RETOURNER LES SOUMISSIONS À :

IRCC.BidsReceiving-Receptiondessoumissions.IRCC@cic.gc.ca

Attn : Jasdeep Jande

POUR LES SOUMISSIONS ÉLECTRONIQUES
La boîte de courrier électronique est automatisée pour envoyer une réponse pour chaque message qu'elle reçoit. Si vous ne recevez pas de réponse à votre courriel, veuillez svp contacter l'autorité contractante pour assurer que votre soumission a bien été reçue. Notez bien que c'est la responsabilité du soumissionnaire d'assurer que leurs soumissions soient reçues dans leur intégralité, par Citoyenneté et Immigration Canada, par la date et heure stipulé dans cette demande de proposition.

AVIS IMPORTANT AUX FOURNISSEURS
Le Service électronique d'appels d'offre du gouvernement sur achatsetventes.gc.ca/appels-d-offres sera la source unique faisant autorité pour les appels d'offres du gouvernement du Canada assujettis aux accords commerciaux ou aux politiques ministérielles qui exigent que les appels d'offres soient annoncés publiquement.

DEMANDE DE PROPOSITION
Proposition à : Citoyenneté et Immigration Canada
Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici et sur toute feuille ci-annexée, au(x) prix indiqué(s).

CE DOCUMENT CONTIENT UNE EXIGENCE DE SÉCURITÉ
Instructions: See Herein
Instructions : Voir aux présentes
Issuing Office – Bureau de délivrance
Citoyenneté et Immigration Canada
Service de l'approvisionnement et des contrats
70, rue Crémazie
Gatineau (Québec) K1A 1L1

Title – Sujet Système de gestion de l'apprentissage (SGA) organisationnel infonuagique pour utilisation à l'échelle du ministère Immigration, Réfugiés et Citoyenneté Canada (IRCC)	
Solicitation No. – N° de l'invitation **CIC-152202**	**Date** **24 juin 2021**
Amendment No. – N° de modification **003**	
Solicitation Closes – L'invitation prend fin at – à *2:00***PM** **on – le 6 juillet 2021**	**Time Zone** **Fuseau horaire** **HAE**
F.O.B. - F.A.B. **Plant-Usine :** ☐ **Destination :** ☐ **Other-Autre :** ☐	
Address Inquiries to: – Adresser toute question à : **IRCC.BidsReceiving-Receptiondessoumissions.IRCC@cic.gc.ca**	
Telephone No. – N° de téléphone : **343-574-4425**	
Destination – of Goods, Services, and Construction: **Destination – des biens, services et construction :** Voir aux présentes	
Delivery required – Livraison exigée ***Voir aux présentes***	
Vendor/firm Name and address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Facsimile No. – N° de télécopieur** **Telephone No. – N° de téléphone**	
Name and title of person authorized to sign on behalf of Vendor/firm **Nom et titre de la personne autorisée à signer au nom du fournisseur/de l'entrepreneur** _____ **(type or print)/ (taper ou écrire en caractères d'imprimerie)** _____ _____ **Signature** **Date**	

Canada

Modification 003 – RFP CIC-152202

Modification 003 est soulevé pour:

1. **Mettre à jour la Partie 3 – Instructions pour la préparation des soumissions ;**
2. **Mettre à jour la Partie 5 – Attestations et renseignements supplémentaires**
3. **Mettre à jour l'appendice B – Conditions supplémentaires**
4. **Mettre à jour l'appendice D – Énoncé des travaux;**
5. **Mettre à jour l'annexe A à l'appendice D – Énoncé des exigences de SGA IRCC ;**
6. **Mettre à jour l'appendice G – Obligations en matière de sécurité et de la privée ;**
7. **Mettre à jour l'appendice H – Processus d'intégrité de la chaîne d'approvisionnement ;**
8. **Mettre à jour l'appendice K – Entente de non-divulgation relatif à l'intégrité de la chaine d'approvisionnement ;**
9. **Mettre à jour l'appendice M –– Exigences relatifs à la sécurité Niveau 1;**
10. **Mettre à jour l'appendice M –– Exigences relatifs à la sécurité - Niveau 2; et**
11. **Mettre à jour l'appendice L - Programme d'évaluation de la sécurité des TI des logiciels-services: processus d'intégration.**

