; 4. comprendre la liste des biens, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification; 5. indiquer les emplacements et les services offerts par le fournisseur proposé. Si la méthode déterminée est utilisée pour exclure les organisations de services en sous-traitance, comme l'hébergement de centres de données, le rapport d'évaluation de l'organisation sous-traitante doit être inclus; 6. être délivré par un tiers indépendant qualifié au titre de l'AICPA ou de CPA Canada ou du régime de certification ISO, et respecter la norme ISO/IEC 17020 relativement aux systèmes de gestion de la qualité. Remarque : • Les certifications doivent être fournies pour toutes les parties du service proposé. • Les certifications doivent être accompagnées de rapports d'évaluation. • Les certifications doivent être valides et avoir été émises dans les 12 mois précédant le début du contrat. Pour le moment, le GC n'accepte aucune autre certification comme équivalente à celles mentionnées comme obligatoires à l'annexe A – Exigences de qualification.