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** 2020-02-28
Client Reference No. - N° de référence du client 20191593	**Amendment No. - N° modif.** 012
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 012 de la demande d'arrangement en matière d'approvisionnement (DAMA)

Méthode d'approvisionnement de logiciels-services (INFONUAGIQUE GC)

Numéro de référence de la demande de soumissions sur Achatsetventes : EN578-191593/F

LA MODIFICATION N^{O} 012 VISE À :	
1.0	Corriger une erreur administrative en R.51 de la modification 011 comme il est précisé à la section 1.0 ci-dessous;
2.0	Répondre aux questions reçues au sujet de la DAMA, comme il est précisé à la section 2.0 ci-dessous;
3.0	Modifier la DAMA, comme il est précisé à la section 3.0 ci-dessous;
4.0	Modifier l'annexe F, Clauses du contrat subséquent, comme il est précisé à la section 4.0 ci-dessous;
5.0	Remplacer les documents d'invitation à soumissionner dans leurs intégralités pour inclure les révisions effectuées aux modifications 001 à 012, comme il est précisé à la section 5.0 ci-dessous; et
6.0	Ajoutez les formulaires 1 à 6 et l'annexe C en version modifiables comme indiqué dans la section 6.0 ci-dessous.
REMARQUE : Les questions d'éclaircissement sont numérotées en fonction de leur ordre d'arrivée à Services publics et Approvisionnement Canada (SPAC). Les répondants doivent prendre note que les questions et les réponses concernant la présente invitation ne seront pas nécessairement affichées dans l'ordre sur le site Achatsetventes.gc.ca.	

1.0 Corriger une erreur administrative en R.51 de la modification 011

ENDROIT	SUPPRIMER	INSÉRER
A.51 of Amendment 011	Enlever le point après le mot contact : contact.@cyber.gc.ca	contact@cyber.gc.ca

2.0 Répondre aux questions sur la DAMA :

Remarque : Le libellé des questions peut avoir été modifié ou abrégé.

QUESTIONS	RÉPONSES
Q.53 Pour le critère O5 (Assurance d'une tierce partie), niveau 1 de l'annexe A – Exigences de qualification, SPC acceptera-t-il l'autoévaluation CAIQ de la Cloud Security Alliance comme solution de rechange à l'autoévaluation CCM de la Cloud Security Alliance? Les deux questionnaires autoadministrés sont fondés sur les mêmes principes fondamentaux et élaborés par la même instance. Toutefois, de nombreux fournisseurs de logiciels-services répondent seulement au questionnaire CAIQ par souci de prudence et de rentabilité. Le questionnaire CIAQ évalue les contrôles de sécurité de base définis dans le CCM. Des couches supplémentaires de contrôles de sécurité sont examinées en fonction des besoins, lorsque des besoins particuliers se présentent.	**R.53** 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.
Q.54 Pour le critère O7 (Gestion des risques de la chaîne d'approvisionnement), niveau 1 de l'annexe A, Exigences de qualification, SPC acceptera-t-il la certification FedRAMP américaine (Federal Risk and Authorization Management Program, https://www.fedramp.gov/cloud-service-providers/)?	**R.54** 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.

QUESTIONS	RÉPONSES
Étant donné que de nombreux fournisseurs de logiciels-services sont situés aux États-Unis, ils choisissent de se conformer aux normes du FedRAMP, qui a établi une approche standard de la gestion des risques aux États-Unis pour les fournisseurs de services infonuagiques. Le programme FedRAMP est soutenu par l'Institut NIST, est compatible avec le contrôle ITSG-33 et est cité dans l'approche canadienne de gestion des risques à la sécurité de l'informatique en nuage (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/services-informatique-nuage/approche-procedures-gestion-risques-securite-informatique-nuage.html)	
Q.55 En ce qui concerne les critères O2 (Protection des données) et O3 (Installations des centres de données), niveau 1 de l'annexe A, Exigences de qualification, un certain nombre de fournisseurs de solutions de logiciels-services n'administrent pas leurs propres centres de données. Leurs solutions sont exclusivement hébergées par un tiers. Dans ce cas-ci, Amazon Web Services (AWS). Est-ce que SPC peut approuver de façon générale les hôtes de centres de données (nommément AWS et MS Azure), à condition que ces derniers aient satisfait aux exigences techniques de SPC?	**R.55** Non. Le gouvernement du Canada n'a pas évalué tous les services infonuagiques des grands fournisseurs. Il n'est donc pas en mesure d'accorder une approbation générale. Le GC recommande que les fournisseurs de solutions SaaS contactent leur CSP et demandent la lettre d'attestation démontrant qu'ils sont un partenaire enregistré d'un CSP et des preuves qu'il a déjà été évalué par le GC.
Q.56 En ce qui concerne le critère O6 (Gestion de la chaîne d'approvisionnement), niveau 1 de l'annexe A, Exigences de qualification, est-ce que SPC peut fournir des instructions sur la manière de savoir si une solution d'infrastructure-service ou de plateforme-service a été évaluée par le programme CCC?	**R.56** Le gouvernement du Canada recommande que le fournisseur de logiciels-services demande ces renseignements auprès de son fournisseur de services infonuagiques.

3.0 Modifier la demande d'AMA comme suit :

ENDROIT	SUPPRIMER	INSÉRER
Section 1.4 – Security Requirements	La présente DAMA comporte des exigences de sécurité, en particulier telles que décrites dans l'Annexe A - Exigences de qualification, l'Annexe B - Obligations en matière de sécurité et protection de la vie privée, et l'Annexe F - Clauses du contrat subséquent, y compris ses appendices. Les travaux et les services de services-logiciels à acquérir dans le cadre de la présente DAMA peuvent également être soumis à des exigences de sécurité supplémentaires, y compris, mais sans s'y limiter, l'invocation de l'exemption relative à la sécurité nationale liée à la DAMA, ainsi que des exigences de sécurité supplémentaires liées en fonction des besoins individuels du client, qui seront décrits dans la demande de soumissions et/ou le contrat du client.	La présente DAMA comporte des exigences de sécurité, en particulier telles que décrites dans l'Annexe A - Exigences de qualification, l'Annexe B - Obligations en matière de sécurité et protection de la vie privée, Annexe G – Exigences relatives à la sécurité pour les entrepreneurs canadiens, Annexe H – Exigences relatives à la sécurité pour les entrepreneurs étranger, Annexe I – LVERS relative aux logiciels-services, Annexe J – Guide de classification de la sécurité, Annexe L – Programme d'évaluation de la sécurité des TI en logiciels-services : processus d'intégration, Formulaire 6 – Formulaire de soumission de SCI et l'Annexe F - Clauses du contrat subséquent, y compris ses appendices. Les travaux et les services de services-logiciels à acquérir dans le cadre de la présente DAMA peuvent également être soumis à des exigences de sécurité supplémentaires, y compris, mais sans s'y limiter, l'invocation de l'exemption relative à la sécurité nationale liée à la DAMA, ainsi que des exigences de sécurité supplémentaires liées en fonction des besoins individuels du client, qui seront décrits dans la demande de soumissions et/ou le contrat du client.
Section 6.5.3 – L'autorité sur la sécurité de la chaine d'approvisionnement	**6.5.3 L'autorité sur la sécurité de la chaine d'approvisionnement** L'autorité sur la sécurité de la chaine d'approvisionnement pour le contrat est: Nom: _____ Titre: _____ SSC : _____ Adresse: _____ Téléphone: _____ Courriel: _____ L'autorité sur la sécurité de la chaine d'approvisionnement est le représentant de SSC et est responsable pour ce qui concerne au processus d'intégrité sur la chaine d'approvisionnement dans le cadre du contrat. Ni l'autorité contractante ni l'autorité technique ne sont habilités à conseiller ou à autoriser des informations relatives au processus d'intégrité de la chaîne d'approvisionnement. Toutes les autres questions liées à la sécurité relèvent de la responsabilité de l'autorité sur la sécurité de la chaine d'approvisionnement.	**6.5.3 L'autorité sur la sécurité de la chaine d'approvisionnement** L'autorité sur la sécurité de la chaine d'approvisionnement pour le contrat est: Nom: _____ Titre: _____ CCC: _____ Adresse: _____ Téléphone: _____ Courriel: _____ L'autorité sur la sécurité de la chaine d'approvisionnement est le représentant de CCC et est responsable pour ce qui concerne au processus d'intégrité sur la chaine d'approvisionnement dans le cadre du contrat. Ni l'autorité contractante ni l'autorité technique ne sont habilités à conseiller ou à autoriser des informations relatives au processus d'intégrité de la chaîne d'approvisionnement. Toutes les autres questions liées à la sécurité relèvent de la responsabilité de l'autorité sur la sécurité de la chaine d'approvisionnement.
Annexe K, Accord de non-divulgation de SPAC relatif à l'intégrité de la chaîne		Les sous-sections suivantes s'appliquent aux situations où **l'entrepreneur/sous-traitant** confirme qu'il a accès aux données du Canada, en prend soin et contrôle.

ENDROIT	SUPPRIMER	INSÉRER
d'approvisionnement		

4.0 Modifier l'annexe F, Clauses du contrat subséquent, comme suit :

ENDROIT	SUPPRIMER	INSÉRER
Section 2 Durée, résiliation et renouvellement automatique		**2.1 Durée de l'abonnement** (f) **Changement en matière de consommation.** L'entrepreneur accorde au Canada l'option irrévocable d'augmenter ou de réduire sa consommation de produits ou de services de logiciel-service décrits à l'annexe A. Si la consommation d'un produit ou d'un service de logiciel-service par le Canada est réduite, l'entrepreneur convient qu'aucune pénalité ou augmentation du prix unitaire ne s'applique en conséquence.
Section 2 Durée, résiliation et renouvellement automatique		**2.5 Changement en matière de consommation.** L'entrepreneur accorde au Canada l'option irrévocable d'augmenter ou de réduire sa consommation de produits ou de services de logiciel-service décrits à l'annexe A. Si la consommation d'un produit ou d'un service de logiciel-service par le Canada est réduite, l'entrepreneur convient qu'aucune pénalité ou augmentation du prix unitaire ne s'applique en conséquence.
Section 4.1 Services de la solution		(k) **Récupération des données:** L'entrepreneur accepte de rendre les données du Canada disponibles pendant au moins 90 jours après la fin du contrat afin de laisser au client suffisamment de temps pour migrer leurs données vers un nouvel environnement, sans frais supplémentaires pour le Canada.
Section 9. Base de paiement		**9.4 Attestation du prix.** L'entrepreneur atteste que le prix proposé n'est pas supérieur au plus bas prix demandé à tout autre client, y compris à son meilleur client, pour une qualité et une quantité semblable de biens, de services ou les deux.

ENDROIT	SUPPRIMER	INSÉRER
Section 12. Limitation de responsabilité	Remarque au fournisseur : SPAC et SPC s'efforce de développer un regroupement de produits de logiciels-services pour fournir une clause de limitation de responsabilité à jour à utiliser à la fois par SPAC et SPC pour l'approvisionnement infonuagique. Cette nouvelle clause de limitation de responsabilité remplacera le libellé actuel de la limitation de responsabilité dès qu'il sera disponible. a) Sauf indiqué expressément dans le paragraphe b), l'entrepreneur est responsable de tous les dommages qu'il cause durant l'exécution ou par manque d'exécution du contrat en relation avec : 1. tout acte ou omission dans le cadre du contrat qui affecte les biens réels ou tangibles que ce soient possédés, détenus ou occupés par le Canada. 2. le manquement à l'obligation de confidentialité par l'entrepreneur en vertu du contrat, mais cette limitation ne s'applique pas à la divulgation de secret commerciaux du Canada ou de tiers en relation avec la technologie informatique. 3. toute charge ou tout privilège sur toute portion des travaux dans le cadre du contrat, qui n'incluent pas les réclamations ou charges relatives aux droits de propriété intellectuelle; et 4. le manquement aux obligations de garantie par l'entrepreneur. Cependant, l'entrepreneur n'est pas responsable envers le Canada des dommages indirects, particuliers ou consécutifs causés par l'aliéna 1 à 4 ci-dessus. b) En ce qui concerne les dommages directs liés à la violation par l'entrepreneur de ses obligations de garantie, la responsabilité maximale de l'entrepreneur envers le Canada est le coût estimatif total du contrat (c'est-à-dire le montant en dollars indiqué sur la première page du contrat dans le bloc intitulé « Coût estimatif total »). Tous les dommages directs non énumérés ci-dessus qui ne sont pas liés à une violation de garantie sont assujettis à un maximum de 0,25 fois le coût total estimatif ou 1 M $, selon le montant le plus élevé. c) Si les dossiers ou les données du Canada sont endommagés à la suite d'une négligence ou d'un acte délibéré de l'entrepreneur, la seule responsabilité de l'entrepreneur consiste à rétablir à ses frais	**12 Limitation des responsabilités** 12.1 **Responsabilité de première partie** (a) **Exécution du contrat :** L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par l'exécution ou l'inexécution du contrat par l'entrepreneur. (b) **Fuite de données:** L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par une infraction à la sécurité ou un manquement à l'obligation de confidentialité entraînant la consultation ou la divulgation non autorisées de dossiers, de données ou de renseignements appartenant au Canada ou à un tiers. (c) **Limitation par incident :** Sous réserve de la clause suivante, quel que soit le fondement ou la nature de la réclamation, la responsabilité totale par incident de l'entrepreneur n'excédera pas la valeur cumulative des factures liées au contrat au cours des douze (12) mois précédant l'incident. (d) **Aucune limitation:** La limitation de responsabilité susmentionnée de l'entrepreneur ne s'applique pas : (i) à toute inconduite volontaire ou à tout acte répréhensible délibéré; (ii) à tout manquement aux obligations relatives à la garantie. Responsabilité de tierce partie : Chaque partie convient qu'elle est pleinement responsable des dommages qu'elle cause à un tiers dans le cadre du contrat, que la réclamation soit déposée par le tiers auprès du Canada ou de l'entrepreneur, ou des deux. Le montant de la responsabilité sera celui précisé dans l'accord conclu entre les parties ou déterminé par la cour. Les parties conviennent de se rembourser mutuellement tout paiement versé à un tiers en lien avec les dommages causés par l'autre partie et de rembourser rapidement leur part de responsabilité.

ENDROIT	SUPPRIMER	INSÉRER
	les dossiers et les données du Canada en utilisant la copie de sauvegarde la plus récente conservée par le Canada. Il incombe au Canada de sauvegarder adéquatement ses dossiers et ses données. d) Les limitations ci-dessus ne s'appliquent pas aux dommages basés sur la perte de vie ou la blessure corporelle, ou les réclamations basées sur la violation des droits de propriété intellectuelle.	
Appendice C – Obligations en matière de sécurité		**13. Changement de contrôle** (a) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle affectant l'entrepreneur (soit à l'entrepreneur lui-même, soit à l'un de ses parents, jusqu'au propriétaire final) peut être préjudiciable à la sécurité nationale, le Canada peut résilier le contrat sur une «Sans faute» en fournissant un avis à l'entrepreneur dans les 90 jours civils suivant la réception de l'avis de l'entrepreneur concernant le changement de contrôle. Le Canada ne sera pas tenu de fournir ses raisons de résilier le CONTRAT en relation avec le changement de contrôle, si le Canada détermine à sa discrétion que la divulgation de ces raisons pourrait elle-même porter atteinte à la sécurité nationale. (b) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle affectant un sous-traitant (que ce soit le sous-traitant lui-même ou l'un de ses parents, jusqu'au propriétaire final) peut être préjudiciable à la sécurité nationale, le Canada avisera l'entrepreneur par écrit. de sa détermination. Le Canada ne sera pas tenu de motiver sa décision si le Canada détermine à sa discrétion que la divulgation de ces raisons pourrait elle-même porter atteinte à la sécurité nationale. L'entrepreneur doit, dans les 30 jours civils suivant la réception de la décision du Canada, prendre des dispositions pour qu'un autre sous-traitant, acceptable pour le Canada, fournisse la partie des services cloud fournie par le sous-traitant existant (ou l'entrepreneur doit livrer cette partie des services cloud lui-même) . Si l'entrepreneur ne le fait pas dans ce délai, le Canada sera en droit de résilier le contrat sans faute en fournissant un avis à l'entrepreneur dans les 120 jours civils suivant la réception de l'avis original de l'entrepreneur concernant le changement de contrôle. (c) Dans le présent article, la résiliation sans faute signifie qu'aucune des parties ne

ENDROIT	SUPPRIMER	INSÉRER
		sera responsable envers l'autre à l'égard du changement de contrôle et de la résiliation qui en résulte, et le Canada ne sera responsable que du paiement des services reçus. jusqu'à la date effective de la résiliation. (d) Malgré ce qui précède, le droit du Canada de résilier sans faute ne s'appliquera pas aux circonstances dans lesquelles il y a une réorganisation interne qui n'affecte pas la propriété de la société mère ultime ou de la société mère de l'entrepreneur ou du sous-traitant , selon le cas; autrement dit, le Canada n'a pas le droit de résilier le CONTRAT en vertu du présent article lorsque l'entrepreneur ou le sous-traitant continue, en tout temps, d'être contrôlé, directement ou indirectement, par le même propriétaire final.

5.0 La demande de soumissions EN578-191593/ F est par les présentes supprimée dans son intégralité et remplacée par une nouvelle version qui incorpore l'amendement 001 à l'amendement 012.

Veuillez trouver ci-joints les documents suivants contenant les modifications apportées aux documents de demande de soumissions de la DAMA.

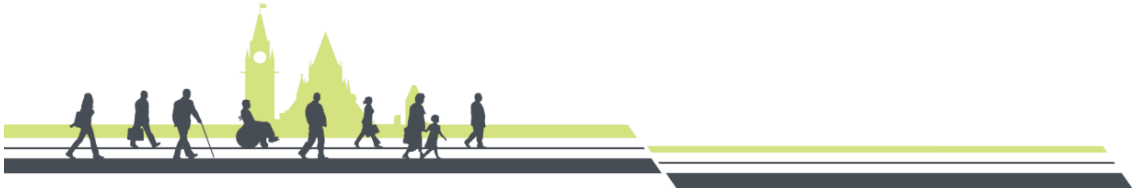
1. DAMA – Méthode d'approvisionnement de logiciels-services (Infonuagique GC) – (FR) – Modification 012; et
2. Annexe F – Logiciels-services – Clauses du contrat subséquent – (FR) – Modification 012.

6.0 Les formulaires 1 à 6 et l'annexe C sont par la présente ajoutés en version modifiables sous la section Pièces jointes de la page Avis d'appel d'offres: DAMA - Méthode d'approvisionnement de logiciels-services (Infonuagiques GC) (EN578-191593/F).

Voir la section des pièces jointes pour télécharger les fichiers en version modifiables:

- Annexe C - Prix plafonds pour les Solutions de logiciels services et les services professionnels;
- Formulaire 1 - Formulaire de présentation des soumissions;
- Formulaire 2 - Formulaire d'attestation de l'éditeur de logiciels-services;
- Formulaire 3 - Formulaire d'autorisation de l'éditeur de logiciels-services;
- Formulaire 4 - Attestation aux fins du Programme de marchés réservés aux entreprises autochtones;
- Formulaire 5 - Liste de vérification de l'exhaustivité de la soumission; et
- Formulaire 6 - Formulaire de soumission de SCI.

TOUTES LES AUTRES MODALITÉS DE LA DEMANDE POUR UN ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT DEMEURENT INCHANGÉES



SERVICES PUBLICS ET APPROVISIONNEMENT CANADA (SPAC)

DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA) CONCERNANT LES SOLUTIONS DE LOGICIELS-SERVICES (INFONUAGIQUES GC)

TABLE DES MATIÈRES

PARTIE 1 – GENERAL INFORMATION GÉNÉRALE

1.1 Préambule

Services publics et approvisionnement Canada (SPAC), au nom du gouvernement du Canada (GC), publie la présente demande d'arrangement en matière d'approvisionnement (DAMA) afin d'établir une nouvelle méthode d'approvisionnement afin de satisfaire aux diverses exigences du logiciel-service. Cette nouvelle méthode d'approvisionnement s'inscrit dans le cadre du Véhicule d'approvisionnement des services infonuagiques du gouvernement du Canada (GC), qui devrait comprendre diverses méthodes d'approvisionnement répondant à des besoins infonuagiques classifiés et non classifiés.

Les objectifs de cette DAMA logiciels-services sont les suivants:

- simplifier le processus d'approvisionnement pour acquérir des solutions de logiciels-services et soutenir les initiatives de modernisation des achats et de simplification des contrats du GC;
- augmenter la concurrence et l'accès aux dernières solutions de logiciels-services sur le marché pour le GC; et
- accroître la transparence, l'ouverture et l'équité des processus d'approvisionnement du secteur public.

Comme le souligne le *Plan stratégique des opérations numériques du GC: 2018-2022* publié par le Secrétariat du Conseil du Trésor du Canada, des outils tels que les DAMA pour les logiciels-services aideront à positionner le GC et les partenaires du secteur public pour qu'ils exploitent les dernières technologies numériques afin d'obtenir de meilleurs résultats pour les Canadiens.

1.1.1 Contexte

Le cadre de véhicule d'approvisionnement en services infonuagique du GC représente une approche novatrice d'achat infonuagique en exploitant diverses méthodes d'approvisionnement pour répondre aux besoins infonuagique du GC et des entités du secteur public, qui peuvent inclure, sans toutefois s'y limiter, les gouvernements provinciaux, territoriaux et municipaux.

Le 7 septembre 2018, Services partagés Canada (SPC) a publié une Invitation à se qualifier (IQ) en tant que premier volet du processus d'achat du véhicule d'approvisionnement en services infonuagique du GC (https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-18-00841719) En parallèle, SPAC a lancé une demande de renseignements le 29 octobre 2018 afin de recueillir les commentaires de l'industrie sur l'approche proposée et les exigences en matière de fourniture de services et de solutions SaaS. SPAC a reçu 47 réponses à la demande de renseignements et organisé des séances individuelles avec les fournisseurs intéressés afin d'affiner l'approche et les exigences de la présente DAMA et de mieux s'aligner sur les meilleures pratiques de l'industrie en matière d'approvisionnement infonuagique.

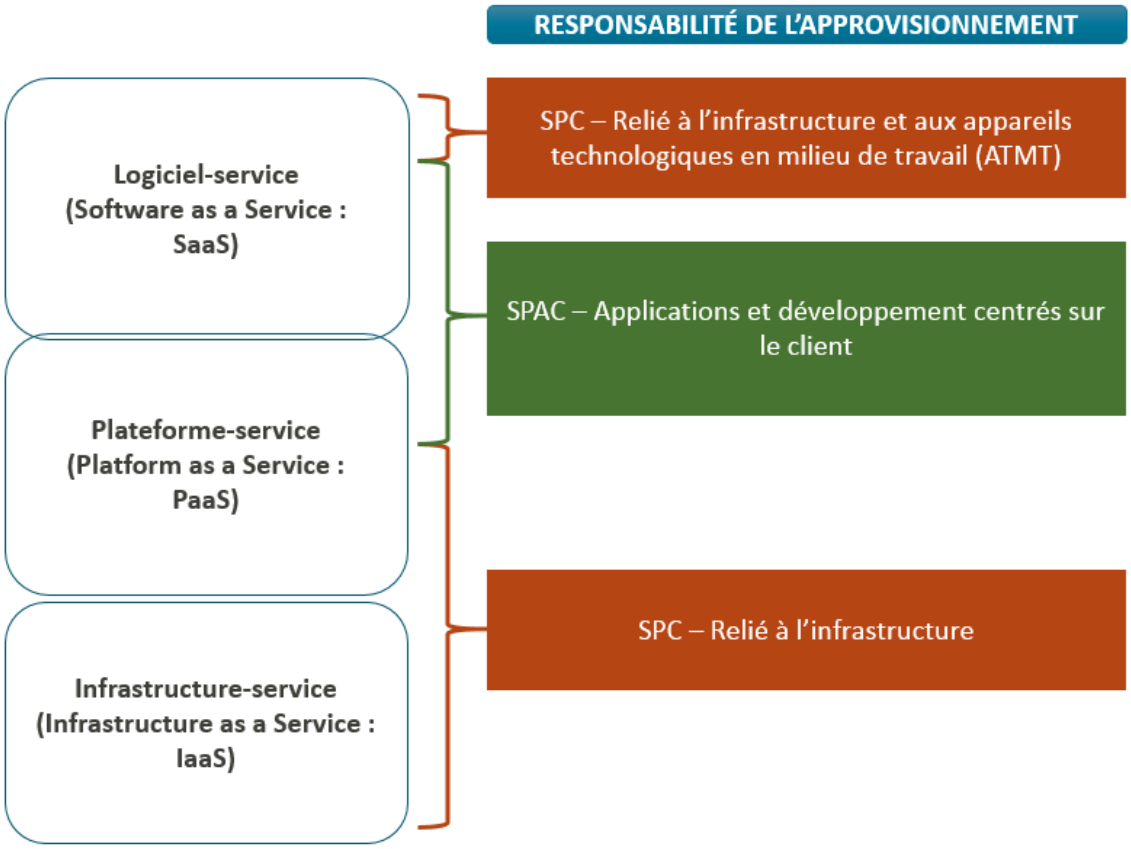
1.1.2 Organisation du GC pour assurer efficacement les achats des logiciels-services

Au sein du GC, SPAC et SPC soutiennent conjointement les organisations fédérales pour leur approvisionnement en biens et services informatiques. En ce qui concerne l'acquisition de services infonuagiques, les responsabilités de chaque organisation en matière d'approvisionnement s'étendent aux divers éléments de la pile infonuagique, de l'infrastructure aux couches d'applications logicielles. La répartition des responsabilités d'acquisition reflète les mandats d'approvisionnement de chaque organisation pour soutenir les clients du GC.

Conformément au mandat de chaque organisation, le rôle d'approvisionnement de SPC dans les offres de services infonuagiques reflète ses responsabilités en fait de gestion de l'infrastructure, des réseaux, d'appareils technologiques usuels en milieu de travail et de la cyber sécurité.

Le rôle de SPAC en matière d'approvisionnement se situe principalement dans le domaine des applications logicielles et du développement, où il appuie les clients dans leurs fonctions de prestation de services et d'arrière-guichet.

Le diagramme ci-dessous ne représente que le partage des responsabilités et n'est pas spécifique à un besoin :



Cette DAMA permettra aux fournisseurs d'émettre des arrangements en matière d'approvisionnement avec des catalogues de logiciels-services et facilitera les processus simplifiés de sollicitation et de passation de marchés pour les besoins de chaque client.

SPAC et SPC travaillent en étroite collaboration pour assurer l'harmonisation des meilleures pratiques en matière d'approvisionnement infonuagique, y compris la mise en place d'un groupe de produits infonuagique afin de répondre à la limitation de responsabilité et aux exigences de sécurité communes. Ces éléments constituent le fondement des activités d'approvisionnement infonuagique au sein du gouvernement.

1.1.3 Structure de la DAMA

Cette demande d'arrangements en matière d'approvisionnement (DAMA) contient sept parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 **Renseignements généraux** : renferme une description générale du besoin;

Partie 2 **Instructions à l'intention des fournisseurs** : renferme les instructions relatives aux clauses et conditions de la DAMA;

Partie 3 **Instructions pour la préparation des arrangements** : donne aux fournisseurs les instructions pour préparer l'arrangement afin de répondre aux critères d'évaluation spécifiés;

Partie 4 **Procédures d'évaluation et Méthode de sélection** : décrit la façon selon laquelle se déroulera l'évaluation, les critères d'évaluation auxquels on doit répondre ainsi que la méthode de sélection;

Partie 5 **Attestations et renseignements supplémentaires** : comprend les attestations et les renseignements supplémentaires à fournir;

Partie 6 **Arrangement en matière d'approvisionnement**: contient l'arrangement en matière d'approvisionnement (AMA) et les clauses et conditions applicables; et

Partie 7 **Sélection des entrepreneurs et Clauses du contrat subséquent**: contient les instructions du processus de demande de soumissions dans le cadre d'un AMA ainsi que des renseignements généraux pour les conditions qui feront partie des contrats émis suite à un AMA.

Les annexes comprennent les Exigences de qualification, les Obligations en matière de sécurité, le Catalogue de logiciels-services et Prix plafond, les Accords sur les niveaux de service (ANS), le Modèle de demande de soumission pour logiciels-services, les Clauses du contrat subséquent, ainsi que le processus d'intégration du Programme d'évaluation de la sécurité des TI des logiciels-services.

Remarque: Les mots en majuscules et les termes techniques utilisés dans la présente DAMA sont définis dans les Clauses du contrat subséquent - **Appendice B - DÉFINITIONS ET INTERPRÉTATION**.

1.2 Sommaire

(a) Services publics et approvisionnement Canada (SPAC), au nom du Canada, met en place le présent outil d'approvisionnement pour la fourniture de diverses solutions de logiciels-services disponibles sur le marché, incluant des services connexes de maintenance et de soutien, la formation et les services professionnels, selon les besoins du Canada, pour appuyer ses divers programmes, besoins opérationnels et projets. La DAMA sert également à établir des arrangements en matière d'approvisionnement avec des entreprises autochtones, tels que définis dans la Stratégie d'approvisionnement pour les entreprises autochtones (SAEA), afin de permettre aux clients de mettre de côté leurs exigences.

(b) Toute demande de livraison au lieu situé dans une région visée par une revendication territoriale sera traitée comme une demande distincte qui ne fera pas partie des arrangements en matière d'approvisionnement (AMA).

(c) Tout AMA subséquent peut être utilisé pour acquérir des solutions de logiciels-services ainsi que la formation et des services professionnels connexes pour tout ministère, tout organisme, toute société d'État, ou toute autre entité du gouvernement du Canada, y compris ceux qui sont mentionnés dans la *Loi sur la gestion des finances publiques*, telle qu'elle est modifiée de temps à autre, ou toute autre

partie au nom de laquelle SPAC a été autorisé à agir de temps à autre en vertu de l'article 16 de la *Loi sur le ministère des Travaux publics et des Services gouvernementaux* (chacun étant un « client »).

(d) Un avis et la DAMA seront affichés de façon continue par le biais du Service électronique d'appels d'offres du gouvernement (SEAOG) pour permettre aux fournisseurs de se qualifier pour un ou des AMA en tout temps.

(e) À mesure que les solutions basées sur le nuage augmentent sur le marché, le Canada reconnaît la nécessité d'agir avec agilité pour faciliter l'accès aux solutions de logiciels-services tout en tenant compte des complexités associées à l'adoption de nouvelles méthodes de fourniture de technologies de l'information (TI). La qualification pour les arrangements en matière d'approvisionnement sera ouverte aux fournisseurs de solutions de logiciels-services fondées sur l'infrastructure-service (IaaS) et la plateforme-service (PaaS) conformes au profil de contrôle de sécurité pour les services infonuagiques du GC (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) et les exigences connexes relatives à la sécurité des TI définies dans la présente DAMA.

(f) Le Canada n'attribuera pas un AMA à un fournisseur ni ne reportera l'attribution d'un ou de plusieurs marchés à d'autres fournisseurs si un fournisseur n'a pas soumis toute la documentation avec sa réponse ou s'il a soumis des documents qui s'écartent des modalités prévues par la DAMA.

(g) Les contrats résultant de cette méthode d'approvisionnement peuvent être assujettis aux dispositions de l'Accord sur les marchés publics de l'organisation mondiale du commerce (AMP-OMC), de l'Accord de libre-échange nord-américain (ALENA), de l'Accord économique et commercial global entre le Canada et l'Union européenne (AECG) et de l'Accord de libre-échange canadien (ALEC).

(h) Cette DAMA permet aux fournisseurs d'utiliser le service Connexion postel offert par la Société canadienne des postes pour la transmission électronique de leurs arrangements. Les fournisseurs doivent consulter la partie 2 de la DAMA, Instructions à l'intention des fournisseurs, pour obtenir de plus amples renseignements sur le recours à cette méthode.

(i) L'ordre d'évaluation des arrangements sera établi à la seule discrétion du Canada.

(j) La présente DAMA n'est pas une demande de soumissions ou de propositions. Aucun contrat ne sera attribué automatiquement à la suite de la qualification en vertu de la présente DAMA.