---

1. **PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS**

Partie 3, sous-article 3.2 c) vii Conformité à l'Appendice G - Obligations en matière de sécurité et protection de la vie privée est supprimé dans son intégralité et remplacé par :

> vii **Conformité à l'Appendice G - Obligations en matière de sécurité et protection de la vie privée:** Les fournisseurs doivent se conformer aux obligations de sécurité et de confidentialité figurant à l'Appendice G - Obligations en matière de sécurité et protection de la vie privée. Les fournisseurs doivent démontrer qu'ils respectent les obligations de sécurité et de confidentialité décrites à l'Appendice G en répondant aux exigences obligatoires détaillées à l'appendice M – Niveau 1 – Exigences de sécurité pour logiciel-service. Les fournisseurs peuvent être invités à démontrer leur conformité continue à l'appendice G – Obligations en matière de sécurité et protection de la vie privée sur demande pendant toute la durée du contrat.

2. **PARTIE 5 – ATTESTATIONS ET RENSEGNEMENTS SUPPLÉMENTAIRES**

Sous-article 5.2.4 *Confirmation de l'inscription au Programme d'évaluation de la sécurité des logiciels services* est supprimé dans son intégralité.

3. APPENDICE B – CONDITIONS SUPPLÉMENTAIRES

Le sous-article B16.3 d) est supprimé dans son intégralité.

4. APPENDICE D – ÉNONCÉ DES TRAVAUX

Sous-article D6. Limitations et contraintes est supprimé dans son intégralité et remplacé par :

D6. Limites et contraintes

L'entrepreneur doit respecter les exigences de sécurité énoncées dans le *Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.htm)*, qui est un ensemble complet de lignes directrices et de mesures fondées sur le guide ITSG-33. La solution de l'entrepreneur doit respecter le *Profil des mesures de sécurité pour les services du GC fondés sur l'informatique en nuage* en offrant l'un de ces éléments :

- Rapport SOC-2 ou SOC-3 valide (ISAE-3402);
- Certification ISO 27001;
- Conformité avec la Publication 800-53 de l'U.S. National Institute of Standards and Technology (NIST);
- Au cours de la période initiale du contrat, l'entrepreneur doit démontrer la conformité à l'appendice M - Niveau 2 – Exigences de sécurité pour logiciel-service.

5. ANNEXE A à APPENDICE D –Énoncé des exigences de SGA IRCC

L'annexe A à l'annexe D a été mise à jour. Veuillez-vous reporter à la modification 001 de l'annexe A à l'annexe D, incluse en pièce jointe.

6. APPENDICE G – Obligations en matière de sécurité et protection de la vie privée

L'appendice G, sous-article 6 - Programme d'évaluation de la sécurité des TI des fournisseurs de services infonuagiques est supprimée dans son intégralité et remplacée par :

6. Programme d'évaluation de la sécurité des TI des fournisseurs de services infonuagiques

a Pendant la durée **initiale** du contrat, l'entrepreneur doit respecter les exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité pour les services de TI du gouvernement du Canada (GC) fondés sur l'infonuagique pour les renseignements classés « PBMM » (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) selon la portée des services infonuagiques offerts par l'entrepreneur.

b La conformité sera évaluée et validée par IRCC conformément aux lignes directrices du CCCS pour les évaluations de sécurité informatique localisées. https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux

L'entrepreneur doit démontrer qu'il a participé au processus, c'est-à-dire qu'il a intégré le programme, qu'il y a participé et qu'il l'a terminé. Il doit notamment fournir les documents suivants :

i. Une copie de la lettre de confirmation stipulant qu'il a intégré le programme;
ii. Une copie du rapport d'évaluation le plus récent fourni par le CCC;
iii. Une copie du rapport sommaire le plus récent fourni par le CCC.

L'entrepreneur devrait communiquer avec le service à la clientèle du CCC, comme il est indiqué à l'appendice L, Programme d'évaluation de la sécurité des TI de SaaS, pour obtenir tout renseignement supplémentaire concernant le Programme d'évaluation de la sécurité des technologies de l'information (STI) s'appliquant aux FSI.