1.3 Aperçu du processus d'évaluation de soumissions

Afin de répondre au mieux aux besoins du gouvernement du Canada et de gérer le volume de soumissions reçues en réponse à la présente DAMA, le processus d'évaluation des soumissions et la catégorisation des fournisseurs se déroulera comme suit:

(a) **Volet 1**: inclura les soumissions des fournisseurs proposant des solutions services-logiciels et des Services conformes aux exigences du Canada en matière de stockage et de traitement des informations Protégées B, comme indiqué à l'annexe A, Exigences de qualification, Palier 2.

(b) **Volet 2**: inclura les soumissions des fournisseurs proposant des solutions de services-logiciels et des Services conformes aux exigences du Canada en matière de stockage et de traitement des informations jusqu'au niveau Protégé A, comme indiqué à l'annexe A, Exigences de qualification, Palier 1.

(c) **Volet 3**: inclura les soumissions des distributeurs à valeur ajoutée proposant des logiciels-services et des services. Les distributeurs à valeur ajoutée qui souhaitent présenter une soumission pour se qualifier en tant fournisseur doivent se conformer à l'annexe A, Exigences de qualification, palier 1 (données jusqu'au niveau Protégé A), et sont tenus de soumettre les attestations de l'éditeur de

logiciels-services, conformément au Formulaire d'autorisation de l'éditeur de logiciels-services (Formulaire 3), pour attester que le fournisseur a été autorisé à fournir la ou les solutions de l'éditeur de logiciels-services. **Les distributeurs à valeur ajoutée ne seront pas autorisés à se qualifier pour le niveau Protégé B.**

Le Canada commencera à évaluer les soumissions du volet 1, 2 et 3 en date du 17 juin 2019.

1.4 Exigences relatives à la sécurité

La présente DAMA comporte des exigences de sécurité, en particulier telles que décrites dans l'Annexe A - Exigences de qualification, l'Annexe B - Obligations en matière de sécurité et protection de la vie privée, Annexe G – Exigences relatives à la sécurité pour les entrepreneurs canadiens, Annexe H – Exigences relatives à la sécurité pour les entrepreneurs étranger, Annexe I – LVERS relative aux logiciels-services, Annexe J – Guide de classification de la sécurité, Annexe L – Programme d'évaluation de la sécurité des TI en logiciels-services : processus d'intégration, Formulaire 6 – Formulaire de soumission de SCI et l'Annexe F - Clauses du contrat subséquent, y compris ses appendices. Les travaux et les services de services-logiciels à acquérir dans le cadre de la présente DAMA peuvent également être soumis à des exigences de sécurité supplémentaires, y compris, mais sans s'y limiter, l'invocation de l'exemption relative à la sécurité nationale liée à la DAMA, ainsi que des exigences de sécurité supplémentaires liées en fonction des besoins individuels du client, qui seront décrits dans la demande de soumissions et/ou le contrat du client.

1.5 Compte rendu

Les fournisseurs peuvent demander un compte rendu des résultats du processus de demande d'arrangements en matière d'approvisionnement. Les fournisseurs devraient en faire la demande sur l'AMA dans les 15 jours ouvrables, suivant la réception des résultats du processus de demande d'arrangements en matière d'approvisionnement. Le compte rendu peut être fourni par écrit, par téléphone ou en personne.

1.6 Termes-clés

Les définitions des termes clés pour l'ensemble de la présente DAMA, y compris les annexes formulaires ci-joints, sont détaillées à l'appendice B de l'annexe F - Clauses du contrat subséquent.

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES FOURNISSEURS

2.1 Instructions, clauses et conditions uniformisées

Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions en matière d'approvisionnement (DAMA) par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Services publics et approvisionnement Canada.

Les fournisseurs qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la DAMA et acceptent les clauses et les conditions sur l'arrangement en matière d'approvisionnement et du ou des contrats subséquents.

Le document 2008 (2018-05-22) Instructions uniformisées - demande de soumissions en matière d'approvisionnement - biens ou services, sont incorporées par renvoi à la DAMA et en font partie intégrante.

Les instructions uniformisées 2008 sont modifiées comme suit :

- l'article 08, Présentation des soumissions, est modifié comme suit :
    - le sous-article 2. est entièrement supprimé et remplacé par le paragraphe suivant :

2. Connexion postel

(a) Sauf indication contraire dans la DAMA, les soumissions peuvent être transmis à l'aide du service Connexion postel fourni par la Société canadienne des postes.

La seule adresse de courriel acceptable avec Connexion postel pour transmettre une réponse à une DAMA établie par l'administration centrale de SPAC est :

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

(b) Pour transmettre une soumission à l'aide du service Connexion postel, le fournisseur doit utiliser l'une des deux options suivantes :

(i) envoyer directement sa soumission uniquement à l'Unité de réception des soumissions de SPAC précisée à l'aide de sa propre licence d'utilisateur du service Connexion postel en vigueur entre son entreprise et la Société canadienne des postes; ou

(ii) envoyer dès que possible et, dans tous les cas, au moins six jours ouvrables avant la date et l'heure de clôture de la DAMA (afin de garantir une réponse), un courriel qui contient le numéro de la DAMA à l'Unité de réception des soumissions de SPAC précisée pour demander d'ouvrir une conversation Connexion postel. Les demandes d'ouverture de conversation Connexion postel reçues après cette heure pourraient rester sans réponse.

(c) Si le fournisseur envoie un courriel demandant le service Connexion postel à l'Unité de réception des soumissions précisée dans la DAMA, un agent de l'Unité de réception des soumissions entamera alors la conversation Connexion postel. La conversation du service Connexion postel créera une notification par courriel de la Société canadienne des postes invitant le fournisseur à accéder au message dans la conversation, et le fournisseur devra prendre les mesures nécessaires pour répondre. Le fournisseur pourra transmettre sa

soumission en réponse à la notification à n'importe quel moment avant la date et l'heure de clôture de la DAMA.

(d) Si le fournisseur utilise sa licence d'entreprise en vigueur pour envoyer sa soumission, il doit maintenir la conversation Connexion postel ouverte jusqu'à au moins 30 jours ouvrables après la date et l'heure de clôture de la DAMA.

(e) Le numéro de la DAMA devrait être indiqué dans le champ réservé à la description dans toutes les transmissions électroniques.

(f) Il est important de savoir qu'il faut avoir une adresse postale canadienne pour utiliser le service Connexion postel. Si le fournisseur n'en a pas, il peut utiliser l'adresse de l'Unité de réception des soumissions indiquée dans la DAMA pour s'inscrire au service Connexion postel.

(g) Dans le cas des transmissions par le service Connexion postel, le Canada ne pourra pas être tenu responsable de tout retard ou panne touchant la transmission ou la réception des soumissions. Entre autres, le Canada n'assumera aucune responsabilité pour ce qui suit :

(i) réception d'un arrangement brouillé, corrompue ou incomplet;
(ii) disponibilité ou état du service Connexion postel;
(iii) incompatibilité entre le matériel utilisé pour l'envoi et celui utilisé pour la réception;
(iv) retard dans la transmission ou la réception de la soumission;
(v) défaut de la part du fournisseur de bien indiquer la soumission;
(vi) illisibilité de la soumission;
(vii) sécurité des données incluses dans la soumission;
(viii) incapacité de créer une conversation électronique par le service Connexion postel.

(h) L'Unité de réception des soumissions enverra un accusé de réception des documents de la soumission au moyen de la conversation Connexion postel, peu importe si la conversation a été initiée par le fournisseur à l'aide de sa propre licence ou par l'Unité de réception des soumissions. Cet accusé de réception ne confirmera que la réception des documents de la soumission et ne confirmera pas si les pièces jointes peuvent être ouvertes ou si le contenu est lisible.

(i) Les fournisseurs doivent veiller à utiliser la bonne adresse courriel pour l'Unité de réception des soumissions lorsqu'ils amorcent une conversation dans Connexion postel ou communiquent avec l'Unité de réception des soumissions et ne doivent pas se fier à l'exactitude d'un copié-collé de l'adresse courriel dans le système Connexion postel.

(j) Un soumission transmis par le service Connexion postel constitue la soumission officielle du fournisseur et doit être conforme à l'article 05.

Le paragraphe 5.4 du document 2008, Instructions uniformisées - demande d'arrangements en matière d'approvisionnement - biens ou services, est modifié comme suit :

Supprimer : 60 jours
Insérer : 180 jours

2.2 Présentation des soumissions

(a) Si le fournisseur choisit d'envoyer sa soumission par voie électronique en utilisant le service Connexion postel, le Canada exige de sa part qu'il respecte l'article 08 des Instructions uniformisées 2008 incorporées par référence. Le système Connexion postel a une limite de 1 Go par message individuel affiché et de 20 Go par conversation. Les formats des documents approuvés peuvent être une combinaison de ce qui suit :

A. documents en format PDF;

B. documents pouvant être ouverts au moyen de Microsoft Word ou Excel.

(b) Si le fournisseur choisit d'envoyer sa soumission par voie de courriel, le Canada exige de sa part qu'il respecte les instructions suivantes :

(i) **Réponses par courriel** : Les soumissions doivent être présentés par courriel à :

TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

(ii) **Présentation des pièces jointes** : Les formats approuvés des pièces jointes peuvent être une combinaison de ce qui suit :

A. documents en format PDF;
B. documents pouvant être ouverts au moyen de Microsoft Word ou Excel.

(iii) **Taille des courriels** : Les fournisseurs doivent s'assurer de soumettre leur réponse en plusieurs courriels si la taille d'un seul courriel, pièces jointes incluses, est supérieure à 5 Mo.

(iv) **Titre des courriels** : Les fournisseurs doivent indiquer le numéro de la DAMA dans la ligne «Objet» de chaque courriel faisant partie de la réponse.

(c) En raison du caractère de la DAMA, les soumissions transmis par courrier ou par télécopieur à l'intention de SPAC ne seront pas acceptés.

(d) **Soumission d'informations confidentielles.** Les fournisseurs sont priés de marquer comme confidentielles toutes les informations confidentielles incluses dans leur soumission. Les informations confidentielles doivent être clairement identifiées en marquant chaque page comme «Confidentiel» et en mettant en évidence toutes les informations confidentielles.

2.3 Programme de contrats fédéraux pour l'équité en matière d'emploi – Avis

Le Programme de contrats fédéraux pour l'équité en matière d'emploi exige que certains entrepreneurs s'engagent formellement auprès d'Emploi et Développement social Canada (EDSC) – Travail, à mettre en œuvre un programme d'équité en matière d'emploi. Si la présente soumission en matière d'approvisionnement mène à l'attribution d'un contrat assujetti au Programme de contrats fédéraux pour l'équité en matière d'emploi, les modèles de demande de soumissions et de contrats subséquents comprendront des exigences à cet effet. Pour obtenir d'autres renseignements sur le Programme de contrats fédéraux pour l'équité en matière d'emploi, consulter le site Web d'Emploi et Développement social Canada (EDSC) – Travail.

2.4 Demandes de renseignements – demande d'arrangements en matière d'approvisionnement

(a) Toutes les demandes de renseignements doivent être présentées par écrit au responsable de l'arrangement en matière d'approvisionnement.

(b) Les fournisseurs devraient citer le plus fidèlement possible le numéro de l'article de la DAMA auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère « exclusif » doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au fournisseur de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les

fournisseurs. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les fournisseurs.

2.5 Lois applicables

(a) L'arrangement en matière d'approvisionnement (AMA) et tout contrat attribué dans le cadre de l'AMA seront interprétés et régis selon les lois en vigueur en Ontario, Canada et les relations entre les parties seront déterminés par ces lois.

(b) À leur discrétion, les fournisseurs peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de l'arrangement ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé dans l'article 6.10 et en insérant le nom de la province ou du territoire canadien de leur choix dans le formulaire 1. Si aucun changement n'est indiqué, cela signifie que les fournisseurs acceptent les lois applicables indiquées.

2.6 Fournisseurs

(a) **Éditeurs de logiciels-services en tant que fournisseurs :** Les éditeurs de logiciels-services sont éligibles pour se qualifier sous le volet 1 et 2 de la présente DAMA. Les éditeurs de logiciels-services doivent soumettre le Formulaire d'attestation de l'éditeur de logiciels (Formulaire 2). Les fournisseurs de services infonuagiques (CSP) qui sont aussi des éditeurs de logiciels-services doivent soumettre le formulaire d'attestation de l'éditeur de logiciels-services (Formulaire 2) pour leurs propres solutions de logiciels-services et le formulaire d'autorisation de l'éditeur de logiciels (Formulaire 3) pour des solutions de logiciels-services hébergées par une tierce partie, tel qu'applicable.

(b) **Revendeurs de valeur ajouté en tant que fournisseurs** : Les revendeurs de valeur ajouté sont éligibles pour se qualifier sous le volet 3 de la présente DAMA. Les revendeurs de valeur ajoutée doivent soumettre le formulaire d'autorisation de l'éditeur de logiciels-services (Formulaire 3), attestant que le fournisseur a été autorisé à fournir les solutions de logiciels-services au Canada.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

Le Canada demande que les documents soient identifiés, groupés et présentés en sections distinctes comme suit :

Section I : Soumission technique
Section II : Soumission financière
Section III : Attestations
Section IV : Informations sur l'intégrité de la chaîne d'approvisionnement
Section V : Exigences en matière de cote de sécurité

3.2 Section I : Soumissions technique

(a) Dans la soumission technique, les fournisseurs doivent démontrer qu'ils satisfont à chaque exigence contenue dans la DAMA et fournir tous les documents et les renseignements demandés. La soumission technique doit être clair et traiter de façon suffisamment approfondie les points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée.

(b) Le Canada demande que les fournisseurs reprennent et présentent les sujets et les renseignements sous la forme indiquée dans les annexes applicables et/ou dans la DAMA.

(c) La soumission technique comprend les éléments suivants :

(i) **Formulaire de présentation des soumissions :** Formulaire 1 - formulaire de présentation des soumissions doit être joint aux soumissions. Il s'agit d'un formulaire commun dans lequel les fournisseurs peuvent fournir les renseignements exigés, comme le nom d'une personne-ressource, le numéro d'entreprise – approvisionnement du fournisseur et le statut du fournisseur au titre du Programme de marchés fédéraux pour l'équité en matière d'emploi. Si le Canada considère que les renseignements requis dans le formulaire de présentation des soumissions sont incomplets ou doivent être corrigés, il accordera au fournisseur la chance de soumettre les corrections requises.

(ii) **Formulaire pour les solutions de logiciels-services en tant que fournisseur:** Formulaire 2 (le cas échéant) - Si l'éditeur du logiciel-service (défini comme l'entité ou la personne titulaire du droit d'auteur sur toute solution de logiciel-service incluse dans la soumission et qui a le droit de: la licence et autoriser des tiers à utiliser sa solution de logiciel-service et tous les composants sous-jacents) a l'intention de soumettre une soumission et de se qualifier en tant que fournisseur de plein droit, cet éditeur de solution de logiciel-service doit soumettre le formulaire de certification 2.

(iii) **Formulaire pour le revendeur avec valeur ajoutée en tant que fournisseur:** Formulaire 3 (le cas échéant) - S'il s'agit d'un revendeur (un tiers qui n'est pas l'éditeur de solutions de logiciel-service, mais est autorisé à distribuer et à revendre les solutions SaaS au tiers partie) a l'intention de soumettre une soumission et de se qualifier de fournisseur à part entière; ce revendeur doit alors certifier que son éditeur, conformément au formulaire 3, certifie qu'il a été autorisé à fournir le logiciel en mode de logiciel-service de l'éditeur de solution de logiciel-service.

(iv) **Justification de la conformité aux exigences de qualification**: les fournisseurs doivent justifier de la conformité aux exigences de qualification énoncées à l'annexe A – Exigences de qualification. La justification ne doit pas être simplement une répétition des exigences, mais doit expliquer et démontrer comment le fournisseur répond à ces exigences. Indiquer simplement que

le fournisseur ou la solution de logiciels-services proposée est conforme n'est pas suffisant. Lorsque le Canada détermine que la justification n'est pas complète, la soumission sera déclarée non recevable et rejetée.

(v) **Accords sur les niveaux de service (ANS) :** Les fournisseurs doivent soumettre des accords sur les niveaux de service (ANS) publiés décrivant les accords de niveaux de service à inclure dans l'annexe D, Accords sur les niveaux de service (ANS). De même, toutes les modalités qui comportent des renseignements sur les prix (comme, mais sans s'y limiter, celles qui tentent d'imposer des conditions financières, des modalités tarifaires ou des pénalités pour non-conformité) figurant à l'annexe D, Accords sur les niveaux de service, seront considérées comme annulées et sont inopérantes.

Les engagements en matière de niveau de service (précisés dans les accords sur les niveaux de service publiés) doivent offrir aux clients commerciaux un soutien qui comprend, au minimum, le soutien offert sur le marché et rendu public (c.-à-d. la garantie et les services de maintenance et de soutien) généralement fourni aux clients des Solutions de logiciels services.

Les accords sur les niveaux de service peuvent être contenus dans un seul document visant l'ensemble des Solutions de logiciels services ou dans plusieurs documents propres à chacune des Solutions de logiciels services. Si un fournisseur fournit différents accords sur les niveaux de service pour différentes Solutions de logiciels services, il doit indiquer clairement la Solution de logiciels services et l'accord correspondant.

Seules les modalités de l'ANS relatives aux niveaux de service et à la prestation de service s'appliqueront. Toute modalité de l'ANS non liée aux niveaux de service et à la prestation des services, telles qu'elles sont décrites ci-dessous, sera réputée annulée et ne s'appliquera pas.

Les conditions générales relatives aux niveaux de service et à la prestation de services en vertu des accords sur les niveaux de service doivent inclure les éléments suivants :

A. Disponibilité – rendement
B. Définition de temps d'arrêt – prévu et non prévu
C. Crédits de service – éléments déclencheurs et calcul
D. Disponibilité des services de soutien
E. Libre-service, base de connaissances, tutoriels en ligne
F. Erreurs : définitions des degrés de gravité
G. Temps moyen de réponse et de réparation
H. Acheminement au palier hiérarchique approprié et procédure
I. Disponibilité d'un système de reprise après sinistre

(vi) **Formulaire 5 - La liste de vérification obligation de l'exhaustivité** de la soumission du fournisseur doit être jointe à la soumission. Il s'agit d'un formulaire commun dans lequel le soumissionnaire peut vérifier que sa soumission comprend tous les renseignements requis afin d'être jugé complet, avant de le présenter. Si le Canada considère que la liste de vérification ou la soumission présenté est incomplet ou doit être corrigé, le Canada accordera au fournisseur la chance de compléter ou de corriger ces renseignements.

(vii) **Conformité à l'annexe B, Obligations en matière de sécurité et de protection de la vie privée.** Les fournisseurs doivent se conformer aux obligations figurant à l'annexe B, Obligations en matière de sécurité et protection de la vie privée, lorsqu'ils présentent une soumission et pendant toute la durée de leur AMA. Les fournisseurs doivent prouver qu'ils respectent les obligations en matière de sécurité et de protection de la vie privée énoncées à l'annexe B en

répondant aux exigences obligatoires énoncées à l'annexe A, Exigences de qualification, paliers 1 et 2 (selon le cas). Les fournisseurs peuvent avoir à prouver qu'ils se conforment toujours à l'annexe B, Obligations en matière de sécurité et de protection de la vie privée, sur demande pendant toute la durée de tout contrat attribué dans le cadre de l'AMA.

(viii) **Confirmation de l'inscription au Programme d'évaluation de la sécurité des logiciels-services (volets 1, 2 et 3) :** La réponse doit comprendre la documentation confirmant que l'éditeur des logiciels-services ou les distributeurs à valeur ajoutée de la solution proposée sont inscrits au processus d'évaluation de la sécurité des logiciels-services décrit à l'annexe L, Programme d'évaluation de la sécurité informatique des logiciels-services : Processus d'intégration.

3.3 Section II : Soumission financière

(a) Dans la soumission financière, les fournisseurs doivent soumettre un catalogue de Solutions de logiciels-services proposées et de services professionnels connexes (tels qu'ils sont décrits à l'alinéa (b) ci-dessous), comportant leurs prix commerciaux et la remise en pourcentage applicable. Les fournisseurs doivent choisir l'une des options suivantes pour soumettre leurs prix plafonds pour les Solutions de logiciels-services et les services professionnels à l'annexe C – Prix plafonds pour les Solutions de logiciels-services et les services professionnels :

(i) Option 1 : Les fournisseurs fournissent un lien vers leur catalogue de Solutions de logiciels-services disponibles dans le commerce et précisent le pourcentage de remise offert au Canada.
(ii) Option 2 : Le fournisseur remplit le tableau à l'annexe C – Prix plafonds pour les Solutions de logiciels-services et les services professionnels en inscrivant leurs prix commerciaux.

Lorsqu'un lien vers un catalogue en ligne est fourni conformément à l'option 1, le Canada se réserve le droit de demander au fournisseur d'inclure dans son catalogue en ligne tous les renseignements demandés dans l'alinéa (d) ci-dessous. Lorsqu'un tableau est fourni conformément à l'option 2, le Canada se réserve le droit de demander au fournisseur de rendre cette information disponible dans un catalogue en ligne à l'avenir. Tous les renseignements sur les prix figurant ailleurs dans la soumission du fournisseur, y compris dans l'annexe D, Accords sur les niveaux de service, seront considérés comme annulés et sont inopérants.

(b) Les services professionnels à acquérir par l'entremise de la DAMA se limitent aux suivants : trousse de formation et de services Guide de démarrage rapide (« GDR »), services de mise en œuvre, services de formation, services d'épuration, de migration et de transition des données et services consultatifs. Toutefois, lorsqu'un lien est fourni vers un catalogue en ligne conformément à l'option 1, les fournisseurs ne sont pas tenus de créer un catalogue personnalisé pour la DAMA.

(c) **Période de mise à jour** – Les titulaires d'arrangements en matière d'approvisionnement sont autorisés à mettre à jour leurs prix plafonds pour les Solutions de logiciels-services et les services professionnels sur une base régulière.

(i) Les fournisseurs sont autorisés à soumettre une nouvelle annexe C – Prix plafonds pour les Solutions de logiciels-services et les services professionnels au plus une fois par mois.
(ii) Lorsqu'un lien est fourni vers un catalogue en ligne, les fournisseurs seront autorisés à mettre à jour leur catalogue en ligne aussi souvent que nécessaire, pourvu qu'ils avisent le responsable de l'arrangement en matière d'approvisionnement avant la publication d'une nouvelle version.
(iii) Tous les prix plafonds pour les Solutions de logiciels-services et les services professionnels sont sujets à examen et le responsable de l'arrangement en matière d'approvisionnement peut demander une référence de prix à tout moment pendant la durée de l'arrangement.

(d) La soumission financière doit traiter de façon claire et suffisamment détaillée des points assujettis aux critères d'évaluation en fonction desquels la soumission sera évaluée. Les points suivants devraient être fournis dans les **prix plafonds pour les Solutions de logiciels-services et les services professionnels** du fournisseur :

(i) **Numéro de pièce de l'éditeur de logiciels-services :** Le fournisseur doit inscrire le numéro de pièce utilisé par l'éditeur de logiciels-services pour identifier la Solution de logiciels-services commercialement.

(ii) **Nom de la Solution de logiciels-services ou des services professionnels :** Le fournisseur doit indiquer le nom commercial utilisé par l'éditeur de logiciels-services pour identifier commercialement la Solution de logiciels-services.

(iii) **Nom de l'éditeur de logiciels-services :** Le fournisseur doit inscrire le nom de l'éditeur de logiciels-services qui possède les droits de propriété intellectuelle de la Solution de logiciels-services.

(iv) **Nom du fournisseur de services infonuagiques (CSP) :** Le fournisseur doit identifier le fournisseur de services infonuagiques (CSP) dont les services infonuagiques sont utilisés pour fournir au Canada la Solution de logiciels-services proposée.

(v) **Prix plafonds :** Le fournisseur doit soumettre les prix plafonds proposés à l'annexe C, Prix plafonds pour les Solutions de logiciels-services et les services professionnels. Les prix doivent respecter les conditions suivantes :

A. la tarification commerciale du fournisseur;
B. prix exprimés en dollars canadiens;
C. exclure la taxe sur les produits et services (TPS) ou la taxe de vente harmonisée (TVH).

(vi) **Unité de mesure :** Le fournisseur doit inscrire l'unité de mesure pour le logiciel-service, telle que « par utilisateur », « par entité », « par jour », etc.) selon laquelle les Solutions de logiciels-services et les services professionnels seront fournis au Canada.

(vii) **Rabais en pourcentage applicable :** Les fournisseurs doivent saisir le pourcentage de rabais qui sera appliqué aux prix unitaires commerciaux plafonds pour la durée de l'AMA.

(viii) **Langue(s) disponible(s) :** Le fournisseur doit fournir la ou les langue(s) disponible(s) pour la Solution de logiciels-services, en indiquant « EN » pour anglais, « FR » pour français, ou « EN, FR » pour les deux.

(ix) **Information sur les Solutions de logiciels-services :** Le fournisseur doit inscrire une adresse de site Web affichant l'information sur la Solution de logiciels-services.

(x) **Mots clés** : Le fournisseur peut fournir des mots-clés associés à sa (ses) solution(s) de logiciels-services et à services professionnels qui seront utilisés dans la fonction de recherche pour aider les clients à repérer facilement dans le catalogue des Solutions de logiciels-services et des services professionnels qui répondent à leurs besoins.

(e) **Référence des prix** : Le fournisseur doit fournir une ou des références de prix pour prouver que les prix proposés sont justes et raisonnables. Sans prétendre à l'exhaustivité, voici quelques exemples de références de prix acceptables:

(i) la liste de prix publiée courante;

(ii) une copie des factures payées pour une qualité et une quantité semblables de biens, de services ou les deux vendus à d'autres clients;

(iii) toutes autres pièces justificatives demandées par le Canada.

3.4 Section III : Attestations

Les fournisseurs doivent présenter les attestations et les renseignements supplémentaires exigés à la Partie 5.

3.5 Section IV : Processus continu d'intégrité de la chaîne d'approvisionnement

(a) Les fournisseurs doivent satisfaire aux exigences en matière d'intégrité de la chaîne d'approvisionnement O6 et O7, palier 1, pour les données jusqu'au niveau Protégé A et O10 et O11, palier 2, pour les données jusqu'au niveau Protégé B (Gestion de la chaîne d'approvisionnement) décrites dans l'annexe A, Exigences de qualification de la DAMA. Les exigences doivent être satisfaites avant qu'un AMA soit attribué.

(b) Les fournisseurs doivent soumettre l'information sur la sécurité de la chaîne d'approvisionnement demandée dans le Formulaire 6, Modèle de soumission SCI et la tenir à jour ou la modifier à la demande du responsable de la sécurité de la chaîne d'approvisionnement. Le Canada utilisera cette information pour évaluer si, à son avis, la chaîne d'approvisionnement proposée par un fournisseur pourrait faire en sorte que la solution de logiciel-service proposée par le fournisseur compromette ou serve à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, conformément au processus d'intégrité de la chaîne d'approvisionnement décrit à la section 4.3**, Processus d'intégrité de la chaîne d'approvisionnement**.

(c) En soumettant son ISCA, et en considération de l'opportunité de participer à ce processus d'approvisionnement, le fournisseur accepte les termes de l'accord de non-divulgation figurant à l'annexe K, SPAC Accord de non-divulgation concernant Intégrité de la chaîne d'approvisionnement.

3.6 Section V : Exigences en matière de cote de sécurité

(a) **Exigences en matière de cote de sécurité :** Les fournisseurs doivent satisfaire aux exigences en matière de cote de sécurité O4, palier 1, pour les données jusqu'au niveau Protégé A et O7, palier 2, pour les données jusqu'au niveau Protégé B (Sécurité du personnel) décrites dans l'annexe A, Exigences de qualification, de la DAMA. Les exigences doivent être satisfaites avant qu'un AMA soit attribué.

(b) **Entrepreneur et sous-traitant :** L'entrepreneur et tous les sous-traitants doivent satisfaire aux exigences en matière de sécurité énoncées à l'annexe G, Exigences relatives à la sécurité pour les entrepreneurs canadiens, à l'annexe H, Exigences relatives à la sécurité pour les entrepreneurs étrangers, à l'annexe I - LVERS pour SaaS et l'annexe J - Guide de classification de sécurité des LVERS dans la DAMA selon le cas.

(c) **Délai :** Les fournisseurs doivent prendre des mesures pour obtenir rapidement les cotes de sécurité nécessaires. Les exigences en matière de cote de sécurité doivent être satisfaites avant qu'un AMA soit attribué.

(d) **Fournisseur faisant partie d'une coentreprise :** Sauf indication contraire dans la demande de soumissions, si le soumissionnaire est une coentreprise, chacun des membres de celle-ci doit respecter les exigences relatives à la sécurité décrit en (b) ci-dessus.

(e) **CCCS mène le processus d'autorisation en matière de cote de sécurité**: SPAC a passé un accord avec le Centre canadien de la cyber sécurité pour traiter les autorisations de cote de sécurité en parallèle avec l'évaluation de la sécurité des TI. SPAC ne contrôle donc pas le processus lui-même. Le processus peut être long et les soumissionnaires devraient l'initier dès que possible. Pour plus d'informations sur les exigences de sécurité, les soumissionnaires doivent se référer à: contact@cyber.gc.ca.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

(a) Les soumissions seront évaluées par rapport à l'ensemble du besoin de la demande des soumissions en matière d'approvisionnement incluant les critères d'évaluation techniques et financiers.

(b) Une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.

(c) **Demande de précisions :** Si le Canada demande des précisions au fournisseur sur sa soumission ou s'il veut vérifier celui-ci, le fournisseur disposera d'un délai de deux (2) jours ouvrables (ou d'un délai plus long précisé par écrit par le responsable de la soumission en matière d'approvisionnement) pour fournir les renseignements nécessaires au Canada. Le défaut de respecter les délais rendra la soumission non recevable, causera sa suspension ou retardera le traitement de l'AMA du fournisseur.

(d) **Droits du Canada**

(i) Le Canada se réserve le droit de refuser tout produit proposé par un fournisseur et de négocier les prix plafonds prévus à l'annexe C, Catalogue de Solutions de logiciels-services et de prix plafonds;

(ii) Le Canada se réserve le droit de refuser ou de négocier les modalités proposées par un fournisseur et soumises à l'annexe D, Accords sur les niveaux de service (ANS). Aucun arrangement d'approvisionnement ne sera accordé avant que le Canada approuve toutes les modalités.

4.2 Évaluation technique et financière

Les soumissions feront l'objet d'un examen pour en déterminer la conformité aux exigences obligatoires de la DAMA. Tous les éléments de la DAMA qui constituent des exigences obligatoires sont désignés précisément par les termes « doit », « doivent » ou « obligatoire ».Les fournisseurs qui ne respectent pas chacune des exigences obligatoires en seront avisés par le responsable de l'arrangement en matière d'approvisionnement. Ce dernier donnera un délai aux fournisseurs afin de se conformer aux exigences en question. À défaut de donner suite à la demande du responsable de l'arrangement en matière d'approvisionnement et de respecter cette exigence dans ce délai, la soumission sera jugé non recevable ou « en attente », ou le traitement de l'AMA du fournisseur sera retardé.

4.2.1 Critères techniques obligatoires

Les exigences techniques obligatoires sont les suivantes :

(i) Formulaire de présentation des soumissions, conformément au paragraphe 3.2(c)(i);
(ii) Justification de la conformité considérable aux exigences de qualification, conformément au paragraphe 3.2 (c) (iv);
(iii) Accords sur les niveaux de service (ANS), conformément au paragraphe 3.2. (c) (v);
(iv) Attestations, conformément au paragraphe 3.4;
(v) Viabilité financière, conformément au paragraphe 4.5.

4.2.2 Évaluation financière obligatoire

Les exigences financières obligatoires sont les suivantes :

(i) Annexe C – Prix plafonds pour les Solutions de logiciels services et les services professionnels, conformément aux alinéas 3.3 (a), (b), (c) et (d);
(ii) Référence des prix conformément à l'alinéa 3.3 (e).

4.2.3 Évaluation obligatoire de la sécurité

Voici les exigences obligatoires relatives à la sécurité :

(i) Cotes de sécurité de l'organisation et du personnel (conformément à l'annexe G, Exigences relatives à la sécurité pour les entrepreneurs canadiens, à l'annexe H, Exigences relatives à la sécurité pour les entrepreneurs étrangers, à l'annexe I - LVERS pour SaaS et l'annexe J - Guide de classification de sécurité des LVERS dans la DAMA).

(ii) Intégrité de la chaîne d'approvisionnement (conformément à la section 4.3).

(iii) Programme d'évaluation de la sécurité des TI des logiciels-services : Processus d'intégration (conformément à l'annexe L).

4.3 Processus d'intégrité de la chaîne d'approvisionnement

(a) L'intégrité de la chaîne d'approvisionnement (SCI) est étudiée lors de l'évaluation de la sécurité des TI des logiciels-services. Les évaluations de l'intégrité de la chaîne d'approvisionnement donnent encore plus la certitude que les mesures de contrôle de la sécurité mises en place sont moins susceptibles d'être ébranlées de manière malveillante par des auteurs de menaces au moyen d'attaques de la chaîne d'approvisionnement.

(b) Pour les fournisseurs de logiciels-services, le processus d'intégrité de la chaîne de l'approvisionnement initié par SPC est employé. Au cours de ce processus, le fournisseur de logiciels-services donne une liste des logiciels, du matériel informatique, des entrepreneurs et des fournisseurs auxquels il a recours pour fournir l'offre de services. Le fournisseur fait également régulièrement des comptes rendus au gouvernement du Canada pour l'informer de tout changement concernant la liste de départ. Si le gouvernement du Canada détermine que la liste des logiciels, du matériel informatique, des entrepreneurs et des fournisseurs est longue, des mesures de protection de l'intégrité de la chaîne d'approvisionnement de niveau 1 peuvent être requises.

(c) **Processus de l'SCI** : SPAC et le Centre canadien pour la cybersécurité en consultation avec Services partagés Canada ont conclu une entente selon laquelle le CCC traite l'évaluation de l'intégrité de la chaîne d'approvisionnement en parallèle avec l'évaluation de la sécurité des TI. SPAC ne contrôle donc pas le processus lui-même. Ce dernier peut être fastidieux; c'est pourquoi les soumissionnaires doivent l'entamer le plus tôt possible. Pour obtenir de plus amples renseignements au sujet des exigences en matière de sécurité, les soumissionnaires devraient se référer à l'annexe L, Programme d'évaluation de la sécurité des TI des logiciels-services : Processus d'intégration, pour en savoir plus sur le processus d'intégration.

(d) Veuillez consulter l'annexe L, Programme d'évaluation de la sécurité des TI des logiciels-services : Processus d'intégration, pour en savoir plus sur le processus d'intégration. Pour obtenir de plus amples renseignements au sujet des exigences relatives à la sécurité, les soumissionnaires doivent écrire à l'adresse : contact@cyber.gc.ca.

4.4 Méthode de sélection

Une soumission doit respecter les exigences de la demande d'arrangement en matière d'approvisionnement et satisfaire à tous les critères d'évaluation techniques et financiers obligatoires, et fournir toutes les certifications obligatoires pour être déclaré recevable.

4.5 Viabilité financière

Clause du *Guide des CCUA* S0030T (2014-11-27) Viabilité financière s'applique à et fait partie de la présente DAMA.

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

(a) Les fournisseurs doivent fournir les attestations et les renseignements supplémentaires exigés pour qu'un arrangement en matière d'approvisionnement (AMA) leur soit émis.

(b) Les attestations que les fournisseurs remettent au Canada peuvent faire l'objet d'une vérification par le Canada à tout moment par ce dernier. À moins d'indication contraire, le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur s'il est établi qu'une attestation est fausse, sciemment ou non, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée de tout arrangement en matière d'approvisionnement découlant de cette AMA et tous contrats subséquents.

(c) Le responsable de l'arrangement en matière d'approvisionnement aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du fournisseur. À défaut de répondre et de coopérer à toute demande ou exigence imposée par le responsable de l'arrangement en matière d'approvisionnement, l'arrangement peut être déclaré non recevable, ou constituera un manquement aux termes du contrat.

5.1 Attestations exigées avec l'arrangement en matière d'approvisionnement

Les fournisseurs doivent fournir les attestations suivantes dûment remplies avec leur soumission.

5.1.1 Dispositions relatives à l'intégrité - déclaration de condamnation à une infraction

Conformément aux dispositions relatives à l'intégrité des instructions uniformisées, tous les fournisseurs doivent présenter avec leur soumission, **s'il y a lieu**, le formulaire de déclaration d'intégrité disponible sur le site Web Intégrité – Formulaire de déclaration (http://www.SPAC-pwgsc.gc.ca/ci-if/declaration-fra.html), afin que sa soumission ne soit pas rejetée du processus d'approvisionnement.

5.1.2 Attestations additionnelles requises avec la soumission

Les certifications additionnelles ci-dessous sont requises dans le cadre de la soumission :

Formulaire 2 - Formulaire d'attestation de l'éditeur de logiciels-services
Formulaire 3 – Formulaire d'autorisation de l'éditeur de logiciels-services
Formulaire 4 – Attestation aux fins du programme de marches réservées aux entreprises autochtones.
Formulaire 5 – Liste de vérification de l'exhaustivité de la soumission

PARTIE 6 – ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT

6.1 Arrangement

Des arrangements en matière d'approvisionnement (AMA) seront attribués pour permettre au Canada de d'acquérir des solutions de logicielles-services y compris les services de maintenance et de soutien, de formation et de services professionnels associés, à la demande du Canada, à l'appui de ses divers programmes, besoins opérationnels et projets.

Les objectifs de cette méthode d'approvisionnement sont les suivants:

(a) simplifier le processus d'achat pour l'acquisition de solutions de logicielles-services ;

(b) appuyer les initiatives canadiennes de modernisation des achats et de simplification des contrats;

(c) accroître la concurrence et l'accès aux dernières solutions de logicielles-services sur le marché canadien; et

(d) accroître la transparence, l'ouverture et l'équité des processus d'approvisionnement du secteur public.

6.2 Exigences relatives à la sécurité

Le fournisseur doit satisfaire aux exigences de sécurité énoncées à l'annexe A, Exigences de qualification.

***Remarque aux fournisseurs**: Cette DAMA contient des exigences obligatoires à respecter pour la qualification. Le Canada se réserve le droit d'ajuster les exigences de sécurité ou les niveaux d'exigence de sécurité indiqués dans le présent arrangement en matière d'approvisionnement à tout moment au cours du processus de la DAMA ou après l'émission de l'arrangement en matière d'approvisionnement. Les fournisseurs qualifiés ne seront pas dispensés de respecter en permanence toutes les exigences en matière de sécurité et pourront être amenés à fournir des informations supplémentaires et à faire l'objet d'une évaluation de sécurité supplémentaire. Les fournisseurs qui ne répondent pas aux exigences de sécurité actuelles peuvent perdre leur statut qualifié.*

Il est à noter que les niveaux différents ou additionnels en matière de sécurité peuvent s'imposer aux clients ou aux travaux des clients, notamment le niveau d'habilitation de sécurité pour le fournisseur ou les ressources du fournisseur. Les exigences additionnelles en matière de sécurité peuvent être inclues dans la demande de soumission subséquente, contrat ou autorisation de travail dans le cadre du contrat de cet arrangement, le cas échéant.

6.3 Clauses et conditions uniformisées

Toutes les clauses et conditions identifiées dans l'arrangement en matière d'approvisionnement (AMA) et contrat(s) subséquent(s) par un numéro, une date et un titre sont énoncées dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Services publics et approvisionnement Canada.

6.3.1 Conditions générales

2020 (2017-09-21), Conditions générales - arrangement en matière d'approvisionnement - biens ou services, s'appliquent au présent arrangement en matière d'approvisionnement et en font partie intégrante.

6.3.2 Arrangement en matière d'approvisionnement - établissement des rapports

Le fournisseur doit compiler et tenir à jour des données sur les biens, les services ou les deux fournis au gouvernement fédéral en vertu de contrats découlant de l'AMA. Ces données doivent comprendre tous les achats, incluant ceux payés au moyen d'une carte d'achat du gouvernement du Canada.

Les données doivent être présentées au responsable des arrangements en matière d'approvisionnements ou mises à sa disposition pour téléchargement tous les trimestres, dans les 30 jours civils suivant la fin de la période de référence.

Voici la répartition des trimestres :

(a) Premier trimestre : du 1er avril au 30 juin;
(b) Deuxième trimestre : du 1er juillet au 30 septembre;
(c) Troisième trimestre : du 1er octobre au 31 décembre;
(d) Quatrième trimestre : du 1er janvier au 31 mars.

6.4 Durée de l'arrangement en matière d'approvisionnement

6.4.1 Période de l'arrangement en matière d'approvisionnement

La période pour attribuer des contrats dans le cadre de l'AMA va de la date d'émission d'un AMA à un fournisseur, jusqu'à la date à laquelle l'arrangement en matière d'approvisionnement est résilié ou arrive à expiration.

6.4.2 Ententes sur les revendications territoriales globales (ERTG)

AMA est d'établir la livraison du besoin décrit dans le cadre de l'AMA aux utilisateurs désignés, et ce, partout au Canada (tel que défini à la section 6.6 ci-dessous), sauf dans les zones visées par des ententes sur les revendications territoriales globales (ERTG) au Yukon, dans les Territoires du Nord-Ouest, au Nunavut, au Québec et au Labrador. Les produits à livrer dans ces zones devront faire l'objet de marchés distincts, attribués en dehors d'AMA.

6.5 Responsables

6.5.1 Responsable de l'arrangement en matière d'approvisionnement

Le responsable de l'arrangement en matière d'approvisionnement est :

Nom: Elizabeth Quenville
Titre: Chef, Approvisionnements

Services publics et approvisionnement Canada
Direction générale des approvisionnements
Direction des achats de logiciels

Les Terrasses de la Chaudière
10, rue Wellington, 4ème étage
Gatineau, Québec K1A OH4

Téléphone : 613-858-6142

Télécopieur : 819-956-2675
Courriel : TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

Le responsable d'AMA est responsable de l'émission de l'arrangement en matière d'approvisionnement, de son administration et de sa révision, s'il y a lieu.

6.5.2 Représentant du fournisseur

Compléter ou supprimer, selon le cas.

6.5.3 L'autorité sur la sécurité de la chaine d'approvisionnement

L'autorité sur la sécurité de la chaine d'approvisionnement pour le contrat est:
Nom: _____
Titre: _____
CCC : _____
Adresse: _____
Téléphone: _____
Courriel: _____

L'autorité sur la sécurité de la chaine d'approvisionnement est le représentant de CCC et est responsable pour ce qui concerne au processus d'intégrité sur la chaine d'approvisionnement dans le cadre du contrat. Ni l'autorité contractante ni l'autorité technique ne sont habilités à conseiller ou à autoriser des informations relatives au processus d'intégrité de la chaîne d'approvisionnement. Toutes les autres questions liées à la sécurité relèvent de la responsabilité de l'autorité sur la sécurité de la chaine d'approvisionnement.

6.6 Utilisateurs désignés

L'AMA peut être utilisé pour acquérir des Solutions de logiciels-services par tout ministère, agence ou organisme ministériel du Canada (ou tout autre organisme du Canada, y compris ceux décrits dans la Loi sur la gestion des finances publiques telle que modifiée de temps à autre), et par toute autre partie pour laquelle SPAC a été autorisé à agir.

6.7 Occasion de qualification continue

Un avis sera affiché de façon continue par l'entremise du Service électronique d'appels d'offres du gouvernement (SEAOG) pour permettre à de nouveaux fournisseurs de se qualifier.

6.8 Ordre de priorité des documents

En cas d'incompatibilité entre le libellé des textes énumérés dans la liste, c'est le libellé du document qui apparaît en premier sur la liste qui l'emporte sur celui de tout autre document qui figure plus bas sur la liste.

(a) les articles de l'arrangement en matière d'approvisionnement;
(b) les conditions générales 2020 (2017-09-21), Conditions générales - arrangement en matière d'approvisionnement - biens ou services
(c) Annexe A, Exigences de qualification;
(d) Annexe B, Obligations en matière de protection de la vie privée;
(e) Annexe C, Catalogue de solutions de logiciels-services et prix plafonds;
(f) Annexe D, Accords sur les niveaux de service (ANS);
(g) Annexe E, Modèle de demande de soumission pour logiciels-services;
(h) Annexe F, Clauses du contrat subséquent;
(i) Annexe G, Exigences relatives à la sécurité pour les entrepreneurs canadiens
(j) Annexe H, Exigences relatives à la sécurité pour les entrepreneurs étrangers
(k) Annexe I - LVERS pour SaaS

(l) Annexe J - Guide de classification de sécurité des LVERS
(m) Annexe K, Accord de non-divulgation de SPAC relatif à l'intégrité de la chaîne d'approvisionnement
(n) Annexe L, Programme d'évaluation de la sécurité des TI des logiciels-services :
(o) soumission du fournisseur daté du _____ (*insérer la date de la soumission*), *(si la soumission a été clarifié ou modifié,* insérer au moment de l'émission de l'arrangement *:* « clarifié le _____ » *ou* « tel que modifié le _____ » (*insérer la ou les dates de la ou des clarifications ou modifications s'il y a lieu)*.

6.9 Attestations et renseignements supplémentaires

6.9.1 Conformité

À moins d'indication contraire, le respect continu des attestations fournies par le fournisseur avec sa soumission ou préalablement à l'émission de l'AMA, ainsi que la coopération constante quant aux renseignements supplémentaires, sont des conditions d'émission de l'AMA et le non-respect constituera un manquement de la part du fournisseur. Les attestations pourront faire l'objet de vérifications par le Canada pendant toute la durée de l'AMA et de tout contrat subséquent qui serait en vigueur au-delà de la période de l'AMA.

6.10 Lois applicables

L'arrangement en matière d'approvisionnement (AMA) et tout contrat découlant de l'AMA doivent être interprétés et régis selon les lois en vigueur _____ *(insérer la loi de la province ou du territoire précisée par le fournisseur dans la soumission, s'il y a lieu)* et les relations entre les parties seront déterminées par ces lois.

PARTIE 7 – SÉLECTION DES ENTREPRENEURS ET CLAUSES DU CONTRAT SUBSÉQUENT

7.1 Pouvoir adjudicateur et limites

Le client et les agents de négociation des contrats de SPAC à qui SPAC a donné le droit d'utiliser l'AMA peuvent émettre les contrats résultants en utilisant leurs pouvoirs d'approbation et de signature des contrats existants.

7.2 Sélection de l'entrepreneur

(a) **Besoins évalués à moins de 25 000 $ CAN (applicables taxes inclus)**

(i) Source unique: Pour les besoins inférieurs à 25 000,00 $ CAN (applicables taxes inclus), le Canada peut choisir, à sa seule discrétion, de sous-traiter des contrats à un fournisseur ou de passer des contrats après la demande de soumissions.

(ii) S'il n'existe qu'une seule source d'approvisionnement pour la solution de logiciel-service, le Canada peut demander au fournisseur de fournir un support de prix avant l'attribution du contrat. Le Canada se réserve le droit de négocier avec le fournisseur s'il est déterminé que les prix proposés ne représentent pas une bonne valeur pour le Canada.

(b) **Besoins évalués à 25 000 $ CAN (TPS / TVH / TVQ incluse) ou plus**

(i) Demande de soumissions: si plusieurs solutions de logiciels-services disponibles dans le catalogue de logiciels-services peuvent répondre aux exigences techniques du Canada, le Canada peut émettre une demande de soumissions. Si le Canada détermine que le catalogue de logiciels-services ne dispose pas de capacités suffisantes ou qu'il s'agit d'une exigence complexe et / ou spécialisée, il peut acquérir la solution de logiciels-services en dehors du catalogue de logiciels-services et étendre le concours à toutes les entreprises en publiant un document de demande de proposition officiel sur le SEAOG.

(c) **Réservé/entreprise autochtone**

(i) À la discrétion de chaque client, certaines sollicitations contre les AMA résultants peuvent être mises de côté pour des entreprises autochtones en vertu du CCSP du gouvernement fédéral.

(ii) Si le Canada souhaite passer un contrat en vertu du CCSP, il peut le faire en utilisant les AMA des fournisseurs autochtones. Toutes les conditions énoncées dans la présente AMA s'appliquent aux AMA des fournisseurs autochtones.

7.3 Procédures de demande de soumissions

(a) Des demandes de soumissions seront émises aux fournisseurs auxquels un arrangement en matière d'approvisionnement (AMA) a été émis, pour des besoins spécifiques dans le cadre de l'AMA.

(b) La demande de soumissions sera publiée par l'entremise du Service électronique d'appels d'offres du gouvernement (SEAOG) ou envoyée directement aux fournisseurs.

(c) Les fournisseurs disposent d'au moins quinze (15) jours civils pour répondre au Canada, ou de la période précisée par l'autorité contractante selon la période la plus longue.

(d) La demande de soumissions comprendra, au minimum :

(i) exigences de sécurité supplémentaires ou mises à jour *(s'il y a lieu)*;

(ii) une description complète de la Solution de logiciels-services à être fournie;

(iii) 2003, Instructions uniformisées - biens ou services - besoins concurrentiels.

Le paragraphe 3.a) de l'article 01 Dispositions relatives à l'intégrité - soumission, des instructions uniformisées 2003 incorporées ci-haut par renvoi, est supprimé en entier et remplacé par ce qui suit :

«au moment de présenter une soumission dans le cadre de la demande d'arrangements en matière d'approvisionnement (DAMA), le soumissionnaire a déjà fourni une liste complète des noms, tel qu'exigé en vertu de la *Politique d'inadmissibilité et de suspension*. Pendant ce processus d'approvisionnement, le soumissionnaire doit immédiatement informer le Canada par écrit de tout changement touchant la liste des noms.»

(iv) les instructions pour la préparation des soumissions;

(v) les instructions sur la présentation des soumissions (l'adresse pour la présentation des soumissions, la date et l'heure de clôture);

(vi) les procédures d'évaluation et la méthode de sélection;

(vii) capacité financière (*s'il y a lieu*);

(viii) les attestations;

(ix) les conditions du contrat subséquent.

(e) Annexe E – Le modèle de demande de soumissions pour logiciels-services peut être utilisé pour mener une des demandes de soumissions.

7.4 Clauses du contrat subséquent

L'arrangement en matière d'approvisionnement stipule que les clauses de l'annexe F doivent être appliquées et intégrées à chaque contrat conclu en vertu de l'arrangement en matière d'approvisionnement. Les clauses du contrat subséquent peuvent inclure des exigences supplémentaires identifiées par le client.

ANNEXE A – EXIGENCES DE QUALIFICATION

Les quinze (15) exigences de sécurité suivantes doivent être respectées afin de démontrer la conformité à l'assurance du Palier 1 **(données jusqu'au niveau Protégé A, inclusivement).**

Palier 1 (Renseignements classés jusqu'au niveau Protégé A, inclusivement)

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O1	**Rôles et responsabilités en matière de sécurité**	Le fournisseur doit définir clairement les rôles et les responsabilités en ce qui concerne les contrôles de sécurité et les fonctionnalités des services entre le fournisseur (tout sous-processeur du fournisseur, le cas échéant) et le Canada.	Dans le document, le fournisseur doit inclure, au minimum, les rôles et responsabilités des parties en ce qui concerne: (a) la gestion des comptes; (b) la protection des frontières; (c) la sauvegarde des actifs et du système d'information; (d) la gestion des incidents; (e) la surveillance du système; et (f) la gestion des vulnérabilités.
O2	**Protection des données**[1]	Les emplacements physiques du logiciel-service public commercial (qui peut contenir des données du Canada) doivent être situés à l'un ou l'autre de ces endroits : (a) un pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN);	Le fournisseur doit présenter une documentation démontrant la façon dont le logiciel-service public commercial proposé satisfait aux exigences obligatoires de l'Exigences relatives à la protection des données. Pour être jugée conforme, la documentation fournie doit inclure :

[1] Aux fins de cette annexe A, Solution disponible dans le commerce. Solution qui est une solution disponible dans le commerce fournie à d'autres clients. Dans le cadre de son abonnement pour utiliser la solution, l'entrepreneur s'engage à mettre à la disposition du Canada toutes les fonctions et fonctionnalités incluses dans la version disponible dans le commerce de la solution, ainsi que les services d'infrastructure informatique auxiliaires et requis nécessaires à la fourniture de la solution, tous qui est inclus dans le prix de l'abonnement.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		(b) un pays membre de l'Union européenne (UE); ou (c) un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité industrielle. **Les fournisseurs sont priés de noter ce qui suit** : De plus amples renseignements sur les pays de l'OTAN sont accessibles à l'adresse suivante : https://www.nato.int/cps/fr/natohq/nato_countries.htm. De plus amples renseignements sur les pays de l'UE sont accessibles à l'adresse suivante : https://europa.eu/european-union/about-eu/countries_fr. Dans le cadre du Programme de sécurité des contrats, des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays énumérés sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html de SPAC, tel qu'il est mis à jour de temps à autre.	(a) une liste à jour des emplacements physiques (y compris la ville et le pays) de chaque centre de données susceptible de contenir des données du Canada, y compris des données sauvegardées ou redondantes. L'Exigences relatives à la protection des données, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O3	**Installations des centres de données**	Le fournisseur du logiciel-service public commercial proposé doit mettre en place des mesures de sécurité qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les données du gouvernement du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommages et de saisie, et qui sont fondées sur une approche de détection et de	Le fournisseur doit présenter une documentation démontrant la façon dont le fournisseur du logiciel-service (et, le cas échéant, l'autre fournisseur de services) des services proposés respecte les exigences relatives aux installations des centres de données. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents de système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures servant à

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		récupération préventive en matière de sécurité physique. Cette description doit inclure, à tout le moins, les éléments qui suivent : (a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont suffisamment disparates sur le plan géographique pour que la perte d'un centre de données n'empêche pas la récupération des données conformément à l'ENS prescrite; (b) l'utilisation adéquate des supports de TI; (c) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; (d) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; (e) la restriction de l'accès physique aux actifs des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, et valider l'accès au moyen de deux formes d'identification; (f) l'accompagnement des visiteurs et la surveillance de leur activité; (g) la tenue des registres de vérification de l'accès physique;	protéger les installations de TI et les actifs du système d'information dans lesquels les données du gouvernement du Canada sont stockées et protégées contre toute forme de manipulation, de perte, de dommages et de saisie, et qui sont fondées sur une approche de détection et de récupération préventive en matière de sécurité physique. Les exigences relatives aux installations du centre de données, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service public commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		(h) le contrôle et la gestion des dispositifs d'accès physique; (i) l'application des mesures de protection des données du GC à d'autres lieux de travail (p. ex., les sites de télétravail); et (j) la consignation et la surveillance de tous les accès physiques aux installations des centres de données et de tous les accès par voie électronique aux composants des systèmes d'information qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.	
O4	**Sécurité du personnel**	Le fournisseur du logiciel-service public commercial proposé doit mettre en place des mesures de sécurité qui accordent et maintiennent le niveau de filtrage de sécurité requis pour son personnel respectif ainsi que pour le personnel de tout sous-traitant, en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Les mesures en matière de filtrage de sécurité seront appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou à une norme équivalente approuvée par le Canada. Cette description doit inclure, à tout le moins, les éléments qui suivent :	Le fournisseur doit présenter une documentation démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences relatives à la sécurité du personnel. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures utilisés pour accorder et maintenir le niveau de filtrage de sécurité requis pour le personnel du fournisseur ainsi que pour le personnel de tout sous-traitant, en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Les exigences relatives à la sécurité du personnel, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		(a) une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du Canada ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services; (b) le processus visant à s'assurer que les employés et les entrepreneurs connaissent, comprennent et respectent leurs responsabilités en matière de sécurité de l'information et que le rôle que l'on compte leur confier leur convient; (c) le processus relatif à la sensibilisation et à la formation en matière de sécurité dans le cadre de l'intégration à l'emploi et lorsque les rôles des employés et des sous-traitants changent; (d) le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi; et (e) approche de détection des initiés malveillants potentiels et des contrôles mis en œuvre pour atténuer le risque d'accès aux données du GC ou d'incidence sur la fiabilité du logiciel-service hébergeant les actifs et les données du gouvernement du Canada.	expliquer et démontrer la façon dont le fournisseur du logiciel-service public commercial proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O5	**Assurance d'une tierce partie**	Le logiciel-service doit être conçu et développé pour assurer la sécurité de leur logiciel-service public proposé disponible sur le marché, y compris la mise en œuvre des politiques, des procédures et des 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

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		Pour les fournisseurs qui ont déjà complété l'évaluation en sécurité en fournissant au CCC les rapports de certification de sécurité SOC 2 Type II et qui ont déjà conclu une entente de non divulgation (END) avec le CCC doivent transmettre leur certification et leurs rapports de certification directement au CCC à contact@cyber.gc.ca afin de se conformer à cette exigence. Pour les fournisseurs qui n'ont pas complété l'évaluation en sécurité, le processus d'intégration commencera une fois que la soumission respectera les exigences de la demande d'arrangement en matière d'approvisionnement et satisfera à tous les critères d'évaluation techniques et financiers obligatoires et fournira tous les éléments obligatoires de certifications pour être déclarée recevable. SPAC référera ensuite le fournisseur aux services clients de CCC pour commencer le processus d'intégration de l'évaluation en TI et pour conclure une END en vue de recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire exigée aux termes de cette exigence.	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 : (a) l'une des certifications 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; (b) autoévaluation 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 : 1. être valide à la date de clôture de la 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

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
			données, le rapport d'évaluation de l'organisation sous-traitante doit être inclus, et 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.
O6	**Gestion de la chaîne d'approvisionnement**	Le fournisseur doit présenter une liste de fournisseurs tiers contenant des renseignements à leur sujet (filiales, sous-traitants, y compris les fournisseurs de services infonuagiques, etc.) qui fourniraient au Canada le logiciel-service public commercial. Aux fins de cette exigence, une entreprise qui n'est qu'un fournisseur de biens du fournisseur du logiciel-service public commercial proposé, mais qui n'exécute aucune partie de la chaîne d'approvisionnement qui pourrait fournir au Canada le logiciel-service public commercial, n'est pas considérée comme un tiers. Parmi les exemples de tiers, mentionnons les techniciens qui pourraient être déployés ou qui seraient affectés à la maintenance du logiciel-service public commercial du fournisseur du	Le fournisseur doit fournir une liste de documentation des sous-processeurs pouvant être utilisés pour exécuter une partie quelconque des services en fournissant les services au Canada. La liste doit inclure les informations suivantes (i) le nom du sous-processeur; (ii) l'identification des activités de périmètre qui seraient réalisées par le sous-processeur; et (iii) le ou les emplacements où le sous-processeur effectuerait les activités requises pour prendre en charge les services. Pour le SaaS, le contractant doit démontrer que l'IaaS/PaaS est mis à profit par ces services: (a) Les sous-processeurs des fournisseurs ont été évalués conformément par le programme CCCS; et (b) Le fournisseur respecte les obligations de sécurité des sous-processeurs et/ou des sous-traitants énoncés dans les exigences pendant toute la durée du contrat.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		logiciel-service qui ont été proposés par le fournisseur. **Remarque :** Les fournisseurs sont avisés que les étapes d'approvisionnement subséquentes peuvent exiger que le fournisseur avise régulièrement le Canada en cas de mise à jour de la liste des fournisseurs tiers.	Si le fournisseur du logiciel-service commercial proposé n'utilise pas de tiers pour effectuer une partie de la chaîne d'approvisionnement susceptible de fournir au Canada le logiciel-service public disponible dans le commerce proposé, il est demandé au fournisseur de l'indiquer leur réponse à cette exigence.
O7	**Gestion des risques de la chaîne d'approvisionnement**	Le fournisseur du logiciel-service public commercial proposé doit mettre en œuvre des mesures de protection afin de réduire les vulnérabilités de la chaîne d'approvisionnement des services de TI et les menaces qui la guettent. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.	Le fournisseur doit démontrer la façon dont le fournisseur du logiciel-service public commercial respecte les exigences, comme le précise le programme d'évaluation de la sécurité de la technologie de l'information du fournisseur du logiciel-service. Pour être jugée conforme, la documentation fournie doit démontrer la conformité du fournisseur à l'une des trois normes suivantes : 1. ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4); ou 2. publication spéciale 800-161 du NIST – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes d'information et organisations du fédéral); ou 3. Catalogue des contrôles de sécurité ITSG-33, sections SA-12 et SA-12(2), où les mesures de sécurité définies et organisées sont documentées dans un plan de gestion des risques de la chaîne d'approvisionnement (GRCA). Le plan de

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
			GRCA doit décrire la démarche du fournisseur du logiciel-service en matière de GRCA et démontrer la façon dont le fournisseur du logiciel-service public commercial proposé réduira et atténuera les risques de la chaîne d'approvisionnement.
O8	**Gestion de l'accès privilégié**	Le fournisseur du logiciel-service public commercial proposé doit fournir des documents de système démontrant la façon dont le logiciel-service est en mesure de répondre aux exigences de sécurité suivantes en matière de gestion de l'accès privilégié : (a) gérer et surveiller l'accès privilégié aux services infonuagiques pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du gouvernement du Canada; (b) restreindre et minimiser l'accès aux services et aux renseignements du Canada seulement aux appareils autorisés et aux utilisateurs finaux ayant explicitement besoin de cet accès; (c) appliquer et vérifier les autorisations d'accès aux services et aux renseignements; (d) restreindre tout l'accès aux interfaces de service qui hébergent des données et des renseignements aux utilisateurs finaux, aux appareils et aux processus (ou services)	Le fournisseur doit démontrer sa conformité en fournissant de la documentation décrivant la capacité du logiciel-service commercial à répondre aux exigences relatives à la sécurité liées aux exigences en matière de gestion de l'accès privilégié : Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou un livre blanc décrivant les politiques, les processus et les procédures utilisés pour gérer la gestion de l'accès privilégié. La justification requise pour la gestion de l'accès privilégié ne peut simplement reprendre l'exigence obligatoire. Le répondant doit présenter des explications et une démonstration et indiquer où se trouvent les documents de référence dans la réponse. Pour ce faire, il doit fournir le titre du document et les numéros de page et de paragraphe et préciser la façon dont le fournisseur du logiciel-service commercial proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		ayant un identifiant, une authentification et une autorisation uniques; (e) mettre en œuvre des politiques relatives aux mots de passe afin de protéger les identifiants contre les attaques en ligne ou hors ligne et de détecter ces attaques en enregistrant et en surveillant des événements tels que : i) l'utilisation réussie des identifiants de connexion, ii) l'utilisation inhabituelle des identifiants de connexion et iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://cyber.gc.ca/fr/node/1842/html/26717); (f) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux (niveau 2 seulement) ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://cyber.gc.ca/fr/node/1842/html/26717); (g) mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux données et aux renseignements du GC; (h) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de	où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		gestion de l'accès des autres rôles opérationnels; (i) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services et aux renseignements; (j) contrôler l'accès aux objets stockés et aux politiques d'autorisation granulaires pour autoriser ou limiter l'accès; (k) utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services et de l'infrastructure du fournisseur; (l) mettre en place un processus automatisé pour effectuer une vérification périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes, au minimum; et (m) révoquer, en cas de cessation d'emploi, les authentificateurs et les justificatifs d'accès associés au personnel de service.	