L'entrepreneur des services infonuagiques proposés a l'obligation continue d'aviser le CCC lorsqu'il y a d'importants changements à la prestation des services de sécurité des TI à l'appui des services offerts par l'entrepreneur.

Les certifications sont présentées ci-dessous et validées au moyen d'évaluations de tiers indépendants.

c Dans les cas où l'entrepreneur est un fournisseur de SaaS utilisant un fournisseur d'IaaS approuvé par le GC qui se conforme déjà aux exigences de l'article 4 – Assurance d'une tierce partie et des sous-sections (1) et (2) de l'article 6 – Programme d'évaluation de la sécurité des TI des fournisseurs de services infonuagiques, le fournisseur de SaaS doit présenter au Canada une copie d'un message électronique fourni par le CCC, confirmant que l'entrepreneur a terminé le Programme d'évaluation de la STI s'appliquant aux FSI du CCC. Le message doit énoncer que le FSI a été évalué par le Programme d'évaluation de la STI s'appliquant aux FSI et qu'il a obtenu un rapport final concernant l'évaluation.

7. APPENDICE H – PROCESSUS D'INTÉGRITÉ DE LA CHAINE D'APPROVISIONNEMENT

Le sous-article 1.1 de l'appendice H est supprimé dans son intégralité et remplacé par :

1.1 Exigences relatives à la présentation des soumissions (obligatoires à la date de clôture de la demande de soumissions). Les soumissionnaires doivent joindre à leur soumission, au plus tard à la date de clôture de la demande de soumissions, l'ISCA suivante :

1.1.1 Liste des produits informatiques: Les fournisseurs doivent identifier les solutions logiciel-service sur lesquelles les données du Canada seraient transmises et / ou stockées, qui seront utilisées et / ou installées pour exécuter toute partie des travaux et / ou des services décrits dans le contrat subséquent, en ce qui concerne la solution logiciel-service, en complétant le modèle de soumission du formulaire 3-SCI fourni dans la DDP, qui comprend les informations suivantes:

a. **Nom OEM**: Entrez le nom du fabricant de l'équipement d'origine (OEM) du produit commandé
b. **Numéro OEM DUNS**: Entrez le numéro DUNS du fabricant OEM. Le système de numérotation universelle des données (DUNS) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer le pointage de crédit d'une entreprise. Si la société ne possède pas de numéro DUNS ou si vous ne parvenez pas à vous en procurer un, veuillez compléter les informations demandées sous «C - Informations sur la propriété». Les informations sur la propriété comprennent les 5 premiers, en pourcentage, les investisseurs et les propriétaires de l'entreprise. Les noms fournis aux investisseurs et aux propriétaires doivent être ceux qui figurent dans les documents d'investissement ou de propriété de la société en question.
c. **Nom du produit**: entrez le nom du fabricant OEM pour le produit.
d. **Numéro de modèle**: Entrez le modèle OEM et / ou le numéro de version du produit.
e. **URL du produit**: entrez l'URL de la page Web du fabricant pour le produit.
f. **Informations sur la vulnérabilité**: Saisissez les informations concernant les 5 derniers problèmes de sécurité signalés concernant le produit. Si le fabricant OEM publie ces informations sur le site Web CVE, indiquez les numéros CVE séparés par des points-virgules (;). Si le fabricant OEM ne publie pas ces informations sur le site Web de CVE, vous devrez lui demander directement des informations sur les failles de sécurité et les fournir au IRCC. Si tel est le cas pour un produit particulier, entrez "voir les informations jointes" dans le champ Informations sur la vulnérabilité et incluez le ou les noms de fichier dans la colonne d'informations supplémentaires fournissant les informations de vulnérabilité requises

8. APPENDICE K – ENTENTE DE NON-DIVULGATION DE SPAC RELATIF A L'INTÉGRITÉ DE LA CHAINE D'APPROVISIONNEMENT est par la présente supprimée dans son intégralité et remplacée par :

L'appendice K – Entente de non-divulgation relatif à l'intégrité de la chaine d'approvisionnement*:*

Note aux fournisseurs: Veuillez noter que cet accord de non-divulgation couvre uniquement les exigences de SCI en vertu de l'article 3.6, Section IV: Exigences relatives à l'intégrité de la chaîne d'approvisionnement.