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O9	**Fédération de l'identité**	**Fédération de l'identité** Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment : (a) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://cyber.gc.ca/fr/node/1842/html/26717); (b) prendre en charge le Security Assertion Markup Language (SAML) 2.0 et OpenID Connect 1.0, où les justificatifs et authentificateurs des utilisateurs finaux pour les services d'infonuagique sont contrôlés uniquement par le Canada; (c) permettre d'associer les identifiants uniques du Canada (p. ex. un numéro d'identification unique du Canada, une adresse de courriel du Canada) aux comptes d'utilisateurs des services d'infonuagique correspondants.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fédération de l'identité. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Fédération de l'identité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O10	**Protection des points d'extrémité**	**Protection des points d'extrémité** Le fournisseur doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés afin de prévenir les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security (CIS) ou d'une norme équivalente approuvée par écrit par le Canada.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection des points d'extrémité. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Protection des points d'extrémité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O11	**Développement sécurisé**	**Développement sécurisé** Le fournisseur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : i) NIST, ii) ISO, iii) ITSG-33, iv) SAFECode ou v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le Canada par écrit.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Développement sécurisé. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Développement sécurisé, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O12	**Gestion à distance du fournisseur**	**Gestion à distance des fournisseurs** Le fournisseur doit gérer et surveiller l'administration à distance du service du fournisseur utilisé pour héberger les services du GC et prendre des mesures raisonnables pour: (a) Mettre en œuvre des mécanismes d'authentification multi-facteurs pour authentifier les utilisateurs d'accès distant, conformément au ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/fr/node/1842/html / 26717); (b) Employer un algorithme cryptographique approuvé par le CSTC pour protéger la confidentialité des sessions d'accès à distance; (c) acheminez tous les accès à distance via des points de contrôle d'accès contrôlés, surveillés et vérifiés; (d) déconnecter ou désactiver rapidement les connexions de gestion à distance ou d'accès à distance non autorisées; (e) Autoriser l'exécution à distance de commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Gestion à distance du fournisseur. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections de la Gestion à distance du fournisseur, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O13	**Fuite d'information**	**Fuite d'information** 1. Le fournisseur doit avoir un processus documenté qui énonce son approche en cas d'incident de fuite d'information. Le processus du fournisseur doit être harmonisé i) aux directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du document ITSG-33, ou ii) à une autre pratique exemplaire du secteur approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information du fournisseur doit comprendre, à tout le moins : (a) un processus d'identification des éléments de données précis utilisés dans la contamination d'un système; (b) un processus visant à isoler et à éradiquer un système contaminé; (c) un processus d'identification des systèmes pouvant avoir été subséquemment contaminés et toute autre mesure prise pour empêcher la propagation de la contamination; (d) une confirmation d'une personne-ressource, de procédures appropriées et d'une entente concernant la communication sécurisée afin d'offrir de l'aide, si possible, aux administrateurs du service à la clientèle. 2. À la demande du Canada, le fournisseur doit fournir un document qui décrit le processus d'intervention en cas de fuite d'information du fournisseur.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fuite d'information. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Fuite d'information, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O14	**Protection Cryotographique**	**Protection cryptographique** Le fournisseur doit fournir au Canada un document décrivant le processus suivi pour répondre à une protection cryptographique de l'information. (a) Configurez toute cryptographie utilisée pour mettre en œuvre des sauvegardes de confidentialité ou d'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (solutions VPN, TLS, modules logiciels, infrastructure à clé publique et jetons d'authentification, le cas échéant), conformément au Centre de la sécurité des communications (CST). - algorithmes cryptographiques, tailles de clés cryptographiques et périodes cryptographiques approuvés; (b) Utilisez des algorithmes cryptographiques, des tailles de clés cryptographiques et des périodes cryptographiques validées par le programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/), et spécifiés dans ITSP.40.111 Algorithmes cryptographiques. pour les informations non classifiées, protégées A et protégées B, ou des versions ultérieures (https://cyber.gc.ca/fr/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111);	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection Cryptographique. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections de la Protection Cryptographique, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
		(c) Assurez-vous que la cryptographie validée FIPS 140 est utilisée lorsque le cryptage est requis, et qu'elle est implémentée, configurée et utilisée dans un module cryptographique, validée par le programme de validation du module cryptographique (https://www.cse-cst.gc.ca/ programme de validation module / crypto-module), dans un mode approuvé ou autorisé, afin de fournir un degré élevé de certitude que le module cryptographique validé FIPS 140-2 fournit les services de sécurité attendus de la manière attendue; et (d) Assurez-vous que tous les modules FIPS 140-2 utilisés possèdent une certification active, à jour et valide. Les produits conformes / validés FIPS 140 auront des numéros de certificat.	

ID de l'exigence obligatoire	Sous-catégorie	Exigence	Obligation de démontrer la conformité au palier 1 (données jusqu'au niveau Protégé A, inclusivement)
O15	**Séparation des données**	Le fournisseur doit, pour les deux pals, mettre en place des contrôles pour assurer l'isolation appropriée des ressources, de sorte que les actifs informationnels ne soient pas mélangés avec les données d'autres locataires, qu'ils soient en cours d'utilisation, de stockage ou de transit, ainsi que dans tous les aspects des fonctionnalités du service fournisseur et de l'infrastructure fournisseur et administration du système. Cela inclut la mise en œuvre de contrôles d'accès et l'application de la séparation logique ou physique appropriée pour prendre en charge: (a) la séparation entre l'administration interne du fournisseur et les ressources utilisées par ses clients; et (b) La séparation des ressources du client dans des environnements multi-locataires afin d'empêcher qu'un consommateur malveillant ou compromis affecte le service ou les données d'un autre.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences.

Les vingt (20) exigences de sécurité suivantes doivent être satisfaites afin de démontrer la conformité à l'assurance du palier 2 **(données jusqu'au niveau Protégé B inclusivement).**

Palier 2 (Renseignements classifiés jusqu'à la catégorie Protégé B inclusivement)

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O1	**Rôles et responsabilités en matière de sécurité**	Le fournisseur doit définir clairement les rôles et les responsabilités en ce qui concerne les contrôles de sécurité et les fonctionnalités des services entre le fournisseur (tout sous-processeur du fournisseur, le cas échéant) et le Canada.	Dans le document, le fournisseur doit inclure, au minimum, les rôles et responsabilités des parties en ce qui concerne: (a) la gestion des comptes; (b) la protection des frontières; (c) la sauvegarde des actifs et du système d'information; (d) la gestion des incidents; (e) la surveillance du système; et (f) la gestion des vulnérabilités.
O2	**Gestion des comptes principaux/racines**	Le fournisseur de logiciels-services commercialement disponible proposé doit pouvoir protéger la confidentialité, l'intégrité et la disponibilité des données des comptes principaux du gouvernement du Canada et des titres de compétences utilisés pour établir l'environnement d'infonuagique du gouvernement du Canada. Cela comprend l'assurance que les justificatifs d'identité restent à l'intérieur des frontières géographiques du Canada.	Le fournisseur doit démontrer sa conformité en fournissant de la documentation qui décrit la capacité du logiciel-service commercialement disponible de protéger la confidentialité, l'intégrité et la disponibilité de l'information et des justificatifs d'identité du compte principal du gouvernement du Canada (GC) utilisés pour établir l'environnement infonuagique du GC. Pour être jugés conformes, les documents doivent comporter les éléments suivants : (a) Documentation du système ou livre blanc décrivant les politiques, les processus et les procédures utilisés pour protéger la confidentialité, l'intégrité et la disponibilité de l'information et des justificatifs d'identité du

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
			compte principal du GC utilisés pour établir l'environnement infonuagique du GC. Pour les exigences, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer où trouver le matériel de référence dans la réponse, y compris le titre du document, ainsi que les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O3	**Isolation de la protection des données**	Les services proposés doivent permettre au GC d'isoler les données au Canada dans un centre de données approuvé. Aux fins de la présente demande de soumissions, un centre de données approuvé est défini comme suit : (a) un centre de données situé physiquement au Canada; (b) un centre de données qui répond à toutes les exigences de sécurité et certifications	Le fournisseur doit fournir une documentation qui démontre comment le fournisseur des services proposés se conforme aux exigences énoncées à la rubrique Exigences relatives aux installations des centres de données. Pour être jugés conformes, les documents doivent comporter les éléments suivants : (a) une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection des installations de TI et des actifs du

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		énoncées dans les exigences relatives aux installations des centres de données. Exigences relatives aux installations des centres de données: Le fournisseur du logiciel-service commercialement disponible proposé doit veiller à mettre en œuvre des mesures de sécurité qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les données du Canada sont stockées et traitées contre toute forme de manipulation, de perte, de dommages et de saisie, en fonction d'une approche de sécurité physique axée sur la prévention, la détection, l'intervention et la reprise. Des mesures de protection physiques doivent être appliquées conformément aux mesures de contrôle de la protection physique et environnementale (PE), de la maintenance (MA) et de la protection des supports (PS) décrits dans les contrôles de sécurité décrits dans ITSG-33 Profil de contrôle de sécurité du gouvernement du Canada pour les services de TI du GC en nuage pour « PBMM » et aux pratiques décrites dans les lignes directrices et normes en matière de sécurité physique de la Gendarmerie royale du Canada (GRC). Cela comprend au minimum : (a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'un centre de données n'empêche	système d'information dans lesquels les données du GC sont stockées et traitées contre toute forme de manipulation, de perte, de dommages et de saisie, en fonction d'une approche de sécurité physique axée sur la prévention, la détection, l'intervention et la reprise. Pour les exigences relatives aux installations des centres de données, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le logiciel-service commercialement disponible satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer où trouver le matériel de référence dans la réponse, y compris le titre du document, ainsi que les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		pas la récupération des données conformément à l'ENS prescrite; (b) l'utilisation adéquate des supports de TI; (c) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; (d) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada; (e) la restriction de l'accès physique aux actifs des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, validé par deux formes d'identification; (f) l'escorte des visiteurs et la surveillance de leurs activités; (g) la tenue de registres de vérification de l'accès physique; (h) le contrôle et la gestion des dispositifs d'accès physique; (i) l'application de mesures de protection des données du Canada à d'autres lieux de travail (p. ex., les sites de télétravail); (j) la consignation et la surveillance de tous les accès physiques aux installations des centres de données et de tous les accès par voie électronique aux composants des systèmes d'information qui hébergent les	

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.	
O4	**Séparation des données**	Le fournisseur doit, pour les deux tiers, mettre en place des contrôles pour assurer l'isolation appropriée des ressources, de sorte que les actifs informationnels ne soient pas mélangés avec les données d'autres locataires, qu'ils soient en cours d'utilisation, de stockage ou de transit, ainsi que dans tous les aspects des fonctionnalités du service fournisseur et de l'infrastructure fournisseur. et administration du système. Cela inclut la mise en œuvre de contrôles d'accès et l'application de la séparation logique ou physique appropriée pour prendre en charge: (a) la séparation entre l'administration interne du fournisseur et les ressources utilisées par ses clients; et (b) La séparation des ressources du client dans des environnements multi-locataires afin d'empêcher qu'un consommateur malveillant ou compromis affecte le service ou les données d'un autre.	Le fournisseur doit fournir une documentation démontrant que le fournisseur des services proposés se conforme aux exigences.
O5	**Protection des données**	Le fournisseur du logiciel-service commercialement disponible proposé doit permettre au GC de stocker et de protéger ses renseignements inactifs, y compris les données de sauvegarde ou les données tenues à des fins	Le fournisseur doit, pour démontrer sa conformité, fournir des documents illustrant la capacité du logiciel-service commercialement disponible proposé d'isoler les données au Canada dans un centre de données approuvé.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		de redondance, à l'intérieur des frontières géographiques du Canada. Cela comprend les éléments suivants : (a) dresser et fournir au GC une liste à jour des lieux physiques, y compris la ville où pourraient se trouver des données du Canada, au Canada, pour chaque centre de données utilisé pour fournir des services; (b) indiquer les parties des services fournis à partir de l'extérieur du Canada, y compris tous les lieux où les données sont stockées et traitées et où les services sont gérés; (c) garantir l'impossibilité de trouver les données d'un client précis sur les supports physiques; (d) utiliser le cryptage pour veiller à ce qu'aucune donnée ne soit inscrite sur le disque de manière non cryptée. **Remarque à l'attention des fournisseurs :** Les fournisseurs sont informés que les étapes d'approvisionnement subséquentes peuvent les obliger ou obliger le fournisseur du logiciel-service commercialement disponible proposé à informer le Canada de toute mise à jour de la liste des lieux physiques où pourraient se trouver des données du Canada	Pour être jugés conformes, les documents doivent comporter les éléments suivants : (a) des captures d'écran du centre de données disponibles dans lesquelles les centres de données canadiens figurent sur la liste de la disponibilité; (b) une liste ou une carte indiquant l'emplacement géographique des centres de données au Canada. Pour ce critère, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le logiciel sous forme de service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O6	**Installations des centres de données**	Le fournisseur du logiciel-service commercialement disponible proposé doit veiller à mettre en œuvre des mesures de sécurité qui assurent la protection des installations de TI et des actifs du système d'information dans lesquels les données du GC sont stockées et traitées contre toute forme de manipulation, de perte, de dommages et de saisie, en fonction d'une approche de sécurité physique axée sur la prévention, la détection, l'intervention et la reprise. Les mesures de protection physique doivent être appliquées en conformité avec, ou utiliser une approche adéquate, basée sur les risques et alignée sur les conditions physiques, alignées sur les contrôles de sécurité physique et les pratiques du Conseil du Trésor sur la sécurité physique (http: //www.tbs- sct.gc.ca/pol/doc-fra.aspx?id=12329). Les mesures de sécurité requises à cet égard comprennent, au minimum; (a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont notamment suffisamment disparates sur le plan géographique pour que la perte d'un centre de données n'empêche pas la récupération des données conformément à l'ENS prescrite; (b) l'utilisation adéquate des supports de TI; (c) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue; (d) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher	Le fournisseur doit fournir une documentation qui démontre comment le fournisseur des services proposés se conforme aux exigences énoncées à la rubrique Exigences relatives aux installations des centres de données. Pour être jugés conformes, les documents doivent comporter les éléments suivants : (a) une documentation du système ou une documentation technique qui décrit les mesures de sécurité, y compris les politiques, les processus et les procédures mis en œuvre pour assurer la protection des installations de TI et des actifs du système d'information dans lesquels les données du Canada sont stockées et traitées contre toute forme de manipulation, de perte, de dommages et de saisie, en fonction d'une approche de sécurité physique axée sur la prévention, la détection, l'intervention et la reprise. Pour les exigences relatives aux installations des centres de données, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le logiciel sous forme de service commercialement disponible satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		l'accès non autorisé aux données du Canada; (e) la restriction de l'accès physique aux actifs des systèmes d'information aux employés autorisés et aux entrepreneurs en fonction du poste ou du rôle et du principe du besoin de savoir, validé par deux formes d'identification; (f) l'escorte des visiteurs et la surveillance de leurs activités; (g) la tenue de registres de vérification de l'accès physique; (h) le contrôle et la gestion des dispositifs d'accès physique; (i) l'application de mesures de protection des données du GC à d'autres lieux de travail (p. ex., les sites de télétravail); (j) la consignation et la surveillance de tous les accès physiques aux installations des centres de données et de tous les accès par voie électronique aux composants des systèmes d'information qui hébergent les données du Canada, au moyen d'une combinaison de registres d'accès et de mécanismes de vidéosurveillance dans toutes les zones sensibles et de détection des intrusions.	trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.
O7	**Sécurité du personnel**	Le fournisseur du logiciel-service commercialement disponible proposé doit mettre en place des mesures de sécurité qui accordent et maintiennent le niveau de filtrage de sécurité requis pour le personnel du fournisseur de	Le fournisseur doit fournir une documentation qui démontre comment le fournisseur des services proposés se conforme aux exigences énoncées à la rubrique Exigences de sécurité du personnel.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		services d'infonuagique et du sous-traitant en fonction de leurs privilèges d'accès aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Les mesures en matière de filtrage de sécurité doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou utiliser un équivalent acceptable convenu par le Canada. Cela comprend au minimum : (a) une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du Canada ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services; (b) le processus visant à s'assurer que les employés et les entrepreneurs connaissent, comprennent et respectent leurs responsabilités en matière de sécurité de l'information et que le rôle que l'on compte leur confier leur convient; (c) le processus relatif à la sensibilisation et à la formation en matière de sécurité données à l'arrivée des employés et lorsque les rôles des employés et sous-traitants changent; (d) le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi; (e) l'approche de détection des initiés malveillants potentiels et les contrôles mis en œuvre pour atténuer le risque d'accès aux	Pour être jugés conformes, les documents doivent comporter les éléments suivants : (a) la documentation du système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, les processus et les procédures qui sont utilisés pour accorder et maintenir le niveau requis de vérification de sécurité pour le fournisseur et le personnel des sous-traitants conformément à leurs privilèges d'accès aux biens du système d'information dans lesquels les données du Canada sont stockées et traitées. Pour les exigences de sécurité du personnel, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer où trouver le matériel de référence dans la réponse, y compris le titre du document, ainsi que les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		données du GC ou de dommage à la fiabilité des services d'infonuagique hébergeant les actifs et données du GC.	
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 oeuvre 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 au moyen du processus d'évaluation de la sécurité des technologies de l'information (TI) du fournisseur de services infonuagiques (CSP) du Centre canadien pour la cybersécurité (CCCS) (ITSM.50.100) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux). Tout fournisseur qui a participé au processus doit fournir de la documentation confirmant qu'il a	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 2. 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 3. 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;

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		terminé le processus d'intégration avec (i) une copie du plus récent rapport d'évaluation rempli fourni par le CCCS; et (ii) une copie du rapport sommaire le plus récent fourni par le CCCS. Cela accélérera le processus de qualification et, en même temps, n'oblige pas le fournisseur à démontrer la conformité. Pour les fournisseurs qui ont déjà complété l'évaluation en sécurité en fournissant au CCC les rapports de certification de sécurité SOC 2 Type II et qui ont déjà conclu une entente de non divulgation (END) avec le CCC doivent transmettre leur certification et leurs rapports de certification directement au CCC à contact@cyber.gc.ca afin de se conformer à cette exigence. Pour les fournisseurs qui n'ont pas complété l'évaluation en sécurité, le processus d'intégration commencera une fois que la soumission respectera les exigences de la demande d'arrangement en matière d'approvisionnement et satisfera à tous les critères d'évaluation techniques et financiers obligatoires et fournira tous les éléments obligatoires de certifications pour être déclarée recevable. SPAC référera ensuite le fournisseur aux services clients de CCC pour commencer le processus d'intégration de l'évaluation en TI et pour conclure une END en vue de recevoir une copie du formulaire de soumission d'intégration, ainsi que toute	(b) indiquer la raison sociale légale du fournisseur du logiciel-service commercialement disponible proposé et du fournisseur de services d'informatique en nuage; (c) indiquer la date ou l'état de la certification actuelle; (d) donner la liste des actifs, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification; (e) 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 (f) 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

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		information supplémentaire exigée aux termes de cette exigence.	la conformité au Profil des mesures de sécurité pour les services de la TI du GC fondés 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.
O9	**Programme d'évaluation de la sécurité des TI**	Le fournisseur doit démontrer qu'il se conforme aux exigences de sécurité choisies dans le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) pour la portée des services fournis par le fournisseur dans le cadre du Programme d'évaluation de la sécurité des TI.	Le fournisseur doit démontrer la conformité aux exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité du GC pour les services infonuagiques de TI du GC disponibles (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) pour la portée des Services fournis par le fournisseur dans le cadre du Programme d'évaluation de la sécurité des TI en vertu de la section 4 intitulée « Programme d'évaluation de la sécurité informatique du fournisseur de services en nuage» de l'annexe B - Obligations en matière de sécurité et protection de la vie privée. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications applicables de l'industrie indiquées ci-dessous, et validée au moyen d'évaluations par des tiers indépendants. La cartographie des contrôles de sécurité doit être incluse;

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
			Profil de contrôle de sécurité du GC pour les services de TI du GC en nuage et Certification de l'industrie dans le cadre d'une assurance par un tiers détaillée au palier 2 O8.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O10	**Gestion de la chaîne d'approvisionnement**	Le fournisseur doit fournir une liste de fournisseurs tiers contenant des renseignements sur tout tiers (p. ex. filiales, sous-traitants, etc.) qui fournirait au Canada le logiciel sous forme de service commercialement disponible. Pour les besoins de cette exigence, une entreprise qui fournit des biens au fournisseur du logiciel-service commercialement disponible proposé, mais qui n'effectue pas une partie de la chaîne d'approvisionnement qui pourrait fournir au Canada le logiciel sous forme de service commercialement disponible proposé, n'est pas considérée comme un tiers. Les exemples de tiers comprennent, par exemple, les techniciens qui pourraient être déployés ou entretenir le logiciel sous forme de service commercialement disponible proposé par le fournisseur dans les exigences générales. **Remarque** : Les fournisseurs sont informés que les étapes d'approvisionnement subséquentes peuvent exiger que le fournisseur avise périodiquement le Canada en cas de mise à jour de la liste des fournisseurs tiers.	Le fournisseur doit fournir des documents qui présentent des renseignements sur tous les tiers auxquels on pourrait faire appel pour effectuer une partie quelconque de la chaîne d'approvisionnement en mesure de fournir au Canada un logiciel sous forme de service commercialement disponible proposé, qu'il s'agisse : (a) des sous-traitants du fournisseur; (b) des sous-traitants de sous-traitants du fournisseur en aval de la chaîne; (c) toute filiale. Le fournisseur doit remplir le formulaire 6 - Modèle de soumission SCI tel que fourni dans la présente DAMA. Si le fournisseur ne fait pas appel à des tiers pour effectuer une partie de la chaîne d'approvisionnement susceptible de fournir au Canada le logiciel-service proposé disponible dans le commerce proposé, il est demandé au fournisseur de l'indiquer dans sa réponse à cette exigence. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O11	**Gestion des risques de la chaîne d'approvisionnement**	Le fournisseur du logiciel-service commercialement disponible proposé doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les services. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.	Le fournisseur doit démontrer en quoi le fournisseur du logiciel disponible dans le commerce proposé en tant que service est conforme aux exigences des exigences de gestion des risques de la chaîne logistique décrites dans le programme d'évaluation de la sécurité des technologies de l'information des fournisseurs. Pour être considérée comme conforme, la documentation fournie doit démontrer que l'approche de gestion des risques de la chaîne d'approvisionnement utilisée dans le commerce comme logiciel disponible dans le commerce s'aligne sur l'une des meilleures pratiques suivantes. 1. ISO / CEI 27036 Technologies de l'information - Techniques de sécurité - Sécurité de l'information pour les relations avec les fournisseurs (parties 1 à 4); ou 2. Publication spéciale NIST 800-161 - Pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes et organisations d'information fédéraux; ou 3. Contrôle de sécurité ITSG-33 pour SA-12 et SA-12 (2) lorsque les garanties de sécurité définies sont documentées dans un plan de gestion des risques liés à la chaîne logistique. Le plan de SCRM doit décrire l'approche du fournisseur en matière de SCRM et indiquer comment les fournisseurs du logiciel-service proposé dans le commerce proposé réduiront et atténueront les risques inhérents à la chaîne d'approvisionnement. Le plan SCRM doit être évalué et validé de manière indépendante par un tiers indépendant certifié selon le régime de certification AICPA ou CPA Canada et / ou ISO.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
			Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O12	**Confidentialité**	Le fournisseur de logiciels-services commercialement disponible proposé doit démontrer qu'il est conforme aux règles, procédures et dispositions relatives à la confidentialité, qui répondent aux exigences de la certification de l'industrie suivante: (a) ISO / IEC 27018: 2014 Technologies de l'information - Techniques de sécurité - Code de pratique pour la protection des informations personnelles identifiables (PII) dans les nuages publics agissant en tant que processeurs PII. Remarque: les fournisseurs sont informés que les phases d'approvisionnement ultérieures peuvent obliger le fournisseur à confirmer régulièrement au Canada de logiciels-services commercialement disponible répond à la certification ci-dessus et que cette certification est valide pour toute la durée du véhicule d'approvisionnement.	Pour démontrer la conformité à la certification, le fournisseur doit fournir: (a) Une copie des documents de certification de logiciels-services commercialement disponible les plus récents, ainsi que des documents de certification ISO 27018, qui doivent avoir été délivrés au plus tard 12 mois avant la date de clôture de la soumission; et (b) Une copie du rapport d'évaluation ISO 27018 de logiciels-services commercialement disponible et de services et de services cloud. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O13	**Confidentialité par conception**	Le fournisseur doit démontrer qu'il met en œuvre une confidentialité par conception au cours du cycle de vie du développement de son logiciel, conformément au 'développement sécurisé', tel qu'énoncé ci-dessous : <u>Développement sécurisé</u> Le fournisseur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : (i) NIST; (ii) ISO 27034; (iii) ITSG-33; (iv) Safecode; (v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS] ou une norme équivalente approuvée par le Canada par écrit). À la demande du Canada, le fournisseur doit fournir un document qui décrit le logiciel documenté de l'entrepreneur, ainsi que l'approche et le processus adoptés relativement au cycle de vie du développement du système.	Le fournisseur doit fournir une documentation démontrant que le fournisseur des services proposés se conforme aux exigences. Les fournisseurs doivent indiquer où trouver le matériel de référence, y compris le titre du document, ainsi que les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O14	**Gestion d'accès privilégié**	Le fournisseur du logiciel-service commercialement disponible proposé doit fournir une documentation de système démontrant comment le logiciel sous forme de service est en mesure de répondre aux exigences de sécurité suivantes en matière de gestion d'accès privilégié : (a) gérer et surveiller l'accès privilégié aux services d'infonuagique pour s'assurer que toutes les interfaces de service dans un environnement à locataires multiples sont protégées contre tout accès non autorisé, y compris celles qui sont utilisées pour héberger les services du GC; (b) restreindre et réduire au minimum l'accès aux services et aux actifs d'information du Canada aux seuls dispositifs autorisés et aux utilisateurs finaux ayant un besoin explicite d'y avoir accès; (c) exécuter et vérifier les autorisations d'accès aux services et aux actifs d'information; (d) limiter tous les accès aux interfaces de service qui hébergent les actifs et les actifs d'information aux utilisateurs finaux, dispositifs et processus (ou services) désignés, authentifiés et autorisés de façon unique; (e) mettre en œuvre des politiques relatives aux mots de passe afin de protéger les justificatifs d'identité contre les attaques en ligne ou hors ligne et de détecter ces	Le fournisseur doit démontrer sa conformité en fournissant de la documentation qui décrit la capacité du logiciel-service commercialement disponible de répondre aux exigences de sécurité liées aux exigences en matière de gestion de l'accès privilégié : Pour être jugés conformes, les documents doivent comporter les éléments suivants : (a) une documentation du système ou un livre blanc décrivant les politiques, les processus et les procédures utilisés pour prendre en charge la gestion de l'accès privilégié. Pour la gestion de l'accès privilégié, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercialement disponible proposé satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		attaques en enregistrant et en surveillant des événements tels que (i) l'utilisation réussie des justificatifs d'identité, (ii) l'utilisation inhabituelle de ces justificatifs et (iii) l'accès et l'exfiltration de la base de données des mots de passe, conformément au document ITSP.30.031 V2 (ou versions ultérieures) (https://www.cse-cst.gc.ca/fr/node/1842/html/26717) du CST; (f) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier (palier 2 seulement) les utilisateurs finaux ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou versions ultérieures) du CST (https://www.cse-cst.gc.ca/fr/node/1842/html/26717); (g) mettre en place des contrôles de l'accès fondés sur le rôle qui forment la base de l'accès aux actifs et aux actifs d'information; (h) définir et mettre en œuvre la séparation des tâches pour, au minimum, séparer les rôles de gestion des services et d'administration des rôles de soutien du système d'information, les rôles de développement des rôles opérationnels et les rôles de gestion de l'accès des autres rôles opérationnels; (i) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services et actifs et aux actifs d'information;	

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		(j) mettre en place des contrôles d'accès aux objets stockés et des politiques d'autorisation granulaires pour autoriser ou limiter l'accès; (k) utiliser des points terminaux à sécurité élevée (ordinateurs, appareils d'utilisateurs finaux, serveurs intermédiaires, etc.) qui sont configurés de façon à offrir seulement des fonctions minimales (par exemple un point terminal dédié qui ne peut pas être utilisé pour naviguer sur Internet ou consulter ses courriels) pour offrir le soutien et l'administration des services et de l'infrastructure; (l) mettre en place un processus automatisé pour effectuer une vérification périodique de la création, de la modification, de l'activation, de la désactivation et de la suppression de comptes; et (m) révoquer, en cas de cessation d'emploi, les authentifiants et les justificatifs d'accès associés au personnel chargé des services.	

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O15	**Fédération de l'identité**	**Fédération de l'identité** Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment : (a) mettre en œuvre des mécanismes d'authentification multifactorielle pour authentifier les utilisateurs finaux ayant un accès privilégié, conformément au document ITSP.30.031 V2 (ou une version subséquente) du CST (https://cyber.gc.ca/fr/node/1842/html/26717); (b) prendre en charge le Security Assertion Markup Language (SAML) 2.0 et OpenID Connect 1.0, où les justificatifs et authentificateurs des utilisateurs finaux pour les services d'infonuagique sont contrôlés uniquement par le Canada; (c) permettre d'associer les identifiants uniques du Canada (p. ex. un numéro d'identification unique du Canada, une adresse de courriel du Canada) aux comptes d'utilisateurs des services d'infonuagique correspondants.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fédération de l'identité. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Fédération de l'identité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O16	**Protection des points d'extrémité**	**Protection des points d'extrémité** Le fournisseur doit mettre en œuvre, gérer et surveiller les points d'accès sécurisés afin de prévenir les attaques et les abus conformément aux lignes directrices de configuration reconnues par l'industrie, comme celles du document NIST 800-123 (Guide to General Server Security [guide relatif à la sécurité générale des serveurs]), des points de référence du Center for Internet Security (CIS) ou d'une norme équivalente approuvée par écrit par le Canada.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection des points d'extrémité. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Protection des points d'extrémité, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O17	**Développement sécurisé**	**Développement sécurisé** Le fournisseur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode ou (v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS]) ou une norme équivalente approuvée par le Canada par écrit.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Développement sécurisé. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Développement sécurisé, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O18	**Gestion à distance du fournisseur**	**Gestion à distance des fournisseurs** Le fournisseur doit gérer et surveiller l'administration à distance du service du fournisseur utilisé pour héberger les services du GC et prendre des mesures raisonnables pour: (a) Mettre en œuvre des mécanismes d'authentification multi-facteurs pour authentifier les utilisateurs d'accès distant, conformément au ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/fr/node/1842/html / 26717); (b) Employer un algorithme cryptographique approuvé par le CSTC pour protéger la confidentialité des sessions d'accès à distance; (c) acheminez tous les accès à distance via des points de contrôle d'accès contrôlés, surveillés et vérifiés; (d) déconnecter ou désactiver rapidement les connexions de gestion à distance ou d'accès à distance non autorisées; (e) Autoriser l'exécution à distance de commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Gestion à distance du fournisseur. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections de la Gestion à distance du fournisseur, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O19	**Fuite d'information**	**Fuite d'information** (1) Le fournisseur doit avoir un processus documenté qui énonce son approche en cas d'incident de fuite d'information. Le processus du fournisseur doit être harmonisé i) aux directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du document ITSG-33, ou ii) à une autre pratique exemplaire du secteur approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information du fournisseur doit comprendre, à tout le moins : (a) un processus d'identification des éléments de données précis utilisés dans la contamination d'un système; (b) un processus visant à isoler et à éradiquer un système contaminé; (c) un processus d'identification des systèmes pouvant avoir été subséquemment contaminés et toute autre mesure prise pour empêcher la propagation de la contamination; (d) une confirmation d'une personne-ressource, de procédures appropriées et d'une entente concernant la communication sécurisée afin d'offrir de l'aide, si possible, aux administrateurs du service à la clientèle. (2) À la demande du Canada, le fournisseur doit fournir un document qui décrit le processus d'intervention en cas de fuite d'information du fournisseur.	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fuite d'information. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections Fuite d'information, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O20	**Protection Cryotographique**	**Protection cryptographique** Le fournisseur doit fournir au Canada un document décrivant le processus suivi pour répondre à une protection cryptographique de l'information. (a) Configurez toute cryptographie utilisée pour mettre en œuvre des sauvegardes de confidentialité ou d'intégrité, ou utilisée dans le cadre d'un mécanisme d'authentification (solutions VPN, TLS, modules logiciels, infrastructure à clé publique et jetons d'authentification, le cas échéant), conformément au Centre de la sécurité des communications (CST). - algorithmes cryptographiques, tailles de clés cryptographiques et périodes cryptographiques approuvés; (b) Utilisez des algorithmes cryptographiques, des tailles de clés cryptographiques et des périodes cryptographiques validées par le programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/), et spécifiés dans ITSP.40.111 Algorithmes cryptographiques. pour les informations non classifiées, protégées A et protégées B, ou des versions ultérieures (https://cyber.gc.ca/fr/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); (c) Assurez-vous que la cryptographie validée FIPS 140 est utilisée lorsque le cryptage est requis, et qu'elle est implémentée, configurée et utilisée dans un module cryptographique, validée par le programme de validation du module cryptographique (https://www.cse-cst.gc.ca/	Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection Cryptographique. Pour être jugée conforme, la documentation fournie doit inclure : (a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité. Pour les sections de la Protection Cryptographique, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur du logiciel-service commercial satisfait à l'exigence. Le fournisseur peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Le fournisseur doit indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe. Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du fournisseur sera jugée non conforme. Dans sa justification, le fournisseur peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer l'endroit dans la réponse où se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		programme de validation module / crypto-module), dans un mode approuvé ou autorisé, afin de fournir un degré élevé de certitude que le module cryptographique validé FIPS 140-2 fournit les services de sécurité attendus de la manière attendue; et (d) Assurez-vous que tous les modules FIPS 140-2 utilisés possèdent une certification active, à jour et valide. Les produits conformes / validés FIPS 140 auront des numéros de certificat	

ANNEXE B – ONBLIAGATIONS EN MATIÈERE DE SÉCURITÉ ET PROTECTION DE LA VIE PRIVÉE

Généralités

Objet

La présente annexe a pour objet d'énoncer les obligations du fournisseur en ce qui concerne la configuration et la gestion appropriées des actifs et des actifs informationnels, afin de protéger ces actifs et ces actifs contre toute modification, accès ou exfiltration non autorisés, le tout conformément à l'AMA, la présente annexe, les mesures de sécurité spécifiques du fournisseur et les politiques canadiennes en matière de sécurité et de confidentialité (collectivement appelées «obligations de sécurité et de confidentialité»).

Exécution des obligations en matière de protection de la vie privée

Les obligations du fournisseur contenues dans les présentes obligations de sécurité et confidentialité doivent être transférées par le fournisseur aux sous-processeurs du fournisseur, dans la mesure où elles s'appliquent à chaque sous-processeur du fournisseur, étant donné la nature des services fournis au fournisseur.

Gestion du changement

Le fournisseur doit, pendant toute la durée de l'AMA, prendre toutes les mesures nécessaires pour mettre à jour et maintenir à jour les obligations en matière de sécurité et de confidentialité afin de se conformer aux pratiques de sécurité des normes de l'industrie.

Le fournisseur doit accepter d'informer le Canada de toutes les améliorations qui pourraient avoir une incidence sur les services dans le contrat, y compris les améliorations techniques, administratives ou tout autre type d'améliorations. Le fournisseur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans supplément pour le Canada.

1. Reconnaissance

Les parties reconnaissent que:

(a) Tous les biens et les actifs informationnels sont assujettis à ces obligations en matière de sécurité et de confidentialité.

(b) Nonobstant toute autre disposition de la présente annexe, les parties partagent la responsabilité d'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux biens et aux actifs informationnels.

(c) Le fournisseur ne doit pas avoir ou tenter d'obtenir la garde d'un actif d'information, ni permettre à un membre du personnel des services à accéder à un actif information avant la mise en œuvre des obligations de sécurité et de confidentialité requises, comme l'exige la présente annexe, au plus tard à l'attribution du marché.

(d) Les obligations de sécurité s'appliquent au Palier 1 (jusqu'à la protection A / blessures faibles) et au Palier 2 (jusqu'à la protection B / blessures moyennes), sauf indication contraire.

2. Sécurisation des actifs informatiques

Les solutions logiciels-services du fournisseur doivent être conçues de manière à protéger les actifs et les actifs informatiques contre tout accès, modification ou exfiltration non autorisés. Cela inclut **la mise en œuvre et la maintenance de stratégies, procédures et contrôles de sécurité des informations appropriés pour** préserver la confidentialité, l'intégrité et la disponibilité des actifs et des actifs informatiques (ci-après dénommés les «mesures de sécurité spécifiques»).

3. Rôles et responsabilités en matière de sécurité

Le fournisseur doit fournir au Canada un document à jour qui définit les rôles et les responsabilités du fournisseur, des sous-traitants du fournisseur et du Canada en matière de contrôles et de caractéristiques de sécurité : (i) sur une base annuelle; (ii) lorsqu'il y a des changements importants à ces rôles et responsabilités à la suite d'un changement aux services; ou (iii) à la demande du Canada.

4. Programme d'évaluation de la sécurité informatique du fournisseur de services en nuage

À la demande du Canada, le fournisseur ou un sous-traitant peut fournir des preuves supplémentaires, y compris des plans de sécurité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système, afin d'achever les rapports de certification et de vérification décrits à la section 5 (audit sur la conformité aux obligations en matière de la sécurité) et de démontrer la conformité du fournisseur avec les certifications requises de l'industrie.

5. Vérification de la conformité aux obligations de sécurité

Le fournisseur doit effectuer les vérifications de confidentialité et de sécurité, de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter et protéger les données du Canada comme suit :

(a) conformément aux certifications obligatoires de l'ISO, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par année;

(b) chaque vérification sera effectuée conformément aux normes et aux règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable;

(c) chaque vérification sera effectuée par un vérificateur tiers indépendant qui (i) est qualifié selon l'AICPA, CPA Canada ou le régime de certification ISO, et (ii) se conforme à la norme ISO/IEC 17020 sur les systèmes de gestion de la qualité, selon le choix et aux frais du fournisseur;

(d) chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être mis à la disposition du Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le vérificateur externe. L'entrepreneur doit, à ses frais, corriger rapidement et à la satisfaction du vérificateur les problèmes et les lacunes soulevés dans tout rapport de vérification.

À la demande du Canada, le fournisseur ou un sous-traitant peut fournir des preuves supplémentaires, y compris des plans de sécurité du système, des conceptions ou des documents d'architecture qui fournissent une description complète du système, afin d'achever les rapports de certification et de vérification décrits à la section 5 (Assurance d'une tierce partie) et de démontrer la conformité de l'entrepreneur avec les certifications requises de l'industrie.

6. Interface de programmation d'application (API)

Le fournisseur (Palier 1 et 2) doit:

(a) Fournir des services qui utilisent des interfaces de programmation d'applications (API) ouvertes, publiées, prises en charge et documentées, afin de prendre en charge l'interopérabilité entre les composants et de faciliter la migration des applications.

(b) Prendre des mesures raisonnables pour protéger les API internes et externes au moyen de méthodes d'authentification sécurisées. Cela implique de s'assurer que toutes les requêtes d'API exposées en externe nécessitent une authentification réussie avant de pouvoir être appelées.

Pour la solution logiciel-service, le fournisseur doit fournir des API qui permettent:

(a) d'interroger des données inactives dans des applications de la solution logiciel-service; et

(b) d'évaluer les événements et les incidents stockés dans les journaux d'applications de la solution logiciel-service.

7. Sécurité des réseaux et des communications

Le fournisseur doit :

(a) permettre au Canada d'établir des connexions sécurisées aux Services, notamment en assurant la protection des données en transit entre le Canada et le Service au moyen de TLS 1.2 ou de versions ultérieures;

(b) utiliser des protocoles ainsi que des algorithmes et des certificats cryptographiques pris en charge et à jour, comme le décrivent les normes ITSP.40.062 (https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) et ITSP.40.111 (https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b) du CST;

(c) utiliser des certificats correctement configurés dans les connexions TLS, conformément aux directives du CST;

(d) permettre au Canada de mettre en œuvre des contrôles d'accès au réseau et des règles de sécurité qui permettent ou refusent le trafic réseau vers les ressources canadiennes.

8. Gestion des clés

Pour le Palier 2, le fournisseur doit posséder la capacité de fournir au Canada un service de gestion de clés qui permet :

(a) la création/génération et la suppression des clés utilisées pour livrer la Solution SaaS de cryptage par le GC;

(b) la définition et l'application de politiques propres au gouvernement du Canada qui contrôlent la façon dont les clés peuvent être utilisées;

(c) la protection de l'accès au matériel clé, y compris la prévention de l'accès du fournisseur au matériel clé de façon non chiffrée; et

(d) la vérification de tous les événements liés aux principaux services de gestion, y compris l'accès des fournisseurs aux fins d'examen par le Canada.

9. Connexions dédiées

Pour le Palier 2, l'entrepreneur doit permettre au GC d'établir une connectivité privée redondante aux services. Cela comprend :

(a) la prise en charge de la virtualisation et de locataires multiples pour tous les composants réseau;

(b) la prise en charge de protocoles de routage dynamiques (Border Gateway Protocol) pour toutes les connexions;

(c) la prise en charge de protocoles approuvés par le GC, qui sont décrits dans les documents suivants :

(i) Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062), Section 3.1 (suites de chiffrement AES)

(ii) Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)

(d) Fournir une description des emplacements géographiques de tous les centres de données au Canada où cette capacité est offerte.

10. Journalisation et vérification (PALIER 1 ET 2)

(a) Le fournisseur doit mettre en œuvre des pratiques et des contrôles de production et de gestion de journaux pour toutes les composantes du service qui stockent ou traitent les biens et les actifs d'information, et qui sont conformes aux pratiques des principaux fournisseurs de services, comme celles de NIST 800-92 (Guide to Computer Security Log Management), ou une norme équivalente approuvée par écrit par le Canada.

(b) Le fournisseur doit permettre au Canada d'examiner et d'analyser de manière centralisée les dossiers de vérification de multiples composants des services offerts par le fournisseur. Ceci comprend la capacité pour le Canada :

(i) d'enregistrer et de détecter les événements de vérification tels qu'un minimum (i) de tentatives de connexion réussies ou non, (ii) de gestion des comptes, (iii) d'accès aux objets et changement de politique, (iv) de fonctions de privilèges et de suivi des processus, (v) d'événements système, (vi) de suppression des données;

(ii) d'enregistrer dans des journaux (ou fichiers journaux) des événements de vérification qui sont synchronisés et horodatés en temps universel coordonné (UTC) et protégés contre l'accès, la modification ou la suppression non autorisé pendant le transport et au repos;

(iii) des incidents de sécurité et des journaux de bord distincts pour les différents comptes du Canada afin de permettre au Canada de surveiller et de gérer les événements à l'intérieur de ses frontières qui ont une incidence sur l'instance d'un service IaaS, PaaS ou SaaS qui lui est fourni par le fournisseur ou un sous-traitant du fournisseur; et

(iv) de transmettre les événements et journaux des locataires du Canada vers un système centralisé de journaux de vérification géré par le gouvernement au moyen d'interfaces d'établissement de rapports, de protocoles et de formats de données (Common Event Format [CEF], Syslog et autres formats communs) et d'interface de programmation d'application normalisés qui permettent la récupération à distance des données de journaux (par l'intermédiaire d'une interface de base de données qui utilise SQL, etc.).

11. Gestion des incidents de sécurité (PALIER 1 ET 2)

(a) Le processus d'intervention en cas d'incident de sécurité du fournisseur pour les services doit englober les pratiques du cycle de vie de la gestion des incidents de sécurité informatique et les pratiques d'appui des activités de préparation, de détection, d'analyse, de confinement et de récupération, conformément à l'une des normes suivantes : (i) ISO/IEC 27035:2011 Technologies de l'information -- Techniques de sécurité -- Management des incidents liés à la sécurité de l'information; ou (ii) NIST SP800-612, Computer Security Incident Handling Guide; ou (iii) Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) [https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html]; ou (iv) autres pratiques exemplaires des principaux fournisseurs de services si le Canada détermine, à sa discrétion, que celles-ci respectent ses exigences en matière de sécurité.

(b) Le processus d'intervention en cas d'incident de sécurité du fournisseur doit comprendre ce qui suit :

(i) des processus et procédures documentés indiquant comment le fournisseur relèvera les incidents de sécurité, y donnera suite et y remédiera, dressera un rapport à leur sujet et les signalera au Canada, y compris : (i) la portée des incidents de sécurité que le fournisseur doit signaler au Canada; (ii) le degré de divulgation et les mesures utilisées par le fournisseur pour détecter les incidents de sécurité, ainsi que les interventions connexes du fournisseur pour des types précis d'incidents de sécurité; (iii) le délai cible de signalement et de transmission des incidents de sécurité; (iv) la procédure de signalement et d'acheminement en cas d'incidents de sécurité; (v) les coordonnées des personnes-ressources pour le traitement des enjeux relatifs aux incidents de sécurité; (vi) tout recours applicable à certains incidents de sécurité.

(ii) des procédures pour répondre aux demandes de preuve numérique potentielle ou d'autres renseignements provenant de l'environnement de service ou de l'infrastructure du fournisseur, y compris les procédures judiciaires et les mesures de protection pour la tenue d'une chaîne de possession des actifs d'information stockés ou traités par le fournisseur ou un sous-traitant du fournisseur. Les pratiques et les contrôles en matière d'éléments de preuve judiciaires et numériques doivent être conformes aux pratiques des principaux fournisseurs de services, comme celles décrites dans la norme NIST 800-62 (Guide to Integrating Forensic Techniques into Incident Response), la norme ISO 27037 (Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuve numérique), ou une norme équivalente approuvée par écrit par le Canada.

12. Vérification de la conformité POUR LES OBLIGATIONS RELIER LA PROTECTION DE LA VIE PRIVÉ SEULEMENT

(a) Si le Canada doit effectuer des vérifications, inspections de sécurité ou examiner d'autres renseignements (documents, description de la protection de données, architecture de données et descriptions de sécurité), les deux parties conviennent de négocier de bonne foi pour trouver une solution et de tenir compte à la fois de la justification de la demande du Canada et des processus et protocoles de l'entrepreneur.

(b) Dans les 30 jours suivant l'attribution du contrat, l'entrepreneur doit retenir les services d'une tierce partie pour effectuer une vérification de la protection des renseignements personnels ou fournir la preuve qu'il ne produit, ne recueille, n'utilise, ne stocke ni ne communique aucun renseignement personnel supplémentaire tel que défini par le Canada, sauf les données du client telles que définies par l'entrepreneur et ne possède pas spécifiquement de PII dans les données de soutien (recueillies par le truchement des journaux [par exemple, les données télémesure, par le contenu et l'en-tête des messages électroniques]).

(c) Le fournisseur doit effectuer les vérifications de confidentialité et de sécurité de la sécurité des ordinateurs, de l'environnement informatique et des centres de données physiques qu'il utilise pour traiter les données du Canada de la façon suivante :

(i) Lorsqu'une norme ou un cadre prévoit des vérifications, une vérification de cette norme ou de ce cadre de contrôle sera entreprise au moins une fois par année;

(ii) Chaque audit sera effectué conformément aux normes et règles de l'organisme de réglementation ou d'accréditation pour chaque norme ou cadre de contrôle applicable;

(iii) Chaque audit sera effectué par des auditeurs de sécurité qualifiés, indépendants et reliés à une tierce partie qui (i) sont qualifiés selon l'AICPA, CPA Canada ou le régime de certification ISO, et (ii) sont conformes à la norme ISO/CEI 17020 sur les systèmes de gestion de la qualité à la sélection et aux frais du fournisseur.

(d) Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être communiqué au Canada. Le rapport d'audit doit indiquer clairement toutes les constatations importantes faites par l'auditeur. Le fournisseur doit corriger rapidement et à la satisfaction du vérificateur les problèmes soulevés dans tout rapport de vérification et doit (i) fournir au Canada le plan pour corriger toute conclusion négative découlant de ces rapports et (ii) fournir au Canada, sur demande, des rapports d'étape sur la mise en œuvre dans un délai de dix jours ouvrables du gouvernement fédéral.

(e) À la demande du Canada, le fournisseur ou un sous-traitant peut fournir des renseignements additionnels sur le fournisseur, y compris des plans de sécurité, des conceptions ou des documents d'architecture du système qui fournissent une description complète du système, afin de compléter les rapports de certification et de vérification décrits dans la présente et de démontrer la conformité du fournisseur avec les certifications requises de l'industrie.

13. Protection des données et d'information

Les données du Canada, y compris tous les renseignements personnels, ne seront utilisées ou autrement traitées que pour fournir au Canada les services, y compris à des fins compatibles avec la prestation de ces services. Le fournisseur ne doit pas utiliser ou autrement traiter les données du Canada ni en tirer de l'information à des fins publicitaires ou commerciales similaires. Entre les parties, le Canada conserve tous les droits, titres et intérêts relatifs aux données clients. Le fournisseur n'acquiert aucun droit sur les données du client, à l'exception des droits que le client accorde au fournisseur pour fournir les services au client.

14. Respect de la vie privée

(a) Le fournisseur doit démontrer par l'intermédiaire de rapports d'évaluation et de rapports d'audit que:

(i) Restreint la création, la collecte, la réception, la gestion, l'accès, l'utilisation, la conservation, l'envoi, la divulgation et la suppression d'informations personnelles à ceux nécessaires à l'exécution du travail;

(ii) A mis en place des processus et des contrôles de sécurité actualisés tels que des contrôles de gestion des accès, des ressources humaines, de la cryptographie et des sécurités physique, opérationnelle et de communication préservant l'intégrité, la confidentialité et l'exactitude de toutes les informations et données, ainsi que de leurs métadonnées, quel que soit leur format.

(b) Ceci s'applique à toutes les informations, données et métadonnées en la possession du fournisseur ou sous sa responsabilité, acquises en vertu de, ou résultant de toute autre manière hors des responsabilités et obligations du contractant en vertu du contrat. L'entrepreneur reconnaît que cela est nécessaire pour que le Canada puisse s'appuyer sur les informations, les données et les métadonnées et pour qu'il puisse s'acquitter de ses propres obligations légales, y compris des obligations légales (voir l'annexe B). Cela est également nécessaire pour garantir que les informations, les données et les métadonnées peuvent être utilisées comme preuves convaincantes devant un tribunal.

15. Responsable de la confidentialité

Dans les 10 jours suivant l'émission de l'arrangement en matière d'approvisionnement, le fournisseur doit fournir au Canada les informations permettant à un particulier de désigner un agent de la protection de la vie privée, qui agira en tant que représentant de l'entrepreneur pour toutes les questions liées aux renseignements personnels et aux dossiers. Le fournisseur doit fournir le nom et les coordonnées de cette personne, y compris son titre commercial, son adresse électronique et son numéro de téléphone.

ANNEXE C – PRIX PLAFONDS POUR LES SOLUTIONS DE LOGICIELS ET SERVICES PROFESSIONNELLES

Option 1: Les fournisseurs fournissent un lien vers leur catalogue de logiciels-services disponible sur le marché et indiquent le pourcentage de réduction offert au Canada.

Lien vers un site Web :
OU
Option 2: Les fournisseurs complètent le tableau ci-dessous.

TABLEAU 1 – LISTE DE PRODUITS ET PRIX PLAFONDS											
N° d'article	**No de pièce de l'éditeur de la Solution de logiciels-services (A)**	**Nom de la Solution de logiciels-services (B)**	**Nom de l'éditeur de la Solution de logiciels-services (C)**	**Nom du fournisseur de services infonuagique (D)**	**Prix plafonds pour les Solutions de logiciels-services (E)**	**Prix plafonds pour les services professionnels facultatifs (F)**	**Unité de mesure (G)**	**Remise en pourcentage applicable (H)**	**Langue(s) disponible(s) (I)**	**Information sur la Solution de logiciels-services (J)**	**Mots clés/étiquettes (K)**
	(inscrire le numéro de pièce que l'éditeur de la Solution de logiciels-services utilise pour identifier la solution)	(inscrire le nom que l'éditeur de la Solution de logiciels-services utilise pour identifier la solution)	(inscrire le nom de l'éditeur de la Solution de logiciels-services qui produit la solution)	(inscrire le nom du fournisseur de services infonuagiques qui héberge la Solution de logiciels-services)	(inscrire le prix unitaire plafonds de la Solution de logiciels-services en dollars canadiens)	(inscrire le prix plafond pour les services professionnels (taux quotidiens, horaires ou forfaitaires) en dollars canadiens pour chaque catégorie : Guide de démarrage rapide (« GDR »), formation et services, services de mise en œuvre, services de formation, services d'épuration, de migration et de transition de données, et	(inscrire l'unité de mesure pour la Solution de logiciels-services, par exemple « par utilisateur », « par entité », etc., **et** abonnement, durée)	(inscrire le pourcentage de remise qui sera appliqué aux prix unitaires commerciaux plafonds pour la durée de l'AMA)	(inscrire la langue de la Solution de logiciels-services (anglais et/ou français)	(inscrire une adresse de site Web contenant de l'information sur la Solution de logiciels-services)	(inscrire des mots clés associés à la Solution de logiciels-services qui aideront les clients à chercher et trouver facilement les Solutions de logiciels-services qui répondent à leurs besoins

						services consultatifs)					
1											
2											

ANNEXE D – ACCORD SUR LES NIVEAUX DE SERVICES (ANS)

Seules les modalités de l'ANS, décrites en détail à 3.2 Section I : Soumission technique, (c) (v), relatives aux niveaux de service et à la prestation des services feront partie de l'arrangement en matière d'approvisionnement. Les fournisseurs peuvent soumettre leurs ANS sous la forme d'adresses URL. Les fournisseurs peuvent mettre à jour leur ANS sur une base continue, pourvu que les changements ne représentent pas une diminution des niveaux de service fournis. Lorsqu'un fournisseur désire ajouter une Solution de logiciels services à son arrangement en matière d'approvisionnement, les ANS doivent être soumis à nouveau au responsable de l'arrangement en matière d'approvisionnement aux fins d'approbation avant d'être intégrés à l'arrangement en matière d'approvisionnement. Les modalités réputées être intégrées par renvoi à des adresses URL, à des fichiers « Lisez moi » ou par un autre moyen, ne font pas partie de l'arrangement en matière d'approvisionnement à moins d'être inscrites intégralement dans l'Annexe D – Accords sur les niveaux de service (ANS) pour les Solutions de logiciels services.

Aucune modalité n'est censée abréger ou proroger les délais pour introduire une action pour violation, une action pour responsabilité délictuelle ou toute autre action de tout type.

ANNEXE E – MODÈLE DE DEMANDE DE SOUMISSION POUR LOGICIELS SERVICES

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

La présente demande de soumissions est émise dans le cadre de l'arrangement en matière d'approvisionnement de logiciels-services du Gouvernement du Canada dont le numéro de dossier de SPAC est le numéro XXX. Toutes les modalités de l'arrangement s'appliquent et font partie de la demande de soumissions et de tout marché subséquent.

La demande de soumissions contient six parties, ainsi que des pièces jointes et des annexes, et elle est divisée comme suit :

Partie 1 **Renseignements généraux** : renferme une description générale du besoin;

Partie 2 **Instructions à l'intention des soumissionnaires** : renferme les instructions, clauses et conditions relatives à la demande de soumissions;

Partie 3 **Instructions pour la préparation des soumissions** : donne aux soumissionnaires les instructions pour préparer leur soumission;

Partie 4 **Procédures d'évaluation et méthode de sélection** : décrit la façon selon laquelle se déroulera l'évaluation et présente les critères d'évaluation auxquels on doit répondre dans la soumission, ainsi que la méthode de sélection;

Partie 5 **Attestations et renseignements supplémentaires** : comprend les attestations et les renseignements supplémentaires à fournir; et

Partie 6 **Exigences relatives à la sécurité, exigences financières et autres exigences** : comprend des exigences particulières auxquelles les soumissionnaires doivent répondre.

1.2 Sommaire

Inclure les éléments énumérés ci-dessous, selon le cas. Pour des raisons d'uniformité, employer la même formulation pour décrire le besoin dans l'Avis de projet de marché (APM), tel que formulé dans cet article.

1.2.1 Insérer une brève description du besoin. La description devrait comprendre suffisamment d'information pour permettre aux fournisseurs de décider de présenter ou non une soumission suite à la demande de soumissions (par exemple, elle pourrait comprendre une liste des sous-catégories de biens ou de services ainsi que de leurs principales caractéristiques propres).

Inclure l'énoncé suivant si le besoin est assujetti à tous les accords commerciaux énoncés dans la clause, sinon modifier cet article en conséquence.

1.2.2 Ce besoin est assujetti aux dispositions de l'Accord sur les marchés publics de l'Organisation mondiale du commerce (AMP–OMC), de l'Accord de libre-échange nord-américain (ALENA), de l'Accord économique et commercial global entre le Canada et l'Union européenne (AECG) et de l'Accord de libre-échange canadien (ALEC).

Inclure l'énoncé suivant pour les marchés réservés dans le cadre de la Stratégie d'approvisionnement auprès des entreprises autochtones (SAEA).

1.2.3 Ce marché est réservé dans le cadre de la Stratégie d'approvisionnement auprès des entreprises autochtones du gouvernement fédéral.

Inclure l'énoncé suivant pour les besoins formulés au nom d'un ministère ou d'un organisme assujetti au Programme de contrats fédéraux, estimés à 1 000 000 $ et plus, excluant les options, taxes applicables incluses.

1.2.4 Le Programme de contrats fédéraux pour l'équité en matière d'emploi s'applique au présent besoin; veuillez-vous référer à la Partie 5 – Attestations.

Ajouter le paragraphe ci-dessous pour informer les soumissionnaires que le service Connexion postel est disponible pour la transmission électronique des soumissions. L'agent de négociation des contrats doit s'assurer que l'adresse physique, le courriel ainsi que le numéro de télécopieur de l'Unité de réception des soumissions sont inscrits dans la demande de soumissions.

1.2.5 Cette demande de soumissions permet aux soumissionnaires d'utiliser le service Connexion postel offert par la Société canadienne des postes pour la transmission électronique de leur soumission. Les soumissionnaires doivent consulter la partie 2, Instructions à l'intention des soumissionnaires, et partie 3, Instructions pour la préparation des soumissions, de la demande de soumissions, pour obtenir de plus amples renseignements.

1.3 Compte rendu

Les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Les soumissionnaires devraient en faire la demande à l'autorité contractante dans les 15 jours ouvrables suivant la réception des résultats du processus de demande de soumissions. Le compte rendu peut être fourni par écrit, par téléphone ou en personne.

1.4 Autorité contractante

Nom : _____
Titre : _____
Adresse : _____
Téléphone : _____
Télécopieur : _____
Courriel : _____

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

Les instructions uniformisées 2003 sont modifiées comme suit :

- l'article 08, Transmission par télécopieur ou par le service Connexion postel, est modifié comme suit :

  le sous-article 2. est entièrement supprimé et remplacé par ce qui suit :

2. Connexion postel

a. Sauf indication contraire dans la demande de soumissions, les soumissions peuvent être transmises à l'aide du service Connexion postel offert par la Société canadienne des postes.

   (i) SPAC, région de la capitale nationale : La seule adresse de courriel acceptable avec Connexion postel pour transmettre une réponse à une demande de soumissions établie par l'administration centrale de SPAC est :

   tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

   ou le cas échéant, l'adresse courriel indiquée dans la demande de soumissions.

   (ii) Bureaux régionaux de SPAC : La seule adresse de courriel acceptable avec Connexion postel pour transmettre une réponse à une demande de soumissions établie par les bureaux régionaux de SPAC est indiquée dans la demande de soumissions.

b. Pour transmettre une soumission à l'aide du service Connexion postel, le soumissionnaire doit utiliser l'une des deux options suivantes :

   (i) envoyer directement sa soumission uniquement à l'Unité de réception des soumissions de SPAC précisée à l'aide de sa propre licence d'utilisateur du service Connexion postel en vigueur entre son entreprise et la Société canadienne des postes; ou

   (ii) envoyer dès que possible et, dans tous les cas, au moins six jours ouvrables avant la date de clôture de la demande de soumissions (afin de garantir une réponse), un courriel qui contient le numéro de la demande de soumissions à l'Unité de réception des soumissions de SPAC précisée pour demander d'ouvrir une conversation Connexion postel. Les demandes d'ouverture de conversation Connexion postel reçues après cette date pourraient rester sans réponse.

c. Si le soumissionnaire envoie un courriel demandant le service Connexion postel à l'Unité de réception des soumissions précisée dans la demande de soumissions, un agent de l'Unité de réception des soumissions entamera alors la conversation Connexion postel. La conversation du service Connexion postel créera une notification par courriel de la Société canadienne des postes invitant le soumissionnaire à accéder au message dans la conversation et à prendre les mesures nécessaires pour répondre. Le soumissionnaire pourra transmettre sa soumission en réponse à la notification à n'importe quel moment avant la date et l'heure de clôture de la demande de soumissions.

d. Si le soumissionnaire utilise sa licence d'entreprise en vigueur pour envoyer sa soumission, il doit maintenir la conversation Connexion postel ouverte jusqu'à au moins 30 jours ouvrables après la date et l'heure de clôture de la demande de soumissions.

e. Le numéro de la demande de soumissions devrait être indiqué dans le champ réservé à la description dans toutes les transmissions électroniques.

f. Il est important de savoir qu'il faut avoir une adresse postale canadienne pour utiliser le service Connexion postel. Si le soumissionnaire n'en a pas, il peut utiliser l'adresse de l'Unité de réception des soumissions indiquée dans la demande de soumissions pour s'inscrire au service Connexion postel.

g. Dans le cas des transmissions par le service Connexion postel, le Canada ne pourra pas être tenu responsable de tout retard ou panne touchant la transmission ou la réception des soumissions. Entre autres, le Canada n'assumera aucune responsabilité pour ce qui suit :

   (i) réception d'une soumission brouillée, corrompue ou incomplète;

   (ii) disponibilité ou état du service Connexion postel;

   (iii) incompatibilité entre le matériel utilisé pour l'envoi et celui utilisé pour la réception;

   (iv) retard dans la transmission ou la réception de la soumission;

   (v) défaut de la part du soumissionnaire de bien indiquer la soumission;

   (vi) illisibilité de la soumission;

   (vii) sécurité des données contenues dans la soumission;

   (viii) incapacité de créer une conversation électronique par le service Connexion postel.

h. L'Unité de réception des soumissions enverra un accusé de réception des documents de la soumission au moyen de la conversation Connexion postel, peu importe si la conversation a été initiée par le fournisseur à l'aide de sa propre licence ou par l'Unité de réception des soumissions. Cet accusé de réception ne confirmera que la réception des documents de soumission et ne confirmera pas si les pièces jointes peuvent être ouvertes ou si le contenu est lisible.

i. Les soumissionnaires doivent veiller à utiliser la bonne adresse courriel pour l'Unité de réception des soumissions lorsqu'ils amorcent une conversation dans Connexion postel ou communiquent avec l'Unité de réception des soumissions et ne doivent pas se fier à l'exactitude d'un copié-collé de l'adresse courriel dans le système Connexion postel.

j. Une soumission transmise par le service Connexion postel constitue la soumission officielle du soumissionnaire et doit être conforme à l'article 05.

Toutes les instructions, clauses et conditions identifiées dans la demande de soumissions par un numéro, une date et un titre sont reproduites dans le Guide des clauses et conditions uniformisées d'achat (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat) publié par Services publics et approvisionnement Canada.

Les soumissionnaires qui présentent une soumission s'engagent à respecter les instructions, les clauses et les conditions de la demande de soumissions, et acceptent les clauses et les conditions du contrat subséquent.

Le document 2003, _____ (*insérer la date*) Instructions uniformisées – biens ou services - besoins concurrentiels, est incorporé par renvoi dans la demande de soumissions et en fait partie intégrante.

Le paragraphe 3.a) de l'article 01, Dispositions relatives à l'intégrité – soumission, des instructions uniformisées 2003 incorporées ci-haut par renvoi, est supprimé en entier et remplacé par ce qui suit :

a. au moment de présenter un arrangement dans le cadre de la demande d'arrangements en matière d'approvisionnement (DAMA), le soumissionnaire a déjà fourni une liste complète des noms, tel qu'exigé en vertu de la *Politique d'inadmissibilité et de suspension*. Pendant ce processus d'approvisionnement, le soumissionnaire doit immédiatement informer le Canada par écrit de tout changement touchant la liste des noms. »

Inclure la modification suivante aux instructions uniformisées 2003 lorsque les soumissions doivent rester valables pendant plus de 60 jours. Insérer le nombre de jours pendant lesquels la soumission doit rester valable.

Le paragraphe 5.4 du document 2003, Instructions uniformisées - biens ou services - besoins concurrentiels, est modifié comme suit :

Supprimer : 60 jours
Insérer : _____ jours

2.2 Présentation des soumissions

Ajouter le paragraphe ci-dessous si l'adresse courriel, le numéro de télécopieur et l'adresse de livraison de l'Unité de réception des soumissions pour acheminer les soumissions sont fournis à la page 1 de la demande de soumission.

Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de Services publics et approvisionnement Canada (SPAC) au plus tard à la date, à l'heure et à l'endroit indiqués à la page 1 de la demande de soumissions.