Entente de non-divulgation

En présentant une réponse, l'entrepreneur doit accepter les modalités de l'entente de non-divulgation cidessous (l'« Entente de non-divulgation ») :

1. L'entrepreneur accepte d'assurer la confidentialité de toute information qu'il reçoit du Canada au sujet de l'évaluation qu'a faite ce dernier de l'information sur la sécurité de la chaîne d'approvisionnement fournie par l'entrepreneur (l'« information sensible »), y compris, sans toutefois s'y limiter, les aspects de l'information sur la sécurité de la chaîne d'approvisionnement qui soulèvent des préoccupations, et les raisons qui ont mené aux interrogations du Canada à cet égard.

L'information sensible comprend, mais pas exclusivement, les documents, instructions, directives, données, éléments matériels, avis ou autres, qu'ils aient été reçus verbalement, sous forme imprimée ou d'une autre façon ou qu'ils soient ou non considérés comme classifiés, exclusifs ou sensibles.

2. L'entrepreneur convient de ne pas reproduire, copier, divulguer, publier ou communiquer, en tout ou en partie, de quelque façon que ce soit, de l'information sensible à une autre personne qu'un employé d'entrepreneur détenant une habilitation de sécurité correspondant à la sensibilité de l'information consultée, sans le consentement écrit préalable de l'autorité de la sécurité de la chaîne d'approvisionnement. L'entrepreneur accepte d'aviser immédiatement l'autorité de la sécurité de la chaîne d'approvisionnement dès qu'une personne, autre que celles autorisées en vertu du présent article, accède à de l'information sensible.

3. Toute l'information sensible demeure la propriété du Canada et doit être retournée à l'autorité de sécurité de la chaîne d'approvisionnement ou détruite à la demande de cette dernière dans les 30 jours suivant cette demande.

4. L'entrepreneur, est conscient qu'un manquement à cette entente de non-divulgation peut entraîner sa disqualification à l'étape de l'arrangement en matière d'approvisionnement (AMA), ou une résiliation immédiate du contrat subséquent. L'entrepreneur reconnaît également que toute violation de cette entente de non-divulgation peut entraîner un examen de sa cote de sécurité ainsi qu'un examen de son statut en tant que soumissionnaire admissible pour d'autres besoins.

5. La présente entente de non-divulgation demeure en vigueur indéfiniment.

9. APPENDICE M – EXIGENCES RELATIFS A LA SÉCURITÉ NIVEAU 1 POUR LOGICIEL-SERVICE

L'annexe M Obligatoire ID O5 – Assurance d'une tierce partie est supprimée dans son intégralité et remplacée par :

O5	**Assurance d'une tierce partie**	Le logiciel-service doit être conçu et développé pour assurer la sécurité du logiciel-service public commercial proposé, y compris la mise en oeuvre de politiques, de procédures et de contrôles de sécurité de l'information	Le fournisseur doit présenter une documentation au Canada démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences relatives l'assurance d'une tierce partie. La conformité doit être démontrée par la présentation d'au moins une des certifications de l'industrie énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants. Le fournisseur doit présenter les certifications suivantes de l'industrie afin de démontrer la conformité du service proposé : 1. l'une des certification suivantes : i. ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, ii. contrôle de l'organisation des services (SOC) de l'AICPA – rapports des SOC 2 de type II; 2. autoévaluation ou évaluations par des auditeurs externes, de ses services par rapport à la version 3.01 (ou une version ultérieure) de la matrice des contrôles infonuagiques (MC) de la Cloud Security Alliance (CSA). Chaque rapport de certification et d'évaluation fourni doit : a. être valide à la date de cloture de la soumission. b. indiquer la dénomination sociale du fournisseur proposé et du soustraitant du fournisseur, s'il y a lieu, y compris le fournisseur de services infonuagiques, c. indiquer la date ou l'état de la certification actuelle, d. comprendre la liste des biens, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification, e. 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 soustraitante doit être inclus, et f. 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.

10. L'APPENDICE M –– EXIGENCES RELATIFS A LA SÉCURITÉ NIVEAU 2 POUR LOGICIEL-SERVICE

L'appendice M Obligatoire ID O8 – Assurance d'une tierce partie est supprimée dans son intégralité et remplacée par :

O8	**Assurance d'une tierce partie**	Le logiciel sous forme de service commercialement disponible doit être conçu et élaboré pour garantir la sécurité du logiciel-service commercialement disponible proposé et comprendre la mise en œuvre de politiques et de procédures sur la sécurité de l'information et de mesures de contrôle de la sécurité. Le fournisseur du logiciel-service commercialement disponible proposé doit également se conformer aux exigences de sécurité sélectionnées dans le Profil des mesures de sécurité pour les services de la TI du GC fondés sur l'informatique en nuage pour les renseignements classés « Protégés B, intégrité moyenne,disponibilité moyenne » (PBMM) pour la portée du logiciel-service commercialement disponible proposé fourni. La conformité sera validée et vérifiée conformément aux lignes directrices du CCCS pour les évaluations de sécurité informatique localisées. Tout fournisseur ayant participé au processus doit fournir une documentation confirmant qu'il a terminé le processus d'intégration avec (i) une copie du rapport d'évaluation complété le plus récent fourni par CCCS; et (ii) une copie du dernier rapport de synthèse fourni par CCCS. Cela accélérera le processus de qualification et ne demandera pas au fournisseur de démontrer la conformité Pour lancer le processus d'intégration, le fournisseur doit contacter le service clientèle de CCCS pour recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire relative au programme d'évaluation informatique du CSP.	Le fournisseur doit démontrer comment le fournisseur du logiciel-service commercialement disponible proposé se conforme aux exigences de la rubrique Exigences relatives à l'assurance des tiers. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications de l'industrie applicables énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants. Le fournisseur doit fournir chacune des certifications suivantes de l'industrie pour démontrer sa conformité : 1) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences 0) ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage 2) AICPA Service Organisation Control (SOC) 2 de type II pour les principes de confiance de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité. Chaque certification ou rapport d'évaluation doit : a) être valide à la date de clôture de la demande de soumissions; d) indiquer la raison sociale légale du fournisseur du logiciel-service commercialement disponible proposé et du fournisseur de services d'informatique en nuage; b) indiquer la date ou l'état de la certification actuelle; p) donner la liste des actifs, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification; c) la portée du rapport doit renvoyer aux lieux et aux services proposés par le logiciel sous forme de service commercialement disponible proposé. Si la méthode créée est utilisée pour exclure les organisations de sous-services comme la prise en charge de centres de données, le rapport d'évaluation de l'organisation de sous-services doit être joint; et d) être délivré par un tiers indépendant certifié en vertu de l'American Institute of Certified Public Accountants (AICPA) ou de CPA Canada (Comptables professionnels agréés du Canada) ou encore du régime de certification ISO, et être conforme à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité. Le fournisseur peut fournir des renseignements supplémentaires tirés de plans de sécurité du système, de documents de conception de système d'information, de documents d'architecture de système d'information ou de documents qui donnent une description détaillée du système, comme l'évaluation de ses services conformément à la version 3.01 de la Cloud Controls Matrix (CCM) de la Cloud Security Alliance (CSA) ou à une version subséquente, pour complémenter les allégations de certifications ci-dessus, afin de démontrer la conformité au Profil des mesures de sécurité pour les services de la TI du GCfondés sur l'informatique en nuage pour les renseignements classés Protégé B, intégrité moyenne et disponibilité moyenne (PBMM). Remarque : • Des certifications doivent être fournies pour toutes les parties des services proposés. • Les certifications doivent être accompagnées de rapports d'évaluation**.**

11. APPENDICE L – PROGRAMME D'ÉVALUATION DE LA SÉCURITÉ DES TI DES LOGICIELS-SERVICES : PROCESSUS D'INTEGRATION

Annexe L – Programme d'évaluation de la sécurité des TI des logiciels-services : processus d'intégration est supprimé dans son intégralité.

TOUS LES AUTRES TERMES ET CONDITIONS RESTENT LES MÊMES