Remarque : Pour les soumissionnaires qui choisissent de présenter leurs soumissions en utilisant Connexion postel pour la clôture des soumissions à l'Unité de réception des soumissions dans la région de la capitale nationale, l'adresse de courriel est la suivante :

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

Remarque : Les soumissions ne seront pas acceptées si elles sont envoyées directement à cette adresse de courriel. Cette adresse de courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'indiqué dans les instructions uniformisées 2003 ou pour envoyer des soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

Ou

Ajouter le paragraphe ci-dessous si l'adresse courriel, le numéro de télécopieur et l'adresse de l'Unité de réception des soumissions pour déposer les soumissions ne sont pas fournis à la page 1 de la demande de soumissions.

Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de Services publics et approvisionnement Canada (SPAC) au plus tard à la date et à l'heure indiquées à la page 1 de la demande de soumissions. Les soumissionnaires doivent acheminer leur soumission à l'endroit suivant :

_____ *(identification de l'Unité de réception des soumissions)*

_____ *(adresse physique de livraison)*

_____ *(ville, province, code postal)*

_____ *(adresse de courriel pour le service Connexion postel)*

Remarque : Les soumissions ne seront pas acceptées si elles sont envoyées directement à cette adresse de courriel. Cette adresse de courriel doit être utilisée pour ouvrir une conversation Connexion postel, tel qu'indiqué dans les instructions uniformisées 2003, ou pour envoyer des

soumissions au moyen d'un message Connexion postel si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postel.

En raison du caractère de la demande de soumissions, les soumissions transmises par télécopieur à l'intention de SPAC ne seront pas acceptées.

2.3 Demandes de renseignements – en période de soumission

Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au moins _____ (*insérer le nombre de jours*) jours civils avant la date de clôture des soumissions. Pour ce qui est des demandes de renseignements reçues après ce délai, il est possible qu'on ne puisse pas y répondre.

Les soumissionnaires devraient citer le plus fidèlement possible le numéro de l'article de la demande de soumissions auquel se rapporte la question et prendre soin d'énoncer chaque question de manière suffisamment détaillée pour que le Canada puisse y répondre avec exactitude. Les demandes de renseignements techniques qui ont un caractère exclusif doivent porter clairement la mention « exclusif » vis-à-vis de chaque article pertinent. Les éléments portant la mention « exclusif » feront l'objet d'une discrétion absolue, sauf dans les cas où le Canada considère que la demande de renseignements n'a pas un caractère exclusif. Dans ce cas, le Canada peut réviser les questions ou peut demander au soumissionnaire de le faire, afin d'en éliminer le caractère exclusif, et permettre la transmission des réponses à tous les soumissionnaires. Le Canada peut ne pas répondre aux demandes de renseignements dont la formulation ne permet pas de les diffuser à tous les soumissionnaires.

2.4 Lois applicables

Tout contrat subséquent sera interprété et régi selon les lois en vigueur _____ (*insérer le nom de la province ou du territoire*), et les relations entre les parties seront déterminées par ces lois.

À leur discrétion, les soumissionnaires peuvent indiquer les lois applicables d'une province ou d'un territoire canadien de leur choix, sans que la validité de leur soumission ne soit mise en question, en supprimant le nom de la province ou du territoire canadien précisé et en insérant le nom de la province ou du territoire canadien de leur choix. Si aucun changement n'est indiqué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées.

2.5 Améliorations apportées au besoin pendant la demande de soumissions

Les soumissionnaires qui estiment qu'ils peuvent améliorer, techniquement ou technologiquement, le devis descriptif ou l'énoncé des travaux contenus dans la demande de soumissions, sont invités à fournir des suggestions par écrit à l'autorité contractante identifiée dans la demande de soumissions. Les soumissionnaires doivent indiquer clairement les améliorations suggérées et les motifs qui les justifient. Les suggestions, qui ne restreignent pas la concurrence ou qui ne favorisent pas un soumissionnaire en particulier, seront examinées à la condition qu'elles parviennent à l'autorité contractante au plus tard _____ jours avant la date de clôture de la demande de soumissions. Le Canada aura le droit d'accepter ou de rejeter n'importe quelle ou la totalité des suggestions proposées.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

a) Si le soumissionnaire choisit d'envoyer sa soumission par voie électronique, le Canada exige de sa part qu'il respecte l'article 08 des instructions uniformisées 2003. Le système Connexion postel a une limite de 1 Go par message individuel affiché et une limite de 20 Go par conversation.

La soumission doit être présentée en sections distinctes comme suit :
Section I : Soumission technique
Section II : Soumission financière
Section III : Attestations

b) Si le soumissionnaire choisit de transmettre sa soumission sur papier, le Canada demande que la soumission soit présentée en sections distinctes, comme suit :

Section I : Soumission technique *(____ copies électroniques sur clé USB);*

Section II : Soumission financière *(____ copies électroniques sur clé USB);*

Section III : Attestations *(____ copies électroniques sur clé USB).*

c) Si le soumissionnaire fournit simultanément plusieurs copies de sa soumission à l'aide de méthodes de livraison acceptable, et en cas d'incompatibilité entre le libellé de la copie électronique transmise par le service Connexion postel et celui de la copie papier, le libellé de la copie électronique transmise par le service Connexion postel aura préséance sur le libellé des autres copies.

d) En raison du caractère de la demande de soumissions, les soumissions transmises en copies papier ou par télécopieur ne seront pas acceptées.

e) Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué dans une autre section de la soumission.

Section I : Soumission technique

Dans leur soumission technique, les soumissionnaires devraient démontrer leur compréhension des exigences contenues dans la demande de soumissions et expliquer comment ils répondront à ces exigences. Les soumissionnaires devraient démontrer leur capacité _____ (*insérer, s'il y a lieu* : « et décrire l'approche qu'ils prendront ») de façon complète, concise et claire pour effectuer les travaux.

La soumission technique devrait traiter clairement et de manière suffisamment approfondie des points faisant l'objet des critères d'évaluation en fonction desquels la soumission sera évaluée. Il ne suffit pas de reprendre simplement les énoncés contenus dans la demande de soumissions. Afin de faciliter l'évaluation de la soumission, le Canada demande que les soumissionnaires reprennent les sujets dans l'ordre des critères d'évaluation, sous les mêmes rubriques. Pour éviter les recoupements, les soumissionnaires peuvent faire référence à différentes sections de leur soumission en indiquant le numéro de l'alinéa et de la page où le sujet visé est déjà traité.

Section II : Soumission financière

3.1.1 Les soumissionnaires doivent présenter leur soumission financière en conformité avec à l'annexe « X »).

3.1.2 Paiement électronique de factures – soumission

Si vous êtes disposés à accepter le paiement de factures au moyen d'instruments de paiement électronique, compléter l'annexe « X » Instruments de paiement électronique, afin d'identifier lesquels sont acceptés.

Si l'annexe « X » Instruments de paiement électronique n'a pas été complétée, il sera alors convenu que le paiement de factures au moyen d'instruments de paiement électronique ne sera pas accepté.

L'acceptation des instruments de paiement électronique ne sera pas considérée comme un critère d'évaluation.

3.1.3 Fluctuation du taux de change

Le besoin ne prévoit pas offrir d'atténuer les risques liés à la fluctuation du taux de change.
Aucune demande d'atténuation des risques liés à la fluctuation du taux de change ne sera prise en considération. Toute soumission incluant une telle disposition sera déclarée non recevable.

3.1.4 Capacité financière

Clause du Guide des CCUA A9033T _____ (*insérer la date*), *Capacité financière*

Section III : Attestations

Les soumissionnaires doivent présenter les attestations et les renseignements supplémentaires exigés à la Partie 5.

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

(a) Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, incluant les critères d'évaluation techniques et financiers.

(b) Une équipe d'évaluation composée de représentants du Canada évaluera les soumissions.

4.1.1 Évaluation technique

Les critères techniques obligatoires (*et les critères techniques cotés [le cas échéant]*) sont inclus dans l'annexe _____.

4.1.2 Évaluation financière

Le prix de la soumission sera évalué en dollars canadiens, excluant les taxes applicables, FAB destination, incluant les droits de douane et les taxes d'accise canadiens.

4.2 Méthode de sélection

Utiliser l'option appropriée pour la méthode de sélection ci-dessous selon les critères obligatoires et/ou critères cotés évalués ci-dessus.

OPTION 1 – BESOINS SIMPLES

Utiliser la clause suivante lorsque la demande de soumissions comprend des critères d'évaluation techniques obligatoires seulement et que la méthode de sélection se fera en fonction de la soumission recevable avec le prix évalué le plus bas.

4.2.1 Critères techniques obligatoires

(a) Une soumission doit respecter les exigences de la demande de soumissions et satisfaire à tous les critères d'évaluation techniques obligatoires pour être déclarée recevable.

(b) La soumission recevable avec le prix évalué le plus bas sera recommandée pour attribution d'un contrat.

OPTION 2 – BESOINS COMPLEXES

Utiliser la clause suivante lorsque la demande de soumissions comprend des critères d'évaluation techniques obligatoires et cotés, et que la méthode de sélection se fera en fonction du résultat obtenu sur le plan du mérite technique et du prix.

4.2.1 Note combinée la plus haute sur le plan du mérite technique et du prix

(a) Pour être déclarée recevable, une soumission doit :

(i) respecter toutes les exigences de la demande de soumissions; et

(ii) satisfaire à tous les critères obligatoires; et

(iii) obtenir le nombre minimal de ____ (inscrire un nombre minimal de points) points exigés pour l'ensemble des critères d'évaluation techniques cotés.
L'échelle de cotation compte ____ (*inscrire le total des points pouvant être accordés*) points.

(b) Les soumissions qui ne répondent pas aux exigences a) ou b) ou c) seront déclarées non recevables.

(c) La sélection sera faite en fonction du meilleur résultat global sur le plan du mérite technique et du prix. Une proportion de ____ % (inscrire le pourcentage pour le mérite technique) sera accordée au mérite technique et une proportion de ____ % (*inscrire le pourcentage pour le prix*) sera accordée au prix.

(d) Afin de déterminer la note pour le mérite technique, la note technique globale de chaque soumission recevable sera calculée comme suit : le nombre total de points obtenus sera divisé par le nombre total de points pouvant être accordés, puis multiplié par ____ % (inscrire le pourcentage accordé au mérite technique).

(e) Afin de déterminer la note pour le prix, chaque soumission recevable sera évaluée proportionnellement au prix évalué le plus bas et selon le ratio de ____ % (*insérer le pourcentage accordé au prix*).

(f) Pour chaque soumission recevable, la cotation du mérite technique et la cotation du prix seront ajoutées pour déterminer la note combinée.

(g) La soumission recevable ayant obtenu le plus de points ou celle ayant le prix évalué le plus bas ne sera pas nécessairement choisie. La soumission recevable qui obtiendra la note combinée la plus élevée pour le mérite technique et le prix sera recommandée pour l'attribution du contrat.

PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES

Les soumissionnaires doivent fournir les attestations et les renseignements supplémentaires exigés pour qu'un contrat leur soit attribué.

Les attestations que les soumissionnaires remettent au Canada peuvent faire l'objet d'une vérification à tout moment par le Canada. À moins d'indication contraire, le Canada déclarera une soumission non recevable, ou à un manquement de la part de l'entrepreneur s'il est établi qu'une attestation du soumissionnaire est fausse, sciemment ou non, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat.

L'autorité contractante aura le droit de demander des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. À défaut de répondre et de coopérer à toute demande ou exigence imposée par l'autorité contractante, la soumission sera déclarée non recevable, ou constituera un manquement aux termes du contrat.

5.1 Attestations exigées avec la soumission

Les soumissionnaires doivent fournir les attestations suivantes dûment remplies avec leur soumission.

5.1.1 Marchés réservés aux entreprises autochtones

Si le marché est réservé dans le cadre de la Stratégie d'approvisionnement auprès des entreprises autochtones, insérer le texte intégral des clauses A3000T et A3001T, et s'il y a lieu, A3002T du Guide des CCUA.

5.2 Attestations préalables à l'attribution du contrat

Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être remplis et fournis avec la soumission mais ils peuvent être fournis plus tard. Si l'une de ces attestations ou renseignements supplémentaires ne sont pas remplis et fournis tel que demandé, l'autorité contractante informera le soumissionnaire du délai à l'intérieur duquel les renseignements doivent être fournis. À défaut de fournir les attestations ou les renseignements supplémentaires énumérés ci-dessous dans le délai prévu, la soumission sera déclarée non recevable.

5.2.1 Programme de contrats fédéraux pour l'équité en matière d'emploi - Attestation de soumission

En présentant une soumission, le soumissionnaire atteste que le soumissionnaire, et tout membre de la coentreprise si le soumissionnaire est une coentreprise, n'est pas nommé dans la liste des « soumissionnaires à admissibilité limitée du PCF » du Programme de contrats fédéraux (PCF) pour l'équité en matière d'emploi disponible au bas de la page du site Web d'Emploi et Développement social Canada (EDSC) – Travail (https://www.canada.ca/fr/emploi-developpement-social/programmes/equite-emploi/programme-contrats-federaux.html#s4).

Le Canada aura le droit de déclarer une soumission non recevable si le soumissionnaire, ou tout membre de la coentreprise si le soumissionnaire est une coentreprise, figure dans la liste des « soumissionnaires à admissibilité limitée du PCF » au moment de l'attribution du contrat.

Insérer les paragraphes suivants pour les besoins formulés au nom d'un ministère ou d'un organisme assujetti au Programme de contrats fédéraux, estimés à 1 000 000 $ et plus, excluant les options, taxes applicables incluses : (consulter l'Annexe 5.1 du Guide des approvisionnements)

Le Canada aura aussi le droit de résilier le contrat pour manquement si l'entrepreneur, ou tout membre de la coentreprise si l'entrepreneur est une coentreprise, figure dans la liste des « soumissionnaires à admissibilité limitée du PCF » pendant la durée du contrat.

Le soumissionnaire doit fournir à l'autorité contractante l'annexe intitulée Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation remplie avant l'attribution du contrat. Si le soumissionnaire est une coentreprise, il doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi - Attestation remplie pour chaque membre de la coentreprise.

ANNEXE « X » - ÉNONCÉ DES TRAVAUX OU BESOIN

(***insérer s'il y a lieu***)

ANNEXE « X » - BASE DE PAIEMENT

(***insérer s'il y a lieu)***

ANNEXE « X » - LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

(***insérer s'il y a lieu)***

ANNEXE « X » - INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE

(insérer s'il y a lieu)

Tel qu'indiqué à la clause 3.1.2 de la Partie 3, le soumissionnaire doit compléter l'information ci-dessous afin d'identifier quels instruments de paiement électronique sont acceptés pour le paiement de factures.

Le soumissionnaire accepte d'être payé au moyen de l'un des instruments de paiement électronique suivants :

( ) Carte d'achat VISA ;
( ) Carte d'achat MasterCard ;
( ) Dépôt direct (national et international) ;
( ) Échange de données informatisées (EDI) ;
( ) Virement télégraphique (international seulement) ;
( ) Système de transfert de paiements de grande valeur (plus de 25 M$)

ANNEXE « X » - PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – ATTESTATION

(insérer s'il y a lieu)

Insérer l'attestation suivante pour les besoins formulés au nom d'un ministère ou d'un organisme assujetti au Programme de contrats fédéraux, estimés à 1 000 000 $ et plus, excluant les options, taxes applicables incluses. (consulter l'Annexe 5.1 du Guide des approvisionnements ainsi que la Partie 5 – Attestations et renseignements supplémentaires)

Je, soumissionnaire, en présentant les renseignements suivants à l'autorité contractante, atteste que les renseignements fournis sont exacts à la date indiquée ci-dessous. Les attestations fournies au Canada peuvent faire l'objet d'une vérification à tout moment. Je comprends que le Canada déclarera une soumission non recevable, ou un entrepreneur en situation de manquement, si une attestation est jugée fausse, que ce soit pendant la période d'évaluation des soumissions, ou pendant la durée du contrat. Le Canada aura le droit de demander des renseignements supplémentaires pour vérifier les attestations d'un soumissionnaire. À défaut de répondre à toute demande ou exigence imposée par le Canada, la soumission peut être déclarée non recevable ou constituer un manquement aux termes du contrat.

Pour obtenir de plus amples renseignements sur le Programme de contrats fédéraux pour l'équité en matière d'emploi, visitez le site Web d'Emploi et Développement social Canada (EDSC) – Travail.

Date : _____ (AAAA/MM/JJ) [si aucune date n'est indiquée, la date de clôture de la demande de soumissions sera utilisée]

Compléter à la fois A et B.

A. Cochez seulement une des déclarations suivantes :

( ) A1. Le soumissionnaire atteste qu'il n'a aucun effectif au Canada.

( ) A2. Le soumissionnaire atteste qu'il est un employeur du secteur public.

( ) A3. Le soumissionnaire atteste qu'il est un employeur sous réglementation fédérale, dans le cadre de la Loi sur l'équité en matière d'emploi.

( ) A4. Le soumissionnaire atteste qu'il a un effectif combiné de moins de 100 employés permanents à temps plein et/ou permanents à temps partiel au Canada.

A5. Le soumissionnaire a un effectif combiné de 100 employés ou plus au Canada; et

( ) A5.1. Le soumissionnaire atteste qu'il a conclu un Accord pour la mise en œuvre de l'équité en matière d'emploi valide et en vigueur avec EDSC – Travail.

OU

( ) A5.2. Le soumissionnaire a présenté l'Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168) à EDSC - Travail. Comme il s'agit d'une condition à l'attribution d'un contrat, remplissez le formulaire intitulé Accord pour la mise en œuvre de l'équité en matière d'emploi (LAB1168), signez-le en bonne et due forme et transmettez-le à EDSC – Travail.

B. Cochez seulement une des déclarations suivantes :

( ) B1. Le soumissionnaire n'est pas une coentreprise.

OU

( ) B2. Le soumissionnaire est une coentreprise et chaque membre de la coentreprise doit fournir à l'autorité contractante l'annexe Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation. (Consultez la section sur les coentreprises des instructions uniformisées.)

ANNEXE F – CLAUSE DU CONTRAT SUBSÉQUENT

(voir en attachement après la DAMA)

LES EXIGENCES DE SECURITE SUIVANTES SONT FACULTATIVES (A UTILISER LORSQUE LE CONTRACTANT AURA ACCES AUX INFORMATIONS PROTEGEES)

L'entrepreneur doit se conformer aux exigences énoncées dans, le cas échéant:

(a) **Annexe G - EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN**

(b) **Annexe H - EXIGENCE RELATIVES À LA SÉCURITÉ POUR LES FOURNISSERUS ÉTRANGERS**

Les approvisionnements requis au moyen de l'arrangement en matière d'approvisionnement peuvent également imposer aux fournisseurs (canadiens et étrangers) une autorisation de sécurité secrète. Les fournisseurs peuvent lancer le processus de filtrage de sécurité des organisations et du personnel dès que possible. Les détails peuvent être trouvés à: https://www.tpsgc-pwgsc.gc.ca/esc-src/enquete-screening-fra.html. Si nécessaire, les fournisseurs peuvent contacter l'autorité d'arrangements en matière d'approvisionnement, qui parrainera toute demande de filtrage de sécurité pour les organisations et le personnel.

ANNEXE G – EXIGENCES RELATIVES À LA SÉCURITÉ POUR LES ENTREPREUNEURS CANADIENS

1. L'entrepreneur ou offrant doit détenir en permanence, pendant l'exécution du marché ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) valide, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ A ou B (selon le cas), délivrées par le Secteur de la sécurité industrielle (SS) de **Services publics et Approvisionnement Canada (SPAC), anciennement Travaux publics et Services gouvernementaux Canada (TPSGC).**

2. Les membres du personnel de l'entrepreneur ou offrant devant accéder à des renseignements, à des biens ou à des lieux de travail de niveau PROTÉGÉ doivent TOUS détenir une cote de sécurité du personnel valide au niveau SECRET ou FIABILITÉ selon la classification de sécurité, délivrée ou approuvée par le SSI ou TPSGC.

3. L'entrepreneur NE doit PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker électroniquement des renseignements PROTÉGÉS tant qu'il n'en a pas reçu l'approbation écrite par le responsable de la sécurité du ministère client. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau PROTÉGÉ A ou B (selon le cas), avec lien électronique au niveau PROTÉGÉ A ou B (selon le cas).
4. Les contrats de sous-traitance comportant des exigences relatives à la sécurité ne doivent PAS être attribués sans l'autorisation écrite préalable du SSI ou de TPSGC.

5. L'entrepreneur ou l'offrant doit respecter les dispositions des documents suivants :

   (a) Liste de vérification relative à la sécurité et guide de sécurité (le cas échéant);
   (b) Manuel de la sécurité industrielle (dernière édition);
   (c) Site Web du SSI : Exigences de sécurité des contrats du gouvernement du Canada, disponibles à l'adresse : https://www.tpsgc-pwgsc.gc.ca/esc-src/.

REMARQUE : Il y a plusieurs niveaux de filtrage de sécurité du personnel liés à ce dossier. Dans le cas présent, un guide de classification de sécurité doit être ajouté à la LVERS afin de clarifier ces niveaux de filtrage de

sécurité. Le guide de sécurité est normalement rédigé par le chargé de projet ou le responsable de la sécurité de l'organisation.

ANNEXE H – EXIGENCES RELATIVES À LA SÉCURITÉ POUR LES ENTREPRESEURS ÉTRANGERS

L'administration désignée en matière de sécurité (ADS canadienne) pour les questions industrielles au Canada est le Secteur de la sécurité industrielle (SSI) de TPSGC, administré par la Direction de la sécurité industrielle internationale (DSII). L'ADS canadienne est chargée d'évaluer la conformité des **entrepreneurs** et des **sous-traitants** aux exigences relatives à la sécurité pour les entrepreneurs étrangers. Les exigences suivantes en matière de sécurité s'appliquent aux **entrepreneurs** et aux **sous-traitants** destinataires étrangers constitués en société ou autorisés à faire des affaires dans un État autre que le Canada et qui livrent et exécutent à l'extérieur du Canada les services ou les travaux décrits dans le contrat, en plus des obligations en matière de sécurité et de vie privée décrites respectivement dans les appendices B et C.

Les paragraphes suivants s'appliquent aux situations où l'**entrepreneur** ou le **sous-traitant** confirme qu'il a accès aux données du Canada et qu'il en a la garde et le contrôle.

1. L'**entrepreneur** ou le **sous-traitant** destinataire étranger doit provenir d'un pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Union européenne (UE) ou d'un pays avec lequel le Canada a conclu une entente internationale bilatérale sur la sécurité industrielle. Le programme de sécurité des contrats a des ententes en matière de sécurité industrielle, protocole d'entente bilatérale ou multinationale industrielle avec les pays mentionnés au site suivant de TPSGC : https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

2. L'**entrepreneur** ou le **sous-traitant** destinataire étranger doit détenir en permanence, pendant l'exécution du **contrat** ou du **contrat de sous-traitance**, une équivalence de l'attestation de vérification d'organisation désignée (VOD) valide, délivrée par l'ADS canadienne, selon la procédure suivante :

   (a) L'**entrepreneur** ou le **sous-traitant** destinataire étranger doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire sur son territoire de compétence.

   (b) L'**entrepreneur** ou le **sous-traitant** destinataire étranger ne doit pas commencer à fournir les services ou à réaliser le travail tant que l'administration désignée en matière de sécurité canadienne (ADS canadienne) n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le contrat. L'ADS canadienne fournira, par écrit, à l'**entrepreneur** ou au **sous-traitant** destinataire étranger, une déclaration qui confirmera la conformité et l'autorisation de fournir les services prévus.

   (c) L'**entrepreneur** ou le **sous-traitant** destinataire étranger doit désigner un agent de sécurité des contrats (ASC) autorisé et un agent remplaçant de sécurité des contrats (ARSC), au besoin, qui sera responsable du contrôle les exigences relatives à la sécurité, telles qu'elles sont définies dans le contrat. Cette personne sera désignée par le président-directeur général ou par un cadre supérieur clé désigné de l'**entrepreneur** ou du **sous-traitant** destinataire étranger proposant. Les cadres supérieurs clés comprennent les propriétaires, les mandataires, les directeurs, les cadres et les partenaires occupant un poste qui leur permettraient de porter atteinte aux politiques ou aux pratiques de l'organisation durant l'exécution du contrat.

   (d) L'**entrepreneur** ou le **sous-traitant** destinataire étranger ne doit pas accorder l'accès aux renseignements ou aux actifs **PROTÉGÉS DU CANADA**, sauf aux membres du personnel qui ont fait l'objet d'une vérification de sécurité conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115) du Conseil du Trésor, ou qui utilisent des mesures équivalentes acceptables

établies par l'entrepreneur dans ses documents publics, et comme convenu par l'ADS canadienne, notamment, sans toutefois s'y limiter :

(i) le personnel a un besoin de savoir pour l'exécution du **contrat**;
(ii) le casier judiciaire et les antécédents des membres du personnel ont fait l'objet d'une vérification par un organisme gouvernemental ou du secteur privé reconnu **de leur pays** ainsi que d'une vérification des antécédents validée par l'ADS canadienne;
(iii) l'**entrepreneur** ou le **sous-traitant** destinataire étranger doit veiller à ce que ses employés consentent à ce que les résultats des vérifications de leur casier judiciaire et de leurs antécédents soient communiqués à l'ADS canadienne et à d'autres fonctionnaires du gouvernement canadien, au besoin; et
(iv) Le gouvernement du Canada se réserve le droit de refuser l'accès à des renseignements ou à des actifs **PROTÉGÉS AU CANADA** à un **entrepreneur** ou à un **sous-traitant** destinataire étranger pour un motif valable.

3. Les renseignements personnels et les biens **DE NIVEAU PROTÉGÉ DU CANADA** qui sont fournis à l'**entrepreneur** ou au **sous-traitant** étranger destinataire, ou qui sont produits par ce dernier, doivent respecter les conditions suivantes :

(a) ils ne doivent pas être divulgués à un autre gouvernement, à une autre personne ou à une autre entreprise (ni à un représentant de cette autre personne ou de cette autre entreprise) qui n'est pas directement lié à l'exécution du **contrat** ou du **contrat de sous-traitance** sans le consentement écrit préalable du gouvernement du Canada. Ce consentement doit être obtenu auprès de son autorité de protection des données (APD) et de l'autorité contractante (en collaboration avec l'ASD canadienne);

(b) ils ne doivent pas être utilisés à des fins autres que l'exécution du **contrat** ou du **contrat de sous-traitance**, sans l'approbation écrite préalable du Canada. Cette approbation doit être obtenue auprès de son autorité de protection des données (APD) et l'autorité contractante (en collaboration avec l'ASD canadienne).

4. L'**entrepreneur** ou le **sous-traitant** destinataire étranger NE DOIT PAS emporter de renseignements ou d'actifs **PROTÉGÉS AU CANADA** hors des établissements de travail visés; et l'**entrepreneur** ou le **sous-traitant** destinataire étranger doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.

5. L'**entrepreneur** ou le **sous-traitant** destinataire étranger ne doit pas utiliser les renseignements ni les actifs **PROTÉGÉS AU CANADA** pour répondre à des besoins autres que l'exécution du **contrat** ou du **contrat de sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette approbation doit être obtenue auprès de l'ADS canadienne.

6. L'**entrepreneur** ou le **sous-traitant** destinataire étranger doit détenir en permanence, pendant l'exécution du **contrat** ou du **contrat de sous-traitance**, une autorisation équivalente à l'autorisation de détenir des renseignements (ADR) de niveau PROTÉGÉ A ou B DU CANADA, selon le cas.

7. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne.

8. L'**entrepreneur** ou le **sous-traitant** destinataire étranger doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité ci-jointe.

9. Le Canada a le droit de rejeter toute demande présentée de manière distincte et indépendante de l'autorisation contenue dans le présent contrat relativement à l'autorisation de l'entrepreneur qui fournit les

services d'accéder, de traiter, de produire, de transmettre ou de stocker électroniquement des renseignements ou des actifs PROTÉGÉS A OU B DU **CANADA** (selon le cas) relativement à la prestation des services ou à la réalisation des travaux dans tout autre pays s'il y a lieu de craindre pour la sécurité, la confidentialité ou l'intégrité des renseignements.

10. Propriété des renseignements personnels et des dossiers

Pour exécuter les services ou les travaux, l'**entrepreneur** ou le **sous-traitant** étranger destinataire se verra remettre ou recueillera des renseignements personnels de tiers. L'**entrepreneur** ou le **sous-traitant** étranger destinataire reconnaît qu'il n'a aucun droit sur ces renseignements personnels ou dossiers et que ces derniers appartiennent au Canada. L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit rendre disponibles, sur demande du Canada, tous les renseignements personnels et dossiers dans un format acceptable pour le Canada.

11. Utilisation des renseignements personnels

L'**entrepreneur** ou le **sous-traitant** étranger destinataire convient de créer, recueillir, recevoir, gérer, utiliser et conserver des renseignements personnels et des dossiers de même que d'y avoir accès et d'en disposer uniquement pour exécuter les services ou les travaux conformément au **contrat** ou au **contrat de sous-traitance**.

12. Collecte de renseignements personnels

Si l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit obtenir des renseignements personnels d'un tiers dans le cadre des services ou des travaux, il ne doit recueillir que les renseignements personnels lui permettant d'exécuter les services ou travaux. L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit recueillir les renseignements personnels auprès de la personne concernée et l'informer (au moment de la collecte ou préalablement) de ce qui suit :

(a) les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;

(b) les usages qui seront faits des renseignements personnels recueillis;

(c) la divulgation des renseignements personnels est volontaire ou, s'il existe une obligation juridique de divulguer les renseignements personnels, les fondements de cette obligation juridique;

(d) les conséquences, le cas échéant, du refus de fournir les renseignements;

(e) l'intéressé a le droit d'accéder à ses renseignements personnels et d'y apporter des corrections;

(f) les renseignements personnels feront partie d'un répertoire particulier (au sens de la *Loi sur la protection des renseignements personnels*), et le demandeur est informé de l'institution fédérale qui gère le répertoire de renseignements personnels, si l'autorité contractante a fourni ces renseignements à l'**entrepreneur** ou au **sous-traitant** étranger destinataire.

13. L'**entrepreneur** ou le **sous-traitant** étranger destinataire et leurs employés respectifs doivent s'identifier auprès des individus desquels ils recueillent des renseignements personnels et leur donner le moyen de vérifier qu'ils sont autorisés à recueillir les renseignements personnels conformément à un contrat passé avec le Canada.

14. Si l'autorité contractante l'exige, l'**entrepreneur** ou le **sous-traitant** destinataire étranger doit élaborer un formulaire de demande de consentement à utiliser lors de la cueillette de renseignements personnels ou un texte dans le cas de la cueillette de renseignements personnels par téléphone. L'**entrepreneur** ou

le **sous-traitant** étranger destinataire ne peut utiliser le formulaire ou le texte sans avoir obtenu l'approbation écrite préalable de l'autorité contractante. Il doit aussi obtenir le consentement de l'autorité contractante avant de modifier le formulaire ou le texte.

15. si, au moment de la collecte de renseignements personnels auprès d'une personne, l'**entrepreneur** ou le **sous-traitant** étranger destinataire soupçonne que cette personne n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit demander des directives à l'autorité contractante.

16. Assurer l'exactitude, la confidentialité et l'intégrité des renseignements personnels

L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit veiller à ce que les renseignements personnels soient les plus exacts, complets et à jour possible. L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit veiller à protéger la confidentialité des renseignements personnels. À cette fin, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit au moins :

(a) ne pas utiliser de données d'identification personnelle (p. ex. le numéro d'assurance sociale) pour lier de nombreuses bases de données qui comprennent des renseignements personnels;

(b) séparer tous les enregistrements des informations et des dossiers de l'**entrepreneur** ou du **sous-traitant** étranger destinataire;

(c) ne donner l'accès aux renseignements personnels et aux dossiers qu'aux personnes qui en ont besoin aux fins de l'exécution des services ou des travaux (par exemple, en utilisant des mots de passe ou un accès biométrique);

(d) donner de la formation à toute personne à laquelle l'**entrepreneur** ou le **sous-traitant** étranger destinataire donne accès aux renseignements personnels concernant l'obligation d'assurer la confidentialité et de ne l'utiliser qu'aux fins de l'exécution des services ou des travaux. L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit donner cette formation avant d'autoriser l'accès aux renseignements personnels et préparer à cet effet un dossier accessible à l'autorité contractante, sur demande;

(e) à la demande de l'autorité contractante, demander aux personnes ayant accès aux renseignements personnels de reconnaître, par écrit (sous une forme approuvée par l'autorité contractante), leurs responsabilités en matière de confidentialité des renseignements personnels, avant de leur en donner l'accès;

(f) garder un registre de toutes les demandes faites par une personne pour la révision de ses renseignements personnels et toutes les demandes de correction d'erreurs ou d'omissions concernant les renseignements personnels (que les demandes soient faites directement par une personne ou par le Canada au nom d'une personne);

(g) joindre une note à tout dossier qu'une personne a demandé de corriger, mais que l'**entrepreneur** ou le **sous-traitant** étranger destinataire a décidé, pour quelque raison que ce soit, de ne pas corriger. Lorsque cela se produit, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit immédiatement informer l'autorité contractante de la correction demandée et des raisons de l'**entrepreneur** ou du **sous-traitant** de l'étranger destinataire de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, l'entrepreneur a l'obligation de le faire;

(h) consigner la date et l'auteur de la dernière mise à jour de chaque dossier;

(i) tenir un journal de vérification électronique qui enregistre tous les accès et toutes les tentatives

d'accès des dossiers électroniques. Le journal de vérification doit être tenu dans un format qui peut être lu par l'**entrepreneur** ou le **sous-traitant** étranger destinataire et le Canada en tout temps;

(j) protéger et contrôler l'accès à tout exemplaire papier des dossiers.

17. Protection des renseignements personnels

L'**entrepreneur** ou le **sous-traitant** étranger destinataire doit, en tout temps, protéger les renseignements personnels en prenant toutes les mesures nécessaires visant la protection de leur intégrité et de leur confidentialité. À cette fin, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit au moins :

(a) stocker les renseignements personnels sous format électronique de manière à ce qu'un mot de passe (ou un mécanisme de contrôle similaire, comme l'accès biométrique) soit requis pour accéder au système ou à la base de données contenant les renseignements personnels;

(b) s'assurer que les mots de passe ou autres moyens d'accès aux renseignements personnels ne sont fournis qu'aux personnes qui le requièrent aux fins de l'exécution des services ou des travaux;

(c) ne pas confier à un tiers (y compris une société affiliée) le stockage électronique des renseignements personnels sans l'autorisation préalable et écrite de l'autorité désignée en matière de sûreté du Canada;

(d) protéger toutes les bases de données ou tous les systèmes informatiques qui contiennent les renseignements personnels contre un accès externe au moyen de méthodes couramment utilisées de temps à autre par des organismes publics et privés canadiens jugés prudents dans le but de protéger les renseignements très protégés et hautement sensibles;

(e) faire une sauvegarde et une mise à jour de tous les dossiers au moins une fois par semaine;

(f) mettre en œuvre toutes les mesures de sécurité ou de protection raisonnables demandées par le Canada de temps à autre;

(g) aviser immédiatement l'autorité contractante et l'autorité désignée en matière de sûreté du Canada de toute infraction à la sécurité; par exemple, chaque fois qu'une personne non autorisée obtient accès aux renseignements personnels.

18. Obligations réglementaires

(a) L'**entrepreneur** ou le **sous-traitant** reconnaît que le Canada est tenu de traiter tous les renseignements personnels et les dossiers conformément aux dispositions de la *Loi sur la protection des renseignements personnels*, de la *Loi sur l'accès à l'information*, L.C., 1985, ch. A-1 et *Loi sur la Bibliothèque et les Archives du Canada*, L.C. 2004, ch. 11. L'**entrepreneur** ou le **sous-traitant** étranger destinataire convient de se conformer aux exigences établies par l'autorité contractante qui sont requises pour permettre au Canada de remplir ses obligations en vertu de ces lois et de toute autre loi qui entre en vigueur.

(b) L'**entrepreneur** ou le **sous-traitant** destinataire étranger reconnaît que les obligations dont il doit s'acquitter en vertu du **contrat** ou du **contrat de sous-traitance** s'ajoutent à toutes celles qui lui incombent en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, ou d'une loi similaire en vigueur dans une province ou un territoire du Canada. Si l'**entrepreneur** ou le **sous-traitant** étranger destinataire croit que l'une ou l'autre des obligations du **contrat** ou du **contrat de sous-traitance** l'empêche de respecter ses obligations en vertu de ces lois, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit immédiatement aviser l'autorité contractante de la disposition particulière du **contrat** ou du **contrat de sous-traitance** et

de la disposition législative avec laquelle il y a conflit selon lui.

19. Obligation juridique de divulguer les renseignements personnels

Avant de divulguer tout renseignement personnel conformément à toute loi, à tout règlement ou toute ordonnance rendue par une cour de justice, un tribunal ou une entité administrative compétente, l'**entrepreneur** ou le **sous-traitant** étranger destinataire doit immédiatement informer l'autorité contractante, afin de lui permettre de participer aux procédures pertinentes.

20. Plaintes

Le Canada et l'**entrepreneur** ou le **sous-traitant** étranger destinataire conviennent de s'informer immédiatement et mutuellement de la réception d'une plainte en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* ou de toute autre loi pertinente concernant les renseignements personnels. Les parties conviennent de s'échanger toute information nécessaire pour faciliter le règlement de la plainte et de s'informer immédiatement l'une l'autre de son dénouement.

21. Exception

Les obligations énoncées dans ces conditions générales supplémentaires ne s'appliquent pas aux renseignements personnels qui sont déjà du domaine public, du moment qu'elles ne sont pas devenues du domaine public à la suite d'une faute ou d'une omission de l'entrepreneur ou de tout sous-traitant, mandataire ou représentant de l'entrepreneur ou de leurs employés.

22. Vérification et conformité

Le Canada peut vérifier en tout temps la conformité du destinataire étranger, y compris l'entrepreneur ou le sous-traitant, avec ces conditions générales supplémentaires. À la demande de l'autorité contractante, l'entrepreneur ou le sous-traitant doit donner au Canada (ou à son représentant autorisé) l'accès à ses locaux et aux renseignements personnels et dossiers à tout moment jugé raisonnable. Si le Canada découvre un problème durant la vérification, l'entrepreneur ou le sous-traitant étranger destinataire doit le corriger immédiatement à ses frais.

ANNEXE I – LVERS RELATIVES AUX LOGICIELS-SERVICES

Clear Data - Effacer les données

Government of Canada / Gouvernement du Canada

English Instructions | Instructions français

Contract Number / Numéro du contrat

Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
4. Brief Description of Work - Brève description du travail	

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No Non	☐ Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No Non	☐ Yes Oui
6. Indicate the type of access required - Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No Non	☑ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p.ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No Non	☐ Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciales sans entreposage de nuit?	☑ No Non	☐ Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion ☑	All NATO countries Tous les pays de l'OTAN ☐	No release restrictions Aucune restriction relative à la diffusion ☐
Not releasable À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :
7. c) Level of information / Niveau d'information		
PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Security Classification / Classification de sécurité
UNCLASSIFIED

TBS/SCT 350-103 (2004/12)

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
Security Classification / Classification de sécurité	UNCLASSIFIED

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets: — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :

Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET - SIGINT / TRÈS SECRET - SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments: / Commentaires spéciaux : Refer to Appendix A - Security Classification Guide

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — ☐ No / Non ☑ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted: — ☐ No / Non ☑ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — ☐ No / Non ☑ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

PART C *(continued)* / PARTIE C *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	Confidential Confidentiel	Secret	Top Secret Très Secret	NATO Restricted NATO Diffusion Restreinte	NATO Confidential NATO Confidentiel	NATO Secret	COSMIC Top Secret COSMIC Très Secret	Protected Protégé A	 B	 C	Confidential Confidentiel	Secret	Top Secret Très Secret
Information / Assets Renseignements / Biens	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Production	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
IT Media Support TI	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
IT Link Lien électronique	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉ et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée.

12. b) Will the document attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

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).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☐ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

17. Contracting Security Authority / Autorisé contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature	
Telephone no. - N° de téléphone	Facsimile - Télécopieur	E-mail address - Adresse courriel	Date

Form

Next Page

Instructions for completion of a Security Requirements Check List (SRCL)

The instruction sheet should remain attached until Block #17 has been completed.

GENERAL - PROCESSING THIS FORM

The project authority shall arrange to complete this form.

The organization security officer shall review and approve the security requirements identified in the form, in cooperation with the project authority.

The contracting security authority is the organization responsible for ensuring that the suppliers are compliant with the security requirements identified in the SRCL.

All requisitions and subsequent tender / contractual documents including subcontracts that contain PROTECTED and/or CLASSIFIED requirements must be accompanied by a completed SRCL.

It is important to identify the level of PROTECTED information or assets as Level "A," "B" or "C," when applicable; however, certain types of information may only be identified as "PROTECTED". No information pertaining to a PROTECTED and/or CLASSIFIED government contract may be released by suppliers, without prior written approval of the individual identified in Block 17 of this form.

The classification assigned to a particular stage in the contractual process does not mean that everything applicable to that stage is to be given the same classification. Every item shall be PROTECTED and/or CLASSIFIED according to its own content. If a supplier is in doubt as to the actual level to be assigned, they should consult with the individual identified in Block 17 of this form.

PART A - CONTRACT INFORMATION

Contract Number (top of the form)

This number must be the same as that found on the requisition and should be the one used when issuing an RFP or contract. This is a unique number (i.e. no two requirements will have the same number). A new SRCL must be used for each new requirement or requisition (e.g. new contract number, new SRCL, new signatures).

1. **Originating Government Department or Organization**

   Form

   Enter the department or client organization name or the prime contractor name for which the work is being performed.

2. **Directorate / Branch**

   This block is used to further identify the area within the department or organization for which the work will be conducted.

3. a) **Subcontract Number**

   If applicable, this number corresponds to the number generated by the Prime Contractor to manage the work with its subcontractor.

   b) **Name and Address of Subcontractor**

   Indicate the full name and address of the Subcontractor if applicable.

4. **Brief Description of Work**

   Provide a brief explanation of the nature of the requirement or work to be performed.

5. a) **Will the supplier require access to Controlled Goods?**

   The Defence Production Act (DPA) defines "Controlled Goods" as certain goods listed in the Export Control List, a regulation made pursuant to the *Export and Import Permits Act* (EIPA). Suppliers who examine, possess, or transfer Controlled Goods within Canada must register in the Controlled Goods Directorate or be exempt from registration. More information may be found at www.cgd.gc.ca.

   b) **Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?**

   The prime contractor and any subcontractors must be certified under the U.S./Canada Joint Certification Program if the work involves access to unclassified military data subject to the provisions of the Technical Data Control Regulations. More information may be found at www.dlis.dla.mil/jcp.

6. **Indicate the type of access required**

   Identify the nature of the work to be performed for this requirement. The user is to select one of the following types:

   a) **Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?**

   The supplier would select this option if they require access to PROTECTED and/or CLASSIFIED information or assets to perform the duties of the requirement.

b) **Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted.**

The supplier would select this option if they require regular access to government premises or a secure work site only. The supplier will not have access to PROTECTED and/or CLASSIFIED information or assets under this option.

c) **Is this a commercial courier or delivery requirement with no overnight storage?**

The supplier would select this option if there is a commercial courier or delivery requirement. The supplier will not be allowed to keep a package overnight. The package must be returned if it cannot be delivered.

7. **Type of information / Release restrictions / Level of information**

Identify the type(s) of information that the supplier may require access to, list any possible release restrictions, and if applicable, provide the level(s) of the information. The user can make multiple selections based on the nature of the work to be performed.

Departments must process SRCLs through PWGSC where:

- contracts that afford access to PROTECTED and/or CLASSIFIED foreign government information and assets;
- contracts that afford foreign contractors access to PROTECTED and/or CLASSIFIED Canadian government information and assets; or
- contracts that afford foreign or Canadian contractors access to PROTECTED and/or CLASSIFIED information and assets as defined in the documents entitled Identifying INFOSEC and INFOSEC Release.

a) **Indicate the type of information that the supplier will be required to access**

Canadian government information and/or assets

If Canadian information and/or assets are identified, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by the Canadian government.

NATO information and/or assets

If NATO information and/or assets are identified, this indicates that as part of this requirement, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by NATO governments. NATO information and/or assets are developed and/or owned by NATO countries and are not to be divulged to any country that is not a NATO member nation. Persons dealing with NATO information and/or assets must hold a NATO security clearance and have the required need-to-know.

Requirements involving CLASSIFIED NATO information must be awarded by PWGSC. PWGSC / CIISD is the Designated Security Authority for industrial security matters in Canada.

Foreign government information and/or assets

If foreign information and/or assets are identified, this requirement will allow access to information and/or assets owned by a country other than Canada.

b) **Release restrictions**

If **Not Releasable** is selected, this indicates that the information and/or assets are for **Canadian Eyes Only (CEO)**. Only Canadian suppliers based in Canada can bid on this type of requirement. NOTE: If Canadian information and/or assets coexists with CEO information and/or assets, the CEO information and/or assets must be stamped **Canadian Eyes Only (CEO)**.

If **No Release Restrictions** is selected, this indicates that access to the information and/or assets are not subject to any restrictions.

If **ALL NATO countries** is selected, bidders for this requirement must be from NATO member countries only.

NOTE: There may be multiple release restrictions associated with a requirement depending on the nature of the work to be performed. In these instances, a security guide should be added to the SRCL clarifying these restrictions. The security guide is normally generated by the organization's project authority and/or security authority.

c) **Level of information**

Using the following chart, indicate the appropriate level of access to information/assets the supplier must have to perform the duties of the requirement.

Form Next Page

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

8. **Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?**

If Yes, the supplier personnel requiring access to COMSEC information or assets must receive a COMSEC briefing. The briefing will be given to the "holder" of the COMSEC information or assets. In the case of a "personnel assigned" type of contract, the customer department will give the briefing. When the supplier is required to receive and store COMSEC information or assets on the supplier's premises, the supplier's COMSEC Custodian will give the COMSEC briefings to the employees requiring access to COMSEC information or assets. If Yes, the Level of sensitivity must be indicated.

9. **Will the supplier require access to extremely sensitive INFOSEC information or assets?**

If Yes, the supplier must provide the Short Title of the material and the Document Number. Access to extremely sensitive INFOSEC information or assets will require that the supplier undergo a Foreign Ownership Control or influence (FOCI) evaluation by CIISD.

PART B - PERSONNEL (SUPPLIER)

10. a) **Personnel security screening level required**

Identify the screening level required for access to the information/assets or client facility. More than one level may be identified depending on the nature of the work. Please note that Site Access screenings are granted for access to specific sites under prior arrangement with the Treasury Board of Canada Secretariat. A Site Access screening only applies to individuals, and it is not linked to any other screening level that may be granted to individuals or organizations.

RELIABILITY STATUS	CONFIDENTIAL	SECRET
TOP SECRET	TOP SECRET (SIGINT)	NATO CONFIDENTIAL
NATO SECRET	COSMIC TOP SECRET	SITE ACCESS

If multiple levels of screening are identified, a Security Classification Guide must be provided.

b) **May unscreened personnel be used for portions of the work?**

Indicating Yes means that portions of the work are not PROTECTED and/or CLASSIFIED and may be performed outside a secure environment by unscreened personnel. The following question must be answered if unscreened personnel will be used:

Will unscreened personnel be escorted?

If No, unscreened personnel may not be allowed access to sensitive work sites and must not have access to PROTECTED and/or CLASSIFIED information and/or assets.

If Yes, unscreened personnel must be escorted by an individual who is cleared to the required level of security in order to ensure there will be no access to PROTECTED and/or CLASSIFIED information and/or assets at the work site.

PART C - SAFEGUARDS (SUPPLIER)

11. **INFORMATION / ASSETS**

a) **Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information and/or assets on its site or premises?**

If Yes, specify the security level of the documents and/or equipment that the supplier will be required to safeguard at their own site or premises using the summary chart.

b) **Will the supplier be required to safeguard COMSEC information or assets?**

If Yes, specify the security level of COMSEC information or assets that the supplier will be required to safeguard at their own site or premises using the summary chart.

PRODUCTION

c) **Will the production (manufacture, repair and/or modification) of PROTECTED and/or CLASSIFIED material and/or equipment occur at the supplier's site or premises?**

Using the summary chart, specify the security level of material and/or equipment that the supplier manufactured, repaired and/or modified and will be required to safeguard at their own site or premises.

INFORMATION TECHNOLOGY (IT)

d) 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?

If Yes, specify the security level in the summary chart. This block details the information and/or data that will be electronically processed or produced and stored on a computer system. The client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document. The supplier must also direct their attention to the following document: Treasury Board of Canada Secretariat - Operational Security Standard: Management of Information Technology Security (MITS).

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

If Yes, the supplier must have their IT system(s) approved. The Client Department must also provide the Connectivity Criteria detailing the conditions and the level of access for the electronic link (usually not higher than PROTECTED B level).

SUMMARY CHART

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier' site(s) or premises.

For users completing the form **online** (via the Internet), the Summary Chart is automatically populated by your responses to previous questions.

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. a) 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 "ecurity Classification".

b) 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 "ecurity Classification"and indicate with attachments (e.g. SECRET with Attachments).

PART D - AUTHORIZATION

13. Organization Project Authority

This block is to be completed and signed by the appropriate project authority within the client department or organization (e.g. the person responsible for this project or the person who has knowledge of the requirement at the client department or organization). This person may on occasion be contacted to clarify information on the form.

14. Organization Security Authority

This block is to be signed by the Departmental Security Officer (DSO) (or delegate) of the department identified in Block 1, or the security official of the prime contractor.

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

A Security Guide or Security Classification Guide is used in conjunction with the SRCL to identify additional security requirements which do not appear in the SRCL, and/or to offer clarification to specific areas of the SRCL.

16. Procurement Officer

This block is to be signed by the procurement officer acting as the contract or subcontract manager.

17. Contracting Security Authority

This block is to be signed by the Contract Security Official. Where PWGSC is the Contract Security Authority, Canadian and International Industrial Security Directorate (CIISD) will complete this block.

ANNEXE J – GUIDE DE CLASSIFICATION DE SÉCURITÉ

LVERS – Guide de classification de sécurité

Nº	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
1.	Tout membre du personnel de l'entrepreneur ayant un accès physique aux centres de données de l'entrepreneur	• Matériel physique • Installations de centres de données • Données telles qu'elles sont stockées sur des supports de sauvegarde locaux de l'entrepreneur	Canada	Fiabilité	Cela concerne le personnel de l'entrepreneur, notamment les ressources chargées de la gestion des installations qui ont physiquement accès au matériel lié aux services infonuagiques dans les centres de données de l'entrepreneur.
2.	Tout membre du personnel de l'entrepreneur ayant un accès logique limité aux services de l'entrepreneur	• Toutes les données opérationnelles • Données telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur	Les deux	Fiabilité	Cela concerne le personnel de l'entrepreneur qui a un accès logique aux données du GC hébergées dans les centres de données de l'entrepreneur et à tout système sensible de même qu'aux données sur les incidents de sécurité. Il peut s'agir de ressources de niveau 1 de type bureau de service.

Nº	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
3.	Tout membre du personnel de l'entrepreneur qui a des rôles privilégiés et un accès logique non restreint à des biens du GC dans les services de l'entrepreneur	• Toutes les données opérationnelles • Données du GC telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur • Biens, dont les données et les justificatifs du GC	Les deux	Secret	Cela concerne le personnel de l'entrepreneur qui a des privilèges élevés assortis d'un accès logique sans restriction aux données du GC hébergées dans les centres de données de l'entrepreneur, à tout système sensible, de même qu'aux données sur les incidents de sécurité. Cela comprend l'accès autorisé par l'intermédiaire d'un processus établi comme les demandes juridiques.

Nº	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
4.	Tout le personnel de l'entrepreneur ayant un accès physique ou logique aux documents de conception détaillés.	• Documents de conception détaillés de la solution de GSTI, notamment les détails de l'application logique et physique, les architectures de la solution d'infrastructure technologique, les contrôles et l'architecture de sécurité, les détails des diagrammes des composantes, le code source, les détails des cas d'utilisation et des schémas des processus d'activités, les détails de l'application, les flux de données et les modèles de données, les conceptions des bases de données, les interfaces de systèmes, les contrôles internes, les plans des essais et les résultats des essais.	Les deux	Fiabilité	Cela concerne surtout l'accès aux documents relatifs à l'architecture et à la conception détaillée.

Nº	Rôle ou fonction	Prévision concernant le type de données consulté	Endroit de l'accès aux données (Canada, autre ou les deux)	Filtrage nécessaire	Détails
5.	Personnel du centre des opérations de sécurité (COS) de l'entrepreneur	• Données telles qu'elles sont stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur	Les deux	Fiabilité	Il s'agit du personnel du COS de l'entreprise.
6.	Soutien de 4e niveau du fabricant d'origine	• Matériel physique • Installations de centres de données • Données telles qu'elles sont stockées sur des supports de sauvegarde locaux de l'entrepreneur	Canada	S. O.	L'entrepreneur aura recours à des sous-traitants pour certains de ses services liés aux opérations du centre de données. L'entrepreneur doit retenir les services de ses sous-traitants comme il se doit en concluant un contrat et en définissant clairement les travaux. Ces ressources n'auront pas un accès physique direct aux données du gouvernement du Canada. Elles peuvent toutefois participer à la résolution de problèmes liés à leur niveau d'expertise avec des ressources de l'entrepreneur qui possèdent les autorisations de sécurité requises et qui ont accès aux données. Si la ressource de soutien de 4e niveau du fabricant d'origine se trouve aux centres de données de l'entrepreneur, elles seront accompagnées par les opérateurs de l'entrepreneur détenteurs d'une attestation de sécurité appropriée. Par exemple : Assistance avec l'équipement réseau, assistance avec le CVC.

En plus des rôles susmentionnés, voici les rôles associés aux services relatifs à la transition et à la migration :

Domaine	Rôle	Responsabilités	Accès	Emplacement (autres que pour les réunions)	Exigences en matière de cote de sécurité du personnel (hypothèse de travail)
Gouvernance	Cadre responsable de l'exécution, gestionnaire de programmes ou gestionnaire de projets	Gouvernance ou gestion du projet	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Peut participer à des réunions au cours desquelles les données de configuration des systèmes protégés sont affichées ou discutées Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Fiabilité ou l'équivalent
Gestion des services de TI (conseils opérationnels)	Architecte et expert-conseil	Animation d'ateliers, création de documents (plans de service, suivi, etc.)	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Peut participer à des réunions au cours desquelles les données de configuration des systèmes protégés sont affichées ou discutées Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Fiabilité ou l'équivalent
Adoption des utilisateurs finaux et gestion du changement	Architecte et expert-conseil	Animation d'ateliers, création de documents, autres activités de gestion du changement requises pour le passage à Office 365	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Peut participer à des réunions au cours desquelles les données de configuration des systèmes protégés sont affichées ou discutées Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Aucun accès (suppose qu'il est escorté lorsqu'il se trouve dans les locaux du partenaire)

Intégration à Microsoft Exchange Online	Architecte	Supervision technique du projet, des conseils généraux, des documents et de l'examen des produits livrables	Aucun accès aux systèmes physiques (ne touche pas aux claviers) Accès possible à des documents du gouvernement du Canada de diverses classifications Aucun accès aux données des utilisateurs	Sur place, S.O. Accès à distance, Oui	Fiabilité ou l'équivalent
	Expert-conseil en déploiement	**Phase de remédiation** – Travailler de concert avec les experts en la matière de SPC et du gouvernement du Canada pour remédier à tout problème avec Active Directory local, la configuration en suspens d'Exchange Online local, l'état de préparation du réseau et des clients (bureau). **Phase de mise en service** – Travailler de concert avec les experts en la matière de SPC et du gouvernement du Canada pour déployer les différents composants (AAD Connect pour la synchronisation, l'établissement de la Fédération pour l'authentification, l'activation de l'accès conditionnel, Azure Information Protection et configuration d'Exchange Online par le locataire)	Accès aux systèmes (location d'Office 365, Active Directory et Exchange versions locales) Accès aux documents du gouvernement du Canada, au besoin, pour aider à la remédiation et à la mise en service Accès potentiel aux données des utilisateurs	Sur place (si SPC l'exige) Accès à distance, Oui	Fiabilité ou équivalent (suppose que SPC gère les environnements indépendamment de la migration des courriels des partenaires)

	Expert-conseil en migration	Migration des données de YES vers Exchange Online, y compris la création des projets de migration. Assistance après la migration pour aider les bureaux de service de SPC et des partenaires	Accès aux systèmes (location d'Office 365 en tant qu'administrateur général, Active Directory et Exchange local, YES en tant que direction de l'organisation ou direction des destinataires) Accès ou accès possible aux données (accès complet à la boîte de réception dans YES et Exchange Online) Accès aux documents du gouvernement du Canada, au besoin, pour effectuer les migrations	Sur place (si SPC l'exige) Accès à distance, Oui	Secret ou équivalent

ANNEXE K – ACCORD DE NON-DIVULGATION DE SPAC REALITF À L'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

Entente de non-divulgation de SPAC

Note aux fournisseurs: Veuillez noter que cet accord de non-divulgation couvre uniquement les exigences de SCI en vertu de la section 3.5: Exigences relatives à l'intégrité de la chaîne d'approvisionnement. Les fournisseurs seront invités à conclure un accord de confidentialité bilatéral (NDA) avec la CCC une fois qu'ils auront intégré le **programme d'évaluation de la sécurité des TI des logiciels-services**. Pour plus d'informations sur le programme d'évaluation de la sécurité des TI des logiciels-services : Processus d'intégration, veuillez-vous reporter à l'annexe L ci-dessous.

En soumettant une réponse, le soumissionnaire accepte les modalités de l'entente de non- divulgation ci-dessous (**l'« entente de non-divulgation »**).

Les sous-sections suivantes s'appliquent aux situations où **l'entrepreneur/sous-traitant** confirme qu'il a accès aux données du Canada, en prend soin et contrôle.

1. Le soumissionnaire s'engage à préserver la confidentialité de l'information qu'il reçoit du Canada concernant l'évaluation par le Canada de son processus d'évaluation de l'information sur la sécurité de la chaîne d'approvisionnement (l'« information de nature délicate »), y compris, sans toutefois s'y limiter, l'aspect du processus d'évaluation de l'information sur la sécurité de la chaîne d'approvisionnement qui préoccupe le Canada et les raisons qui expliquent ces préoccupations.

2. L'information de nature délicate 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 classifiés, exclusifs ou de nature délicate.

3. Le soumissionnaire s'engage à ne pas reproduire, copier, divulguer diffuser ou publier, en tout ou en partie, de quelque manière ou forme que ce soit, de l'information de nature délicate à une autre personne que ses employés qui détiennent une cote de sécurité correspondant au niveau de sensibilité de l'information consultée, sans avoir reçu au préalable le consentement écrit de l'autorité contractante. Le soumissionnaire s'engage à aviser l'autorité contractante si des personnes autres que celles autorisées par le présent article consultent à tout moment de l'information de nature délicate.

4. Toute l'information de nature délicate demeure la propriété du Canada et doit être retournée à l'autorité contractante ou détruite à la demande de cette dernière dans les 30 jours suivant cette demande.

5. Le soumissionnaire est conscient qu'un manquement à cette entente de non-divulgation pourrait entraîner sa disqualification à l'étape de la demande de propositions, ou une résiliation immédiate du marché subséquent. Le soumissionnaire 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.

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

ANNEXE L – PROGRAMME D'ÉVALUATION DE LA SÉCURITÉ DES TI DES LOGICIELS-SERVICES : PROCESSUS D'INTÉGRATION

1. Présenter une soumission au Programme d'évaluation de la sécurité des TI des logiciels-services

(a) Pour présenter une soumission au Programme, le soumissionnaire doit suivre les étapes suivantes :

(ii) Communiquer avec le Centre d'appel du CCC à l'adresse contact@cyber.gc.ca, au 613-949-7048 ou au 1-833-CYBER-88.

(iii) Se préparer à conclure une entente de non-divulgation bilatérale avec le CCC.

(iv) Fournir tous les documents nécessaires à l'évaluation au Centre de contact du CCC. Lorsqu'il fournit des documents, il devrait utiliser les identifiants du programme de cryptage PGP (Pretty Good Privacy) pour chiffrer les documents. Voir la section 2, Clé PGP, pour obtenir une copie de ladite clé.

2. Clé PGP

(a) Envoyer un courriel ou téléphoner au Centre de contact du CCC pour demander la clé publique requise pour la clé PGP du CCC. Utiliser cette clé pour chiffrer les documents sensibles à soumettre dans le cadre du Programme d'évaluation de la sécurité des TI du PSC.

3. Personnes-ressources et assistance

(a) Le centre d'appel du CCC est le point de contact pour toutes les soumissions de documents liés au programme d'évaluation de la sécurité des TI des logiciels-services. Le responsable de l'équipe d'évaluation des logiciels-services, ou un délégué autorisé, a accès à cette boîte de réception. Tous les documents d'évaluation de la sécurité des TI du PSC seront gérés et protégés au moyen du chiffrement PGP pendant leur transmission (voir la section 2 pour obtenir une copie de la clé PGP). Tous les documents seront également traités et gérés conformément aux politiques de gestion de l'information du CCC.

Centre d'appel du CCC
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Formulaire 1 – Formulaire de présentation des soumissions		
Dénomination sociale du fournisseur		
Représentant autorisé du fournisseur aux fins de l'évaluation (p. ex., pour des précisions)	Nom	
	Titre	
	Adresse	
	Téléphone	
	Télécopieur	
	Courriel	
Numéro d'entreprise-approvisionnement (NEA) du fournisseur *[voir la clause 2008 des instructions uniformisées]*		
Liste des membres du conseil d'administration [Les fournisseurs sont priés d'indiquer les noms de l'ensemble des membres du conseil d'administration dans l'entreprise.]	Nom :_____ Nom :_____ Nom :_____	
Compétence juridique relative au marché Province du Canada choisie par le fournisseur qui aura la compétence juridique pour l'arrangement en matière d'approvisionnement et tout marché subséquent (contrats) (s'il s'agit d'une autre province que l'Ontario, au Canada).		
Nombre d'équivalents temps plein (ETP) (On demande aux fournisseurs d'indiquer le nombre total de postes équivalents à temps plein qu'ils devront créer et conserver si le contrat leur était attribué. Ces renseignements ne sont demandés qu'à titre indicatif et ne seront pas évalués.)		
Niveau d'attestation de sécurité du fournisseur *(indiquer le niveau et la date d'attribution)*		
Entreprises autochtones (Les fournisseurs doivent indiquer s'ils répondent aux exigences précisées dans le Programme de marchés réservés aux entreprises autochtones.)		
Petites et moyennes entreprises canadiennes *(Les fournisseurs doivent indiquer s'ils répondent à la définition d'une petite et moyenne entreprise canadienne [100 à 500 employés = moyenne; 10 à 100 = petite; 1 à 10 = très petite].)*		
Entreprise canadienne *(Les fournisseurs doivent indiquer s'ils sont canadiens.)*		
Entreprise écologique		

[Les fournisseurs doivent indiquer si leurs installations fonctionnent à l'aide d'un système de gestion de l'environnement (SEG) qui a été certifié conforme à la norme internationale ISO 14001.]	
Approvisionnement écologique *Les fournisseurs doivent s'engager à fournir des produits qui respectent l'environnement.)*	
Attestation du fournisseur que les Solutions de logiciels-services sont disponibles dans le commerce [Les fournisseurs doivent certifier que toutes les Solutions de logiciels-services proposées en réponse à cette DAMA sont disponibles dans le commerce, notamment chaque composant logiciel qui ne requiert aucune recherche ou développement supplémentaire, et qu'ils font partie intégrante d'une gamme de produits existante dont le fonctionnement est éprouvé (ils n'ont pas simplement fait l'objet d'essais en laboratoire ou dans un environnement expérimental). Si une Solutions de proposée est une extension entièrement compatible d'une gamme de produits éprouvés, elle doit avoir été annoncée publiquement au plus tard à la date à laquelle l'soumission est soumis. En présentant une soumission, le fournisseur atteste que toutes les Solutions de logiciels-services proposées sont disponibles dans le commerce.]	
En apposant ma signature ci-dessous, je confirme, au nom du fournisseur, que j'ai lu la demande d'arrangement en matière d'approvisionnement en entier, y compris les documents qui y sont incorporés par renvoi, et j'atteste que : 1. le soumissionnaire considère qu'il a les compétences et que ses produits sont en mesure de satisfaire aux exigences obligatoires décrites dans la DAMA; 2. tous les renseignements fournis en réponse à la DAMA sont complets, véridiques et exacts; 3. si le fournisseur conclut une soumission avec le Canada et qu'il se voit attribuer des marchés, il se conformera à toutes les modalités énoncées dans les clauses du marché subséquent et comprises dans la DAMA.	
Signature du représentant autorisé du fournisseur	

Formulaire 2 - Formulaire d'attestation de l'éditeur de logiciels-services

(à remplir lorsque le fournisseur est l'éditeur de logiciels)

Le fournisseur atteste qu'il est l'éditeur des logiciels et de tous les produits logiciels suivants et qu'il a les droits requis pour accorder les licences conformément aux modalités de l'AMA au Canada :

_____

_____

_____

(Les fournisseurs doivent ajouter ou supprimer des lignes au besoin.)

Nom de l'éditeur de logiciels-services (ELS) _____

Signature du signataire autorisé de l'ELS _____

Nom du signataire autorisé de l'ELS _____

Titre du signataire autorisé de l'ELS _____

Adresse du signataire autorisé de l'ELS _____

Téléphone du signataire autorisé de l'ELS _____

Courriel du signataire autorisé de l'ELS _____

Date _____

Numéro de la DAMA _____

Formulaire 3 - Formulaire d'autorisation de l'éditeur de logiciels-services

(à remplir lorsque le fournisseur n'est pas l'éditeur de logiciels)

Ce formulaire vise à confirmer que l'éditeur de logiciels-services nommé ci-dessous comprend et atteste que [inscrire le nom du revendeur] a présenté une soumission en réponse à la demande d'arrangement en matière d'approvisionnement émise par SPAC le [inscrire la date _____], numéro de référence _____. L'éditeur de logiciels confirme par la présente que

(i) le fournisseur nommé ci-dessous est autorisé à fournir les Solutions de logiciels-services décrites ci-dessous ou jointes aux présentes, par l'entremise de son AMA;

(ii) l'éditeur de logiciels-services accepte d'accorder toutes les licences qui doivent être acquises dans le cadre de l'AMA, conformément aux modalités du contrat subséquent établies dans l'AMA.

L'éditeur de logiciels-services reconnaît que le fournisseur a proposé à l'État les logiciels exclusifs de l'entreprise suivants en réponse à la DAMA.
[*Inscrire tous les logiciels exclusifs faisant l'objet d'une licence qui sont proposés par le fournisseur*.]

_____
_____
_____
_____
_____
_____
(Les fournisseurs doivent ajouter ou supprimer des lignes au besoin.)

Nom de l'éditeur de logiciels-services _____

Signature du fondé de signature de l'éditeur de logiciels-services _____

Nom en caractères d'imprimerie du fondé de signature

de l'éditeur de logiciels-services _____

Titre en caractères d'imprimerie du fondé de signature

de l'éditeur de logiciels-services _____

Adresse du fondé de signature de l'éditeur de logiciels-services _____

Nº de téléphone du fondé de signature de l'éditeur de

Logiciels-services _____

Nº de télécopieur du fondé de signature de l'éditeur de

Logiciels _____

Date de signature _____

Numéro de la demande de soumissions _____

Nom du fournisseur _____

Formulaire 4 - Attestation aux fins du Programme de marchés réservés aux entreprises autochtones

Le fournisseur :
(i) atteste qu'il respecte, et continuera de respecter, pendant toute la durée de l'arrangement en matière d'approvisionnement, les exigences décrites dans l'annexe 9.4, Exigences relatives au Programme de marchés réservés aux entreprises autochtones, du Guide des approvisionnements (https://achatsetventes.gc.ca)
(ii) convient que tout sous-traitant auquel il aura recours dans le cadre de l'arrangement en matière d'approvisionnement doit respecter les exigences de l'annexe mentionnée précédemment;
(iii) accepter de fournir au Canada, immédiatement sur demande, une preuve de la conformité de sous-traitant aux exigences décrites dans l'annexe mentionnée précédemment.

Le fournisseur doit cocher l'énoncé qui s'applique ci-dessous :
( ) Le fournisseur est une entreprise autochtone à propriétaire unique, une bande, une société à responsabilité limitée, une coopérative, une société de personnes ou un organisme sans but lucratif. OU
( ) Le fournisseur est une coentreprise comprenant deux ou plus de deux entreprises autochtones ou une coentreprise entre une entreprise autochtone et une entreprise non autochtone*.

Le fournisseur doit cocher l'énoncé qui s'applique ci-dessous :
( ) L'entreprise autochtone a moins de six employés à plein temps.
OU
( ) L'entreprise autochtone a six employés à plein temps ou plus.

L'entreprise autochtone compte six employés à temps plein ou plus. À la demande du Canada, le fournisseur doit présenter tout renseignement et toute preuve justifiant la présente attestation. Le fournisseur doit s'assurer que cette preuve soit disponible pour examen par un représentant du Canada durant les heures normales de travail, lequel représentant du Canada pourra tirer des copies ou des extraits de cette preuve. Le fournisseur fournira toutes les installations nécessaires à ces vérifications.

En déposant une soumission, le fournisseur atteste que l'information fournie par le fournisseur pour répondre aux exigences plus haut est exacte et complète.

Nom du fournisseur _____
Signature du signataire autorisé du fournisseur _____
Nom en caractères d'imprimerie du signataire autorisé du fournisseur _____
Titre en caractères d'imprimerie du signataire autorisé du fournisseur _____
Adresse du signataire autorisé du fournisseur _____
Courriel du signataire autorisé du fournisseur _____
Date de signature _____
Numéro de la DAMA _____

***Coentreprise autochtone** : Une coentreprise composée de deux entreprises autochtones ou plus, ou composée d'entreprises autochtones et d'entreprises non autochtones, pourvu que la ou les entreprises autochtones détiennent au moins 51 p. 100 des intérêts et du contrôle de la coentreprise. La coentreprise doit respecter l'exigence en matière de contenu autochtone à l'effet que 33 % de la valeur des travaux dans le cadre d'un contrat doit être exécuté par la ou les entreprises autochtones.

Formulaire 5 - List de vérification de l'exhaustivité de la soumission

NOM DU FOURNISSEUR: _____

1) Soumission technique, Soumission financier, Attestations et information sur l'intégrité de la chaîne d'approvisionnement:

- *a)* ☐ Soumission technique
- *b)* ☐ Soumission financière
- *c)* ☐ Attestations
- *d)* ☐ Information sur l'intégrité de la chaîne d'approvisionnement

FORMULAIRES:

1) Formulaire de présentation des arrangements (DAMA Formulaire 1)

- *a)* ☐ Dénomination sociale du fournisseur
- *b)* ☐ Représentant autorisé du fournisseur aux fins de l'évaluation
- *c)* ☐ Numéro d'entreprise-approvisionnement (NEA) du fournisseur
- *d)* ☐ Liste des membres du conseil d`administration
- *e)* ☐ Compétence juridique relative au marché
- *f)* ☐ Nombre d`équivalents temps plein (ETP)
- *g)* ☐ Niveau d`attestation de sécurité du fournisseur et ses revendeur
- *h)* ☐ Entreprises autochtones
- *i)* ☐ Petites et moyennes entreprises canadiennes
- *j)* ☐ Entreprise canadienne
- *k)* ☐ Entreprise écologique
- *l)* ☐ Approvisionnement écologique
- *m)* ☐ Attestation du fournisseur que le système est disponible dans le commerce
- *n)* ☐ Signature du représentant autorisé du fournisseur

2) Formulaire d'attestation de l'éditeur de logiciels (à remplir lorsque le fournisseur est l'éditeur de logiciels) *(Formulaire 2)* ☐

3) Formulaire d'autorisation de l'éditeur de logiciels (à remplir lorsque le fournisseur n'est pas l'éditeur de logiciels) *(Formulaire 3)* ☐

4) Attestation aux fins du Programme de marchés réservés aux entreprises autochtones ☐
(Obligatoire lorsque le fournisseur est une entreprises autochtone et souhaite être identifié comme tel)
(Formulaire 5)

5) Formulaire de soumission SCI (Formulaire 6) ☐

ANNEXES:

Annexe A – Exigences de qualification ☐

Annexe C - Catalogue de Solutions de logiciels-services et prix plafond ☐

- *a)* ☐ Doit être soumis au moyen du format défini à l'annexe C.
- *b)* ☐ **Nº d'article**, inclus pour chaque produit.

c) ☐ **Nº de pièce de l'éditeur de logiciel**. *(*le numéro de pièce utilisé par l'éditeur de logiciels pour le produit)*)*

d) ☐ **Nom de la Solution de logiciels-services** *(*le nom utilisé par l'éditeur de logiciels pour le produit. *Si une année de maintenance et de soutien est comprise dans les achats des nouvelles licences, veuillez l'indiquer dans le nom du produit. En ce qui a trait aux articles génériques de maintenance et de soutien, assurez-vous de détailler la manière dont les coûts connexes sont calculés, p. ex., 15 % du prix plafond)*

e) ☐ **Nom de l'éditeur** *(*le nom de l'éditeur de logiciels qui crée la Solution de logiciels-services*)*

f) ☐ **Nom du fournisseur de services infonuagiques** (le nom du fournisseur de services infonuagiques utilisés pour fournir les Solutions de logiciels-services)

g) ☐ **Prix unitaire plafond** *(requis pour chaque article***)**

h) ☐ **Unité de mesure (**entrez l'unité de mesure pour le logiciel-service, telle que «par utilisateur», «par entité», etc. et abonnement, durée)

i) ☐ **Remise en pourcentage applicable** *(*entrez le pourcentage de réduction qui sera appliqué aux prix unitaires plafonds pour la durée de l'arrangement)

j) ☐ **Langues** disponibles *(*la langue du logiciel, p. ex, français, anglais *et/out autre)*

k) ☐ **Information sur les Solutions de logiciels-services** *(*site Web affichant cette information*)*

l) ☐ **Mots-clés / tags (**entrez des mots-clés associés à la solution logiciels-services qui aideront les clients à rechercher et à trouver facilement des solutions logiciels-services qui répondent à leurs besoins)

Annexe D – Accords sur les niveaux de service (ANS)

Accords sur les niveaux de service (ANS) :

a) ☐	Disponibilité – rendement	No de PAGE ____
b) ☐	Définition de temps d'arrêt – prévu et imprévu	No de PAGE ____
c) ☐	Crédits de service – éléments déclencheurs et calcul	No de PAGE ____
d) ☐	Disponibilité des services de soutien	No de PAGE ____
e) ☐	Libre-service, base de connaissances, tutoriels en ligne	No de PAGE ____
f) ☐	Erreurs : définitions des degrés de gravité	No de PAGE ____
g) ☐	Temps moyen de réponse et de réparation	No de PAGE ____
h) ☐	Acheminement au palier hiérarchique approprié et procédure	No de PAGE ____
i) ☐	Disponibilité d'un système de reprise après sinistre	No de PAGE ____

Nom du représentant autorisé du fournisseur : _____

Signature du représentant autorisé du fournisseur (date): _____

Formulaire à l'intention des fournisseurs

PARTIE A - INFORMATION SUR LE SOUMISSIONNAIRE	
Nom de la soumission :	
Date de soumission :	
Numéro de la soumission :	
Nom du soumissionnaire :	
Numéro DUNS du soumissionnaire :	

PARTIE B - LISTE DES PRODUITS
CLIQUEZ ICI POUR AJOUTER DES ÉLÉMENTS

PARTIE C - INFORMATION SUR LA PROPRIÉTÉ
CLIQUEZ ICI POUR AJOUTER DES ÉLÉMENTS

B - Liste des produits

Exemple d'une liste de prod

Article	Nom du FEO	Numéro DUNS du FE	Nom du produit	Modèle / Version	URL du produit	Information sur les vulnérabi	Nom du fourniss	Numéro DUNS du fourni	URL du fournisseur	Info supplémentaire
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										

Government of Canada / Gouvernement du Canada

TLP:AMBER
une fois rempli

C - Information sur la propriété

F - Exemple d'information sur la propriété

Remplissez cette partie uniquement pour les FEO et les fournisseurs qui n'ont pas de numéro DUNS.

Article	Nom du FEO ou du fournis	Propriétaires	Investisseurs	Membres de la directio	Pays / Nationalité	Lien vers le site Web de l'entre
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

D - Aide

Champ	Guide	Remarques
Formulaire 2 sur la SCSI		
Nom de la soumission	Si ce champ ne s'applique pas, laissez-le vide. Autrement, inscrivez le nom associé à l'approvisionnement de produits multiples (p. ex. WTD Print, Projet Telesto).	
Date de soumission	AAAA-MM-JJ	

Numéro de la soumission	Si ce champ ne s'applique pas, laissez-le vide. Autrement, inscrivez le numéro de la soumission liée à l'approvisionnement de produits multiples.	
Nom du soumissionnaire	Si ce champ ne s'applique pas, laissez-le vide. Inscrivez le nom de l'organisation qui se charge de présenter la soumission.	
Numéro DUNS du soumissionnaire	Si ce champ ne s'applique pas, laissez-le vide. Inscrivez le numéro DUNS de l'organisation qui se charge de présenter la soumission. Si l'organisation n'a pas de numéro DUNS ou que vous n'arrivez pas à le trouver, veuillez remplir la partie C : « Information sur la propriété ». L'information sur la propriété concerne les 5 principaux propriétaires et investisseurs de l'entreprise, en fonction du pourcentage. Le nom des investisseurs et propriétaires doit correspondre à celui qui paraît dans les documents d'investissement ou de propriété de l'entreprise en question.	

LISTE DES PRODUITS DE TI

Nom du FEO	Inscrivez le nom du fabricant d'équipement d'origine (FEO) du produit commandé.	**Seuls les produits admissibles à l'évaluation de l'intégrité de la chaîne d'approvisionnement doivent paraître dans cette liste. Ne tenez pas compte des câbles d'alimentation, des panneaux de remplissage de bâtis, des coûts liés à la garantie, des frais d'expédition et d'autres éléments non liés aux technologies de l'information et des communications (TIC). Si ce type de produit est inscrit dans le formulaire, ce dernier vous sera renvoyé et aucune évaluation ne sera réalisée.** **Tout produit inscrit dans le formulaire doit respecter la définition de « produit », c'est-à-dire « tout matériel qui fonctionne dans la couche de liaison de données du modèle OSI [Open Systems Interconnection] (couche 2) ou supérieure, tout logiciel et tout appareil technologique en milieu de travail ».**
Numéro DUNS du FEO	Inscrivez le numéro DUNS du FEO. Le numéro *Data Universal Numbering System* (DUNS) est un identifiant numérique unique de neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme internationale qui sert à établir la cote de crédit d'une entreprise. Si l'organisation n'a pas de numéro DUNS ou que vous n'arrivez pas à le trouver, veuillez remplir la partie C : « Information sur la propriété ». L'information sur la propriété concerne les 5 principaux propriétaires et investisseurs de l'entreprise, en fonction du pourcentage. Le nom des investisseurs et propriétaires doit correspondre à celui qui paraît dans les documents d'investissement ou de propriété de l'entreprise en question.	
Nom du produit	Inscrivez le nom attribué par le FEO au produit.	
Numéro de modèle	Inscrivez le numéro de modèle ou de version attribué par le FEO au produit.	
URL du produit	Inscrivez l'adresse URL de la page Web du FEO où se trouve le produit.	

Information sur les vulnérabilités	Inscrivez l'information sur les 5 derniers problèmes de sécurité qui ont touché le produit. Si le FEO affiche cette information sur le site Web des vulnérabilités et expositions courantes (CVE), inscrivez les numéros CVE et **séparez-les par un point-virgule (;)**. Si le FEO n'affiche pas cette information sur le site Web des CVE, vous devrez communiquer directement avec lui pour obtenir les renseignements sur les vulnérabilités informatiques, puis les transmettre au Centre canadien pour la cybersécurité. Si cette situation s'applique à un produit particulier, inscrivez « voir l'information ci-jointe » dans le ou les champs pertinents.	
Nom du fournisseur	Inscrivez le nom du fournisseur du produit commandé (c'est-à-dire les sous-traitants, les revendeurs, les distributeurs, les entités chargées du traitement des données, etc.). Il s'agit de toute entité commerciale appelée à fournir des produits ou services dans le but de remplir les exigences de la soumission. **Dans le cas d'un arrangement en matière d'approvisionnement relatif à l'infrastructure matérielle (AAIM), d'une offre à commandes principale et**	

	nationale (OCPN), ou d'autres listes, le champ peut rester vide.	
Numéro DUNS du fournisseur	Inscrivez le numéro DUNS du fournisseur. Le numéro Data Universal Numbering System (DUNS) est un identifiant numérique unique de neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme internationale qui sert à établir la cote de crédit d'une entreprise. Si l'organisation n'a pas de numéro DUNS ou que vous n'arrivez pas à le trouver, veuillez remplir la « partie C - Information sur la propriété ». L'information sur la propriété concerne les 5 principaux propriétaires et investisseurs de l'entreprise, en fonction du pourcentage. Le nom des investisseurs et propriétaires doit correspondre à celui qui paraît dans les documents d'investissement ou de propriété de l'entreprise en question. **Dans le cas d'un AAIM, d'une OCPN, ou**	

	d'autres listes, le champ peut rester vide.	
URL du fournisseur	Inscrivez l'adresse URL de la page Web du fournisseur où se trouve le produit. **Dans le cas d'un AAIM, d'une OCPN, ou d'autres listes, le champ peut rester vide.**	
INFORMATION SUR LA PROPRIÉTÉ		
Nom du FEO ou du fournisseur	Inscrivez le nom du fabricant d'équipement d'origine (FEO) du produit commandé ou le nom du fournisseur (c'est-à-dire les sous-traitants, les revendeurs, les distributeurs, les entités chargées du traitement des données, etc.) du produit ou service commandé.	**Vous devez remplir les champs de la partie C : « Information sur la propriété » uniquement si vous n'êtes pas en mesure de fournir le numéro DUNS du FEO ou du fournisseur.**

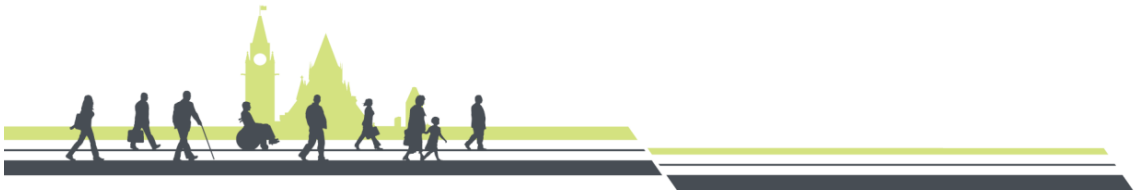
Propriétaires	Il s'agit des 5 principaux propriétaires du FEO ou du fournisseur, en fonction du pourcentage. Le nom des propriétaires doit correspondre à celui qui paraît dans les documents de propriété de l'entreprise en question.	**Chaque ligne et chaque cellule du tableau doit comporter un seul élément d'information.**
Investisseurs	Il s'agit des 5 principaux investisseurs du FEO ou du fournisseur, en fonction du pourcentage. Le nom des investisseurs doit correspondre à celui qui paraît dans les documents d'investissement de l'entreprise en question.	
Membres de la direction	Inscrivez le nom des membres de la direction et du conseil d'administration de l'entreprise en question.	
Pays / Nationalité	Il s'agit du pays de nationalité de la personne ou du pays où l'entité commerciale est enregistrée.	
Lien vers le site Web de l'entreprise	Pour chaque FEO, fournisseur, propriétaire, investisseur ou membre de la direction inscrit dans le tableau, donnez l'adresse URI / URL vers l'information à l'appui des renseignements fournis dans chacun des champs.	

E - Exemple d'une liste de produits d

Article	Nom du FEO	Numéro DUNS du FEO	Nom du produit	Modèle / Version	URL du produit	Information sur les vulnérabilités	Nom du fournisseur	Numéro DUNS du fournisseur	URL du fournisseur	INFORMATION ADDITIONNELLE
1	Cisco	137660665	1941	K9	https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW				Exemple d'un AAIM
2	Cisco	137660665	1941	K9	https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW	LocalHardware	4567891234	https://www.lhinc.ca	Exemple d'arrangement autre qu'un AAIM ou de l'approvisionnement d'un seul produit

F - Exemple d'information sur la propri

Nom du FEO ou du fournisseur	Propriétaires	Investisseurs	Membres de la direction	Pays / Nationalité	Lien vers le site Web de l'entreprise
newkid software	M. A (60 %)			Canada	newkid.com/profiles/mra
newkid software	Mme B (30 %)			France	newkid.com/profiles/msb
newkid software	M. C (10 %)			États-Unis	newkid.com/profiles/mrc
newkid software		Entreprise A (10 %)		États-Unis	newkid.com/investor_relations/filings
newkid software		Entreprise B (9 %)		Chine	newkid.com/investor_relations/filings
newkid software		Entreprise C (8 %)		Corée du Sud	newkid.com/investor_relations/filings
newkid software		Entreprise D (5 %)		Canada	newkid.com/investor_relations/filings
newkid software		Entreprise E (5 %)		Espagne	newkid.com/investor_relations/filings
newkid software			M. A	Canada	newkid.com/profiles/mra
newkid software			Mme B	France	newkid.com/profiles/msb
newkid software			M. Q	Portugal	newkid.com/profiles/mrq



ANNEXE F – CLAUSES DU CONTRAT SUBSÉQUENT RALATIVES AU LOGICIEL-SERVICES (SAAS)

DE LA DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA) CONCERNANT LES SOLUTIONS DE LOGICIELS-SERVICES (INFONUAGIQUES GC)

TABLE DES MATIÈRES

Solution de logiciel-service (SaaS)

Clauses du contrat subséquent

Note aux fournisseurs : *La présente version préliminaire des clauses du contrat subséquent vise à constituer le fondement de tous les contrats subséquents à la demande d'arrangements en matière d'approvisionnement (DAMA). Sauf dans les cas indiqués expressément dans les présentes clauses du contrat subséquent, l'acceptation par les fournisseurs de toutes les clauses est une exigence obligatoire de la présente DAMA.*

Aucune modification ou autre condition incluse dans la soumission ne s'appliquera au contrat subséquent, même si la proposition fait partie dudit contrat.

Tout fournisseur présentant une soumission qui comprend des énoncés qui laissent entendre que la soumission est fonction de l'apport de modifications aux présentes clauses du contrat subséquent (y compris tous les documents intégrés par renvoi) ou qui comprend des modalités et conditions qui prétendent remplacer ces clauses, sera jugé non recevable. Par conséquent, les fournisseurs qui ont des préoccupations au sujet des présentes clauses du contrat subséquent devraient les communiquer conformément aux dispositions relatives à la présente DAMA.

Si une soumission soulève d'autres questions de droit, le Canada se réserve le droit d'y répondre dans tout contrat subséquent à la présente DAMA. Le fournisseur peut retirer sa soumission s'il juge que les dispositions additionnelles sont inacceptables.

Le présent contrat est conclu le [DATE DU CONTRAT] entre [NOM DE L'ENTREPRENEUR] (l'« entrepreneur ») et [ENTITÉ DU GOUVERNEMENT DU CANADA] (le « Canada »).

Ce contrat est émis conformément à l'arrangement en matière d'approvisionnement (AMA) [numéro d'AMA de la page 1]. Les conditions générales énoncées dans le contrat de sécurité font partie intégrante de ce contrat.

1. Exigence

1.1 L'entrepreneur convient de fournir les services et d'exécuter les travaux décrits dans le contrat conformément aux spécifications et aux prix énoncés dans la soumission en matière d'approvisionnement, à l'annexe C – Catalogue de Solutions de logiciels-services et Prix Plafonds, ou dans la soumission de l'entrepreneur, le cas échéant.

1.2 **Services**. L'entrepreneur accepte de fournir les services suivants :

(a) Fournir les services identifiés à l'appendice A, qui inclut au minimum:

(i) accorder des droits d'utilisation sur les applications logicielles («solution (s)») identifiées au appendice fournies à une ou à plusieurs solutions fournies ou hébergées par l'entrepreneur;

(ii) fournir la documentation de la solution;

(iii) assurer la maintenance, la mise à niveau et la mise à jour de la ou des solutions;

(iv) gérer les incidents et les défauts pour s'assurer que la ou les solutions fonctionnent aux niveaux de service applicables;

(v) fournir des services d'infrastructure de technologie de l'information accessoires et additionnelle requis.

(vi) Services d'infrastructure requis pour livrer la solution.

1.3 Services professionnels. L'entrepreneur s'engage à fournir les services professionnels suivants, sur demande du Canada, en utilisant le processus d'autorisation de tâches :

(a) la trousse de formation et de services Guide de démarrage rapide (« GDR »);

(b) les services de mise en œuvre;

(c) les services de formation;

(d) les services d'épuration, de migration et de transition des données;

(e) les services consultatifs.

1.4 Client. Conformément au contrat, le « client » est _____.

1.5 Réorganisation des clients. Toute forme de restructuration ou de réaménagement du client n'aura aucune incidence sur l'obligation de l'entrepreneur en ce qui a trait aux travaux et à la prestation des services (et ne donnera pas lieu non plus au paiement d'honoraires additionnels). Le Canada peut désigner une autorité contractante ou un responsable technique de remplacement.

2. Durée, résiliation et renouvellement automatique

Remarque: Cet article sera ajusté à l'attribution du contrat pour inclure les clauses de durée déterminée ou de durée d'abonnement, conformément aux conditions commerciales soumises par l'entrepreneur à l'annexe D, Accords sur les niveaux de service ou à la soumission gagnante.

2.1 Durée du contrat. La durée du contrat comprend la période pendant laquelle l'entrepreneur est tenu de fournir les services et d'effectuer les travaux.

2.2 Durée initiale. Le présent contrat entre en vigueur à la date d'attribution du contrat et se termine le [DATE D'EXPIRATION/nombre d'années].

2.3 Périodes d'option. Le Canada peut exercer l'option irrévocable à étendre la durée du contrat jusqu'à la période [série d'extension] [période d'extension] en appliquant les mêmes termes et conditions. L'entrepreneur convient que pendant l'extension de période du contrat, il sera paye conformément aux provisions identifiées dans la section « Paiement de base ». Le Canada peut exercer cette option(s) à n'importe quel moment en envoyant un avis écrit à l'entrepreneur au moins 90 jours civils avant la date d'expiration du contrat. L'option ne pourra être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

2.4 Retrait de renouvellement automatique. Par la présente, le Canada avise l'entrepreneur qu'il choisit de ne pas renouveler automatiquement la durée de l'obligation. L'entrepreneur accuse réception de l'avis et déclare que le présent contrat ne sera valide que jusqu'à la fin de la période du contrat, tel que défini ci-dessus.

2.5 Changement en matière de consommation. L'entrepreneur accorde au Canada l'option irrévocable d'augmenter ou de réduire sa consommation de produits ou de services de logiciel-service décrits à l'annexe A. Si la consommation d'un produit ou d'un service de logiciel-service par le Canada est réduite, l'entrepreneur convient qu'aucune pénalité ou augmentation du prix unitaire ne s'applique en conséquence.

OU

2.1 Durée de l'abonnement

(a) ***Services par abonnement.*** *Le Canada reconnaît que l'entrepreneur peut fournir les services par abonnement, sans avoir la durée du contrat prescrite. Le Canada comprend en outre que, même si une durée du contrat définie est déterminée, l'offre commerciale de l'entrepreneur peut prévoir un renouvellement automatique des services par abonnement.*

(b) ***Métriques.*** *L'entrepreneur fournit au Canada l'accès à la solution par abonnement, le tout aux prix indiqués dans la soumission en matière d'approvisionnement, à l'annexe C – Solutions Catalogue de Solutions de logiciels-services et Prix Plafonds, ou dans la soumission de l'entrepreneur, le cas échéant.*

(c) ***Avis de renouvellement automatique.*** *L'entrepreneur reconnaît que, même si le Canada convient des conditions commerciales habituelles de l'entrepreneur, le Canada est assujetti à un cadre réglementaire juridique régissant les autorisations de dépenses financières.*

L'entrepreneur convient de fournir au Canada, dans le cadre des services, une fonctionnalité ou un outil de notification afin d'aider le Canada à administrer le contrat. L'entrepreneur convient en outre d'envoyer des avis à la fois à l'autorité contractante et au responsable technique avant l'expiration des services d'abonnement ou de la durée du contrat.

(d) ***Délai de grâce.*** *L'entrepreneur s'engage à accorder au Canada un délai de grâce facultatif de quatre semaines pour mettre fin à la durée du contrat si le Canada ne met pas fin à son utilisation du service au plus tard à la fin de la durée du contrat définie. En tout temps avant l'expiration du délai de grâce, et nonobstant toute clause de renouvellement automatique ailleurs dans le contrat, l'autorité contractante peut résilier le contrat en avisant par écrit l'entrepreneur de la décision du Canada de résilier le contrat. À la remise de l'avis de résiliation, la résiliation prendra effet immédiatement ou au moment indiqué dans l'avis de résiliation. Le Canada sera libéré de toute autre obligation en vertu du contrat après la date de résiliation et sera expressément libéré de toute prolongation de la durée découlant d'une clause de renouvellement automatique. L'entrepreneur n'appliquera aucune pénalité ou frais additionnel dans ces circonstances.*

(e) ***Responsabilité du Canada.*** *Nonobstant les dispositions relatives au délai de grâce, le Canada demeure responsable de surveiller ses obligations en vertu du contrat, y compris les frais, les dates de renouvellement et d'expiration, la consommation, l'utilisation, le paiement, la résiliation et les renouvellements.*

(f) **Changement en matière de consommation.** L'entrepreneur accorde au Canada l'option irrévocable d'augmenter ou de réduire sa consommation de produits ou de services de logiciel-service décrits à l'annexe A. Si la consommation d'un produit ou d'un service de

logiciel-service par le Canada est réduite, l'entrepreneur convient qu'aucune pénalité ou augmentation du prix unitaire ne s'applique en conséquence.

3. Solution

3.1 Logiciel-service. L'entrepreneur fournira la solution en mode de prestation de logiciels-services, ce qui permettra au Canada d'accéder à la solution hébergée par l'entrepreneur et de l'utiliser.

3.2 Solution commercialement disponible. Le Canada reconnaît que la solution est une solution commercialement disponible offerte à d'autres clients. Dans le cadre de l'abonnement à la solution, l'entrepreneur s'engage à mettre à la disposition du Canada toutes les caractéristiques et fonctionnalités incluses dans la version commercialement disponible de la solution, ainsi que les services d'infrastructure informatique accessoires et requis, qui sont tous inclus dans le prix de l'abonnement.

3.3 Évolution du logiciel; caractéristiques ou fonctionnalités. Le Canada reconnaît que la solution ou l'infrastructure connexe peut évoluer au cours de la durée du contrat. L'entrepreneur convient de continuer à fournir les services sous forme de solution commercialement disponible, avec des fonctionnalités ou des caractéristiques et à des conditions qui ne sont pas moins favorables qu'au moment de l'attribution du contrat.

3.4 Améliorations et évolution de la solution. Les parties reconnaissent que la technologie et les modèles d'affaires évoluent rapidement et que toute solution fournie au début de la durée du contrat sera inévitablement différente de la solution fournie à la fin de la durée du contrat, et que la ou les méthodes par lesquelles la solution et tout périphérique potentiel sont livrés au Canada soient susceptibles de changer ou d'évoluer et que, au moment de la conclusion du présent contrat, les parties ne puissent envisager tous les biens ou services qui peuvent être livrés aux termes du présent contrat, mis à part le fait qu'ils seront livrés aux utilisateurs. Dans cet esprit, les parties s'entendent sur ce qui suit :

(a) L'entrepreneur doit maintenir et améliorer continuellement la solution et l'infrastructure tout au long de la durée du contrat sur une base commercialement raisonnable, et doit fournir ces améliorations au Canada dans le cadre de l'abonnement du Canada, sans ajustement de prix si ces améliorations sont également offertes aux autres clients sans frais additionnel.

(b) Si l'entrepreneur supprime des fonctions de l'offre commerciale de la solution et les offres dans tout autre service ou produit, ou tout service ou produit nouveau, l'entrepreneur doit continuer de les fournir au Canada dans le cadre de l'abonnement du Canada aux services, selon les modalités actuelles du contrat, peu importe si ces autres services ou produits contiennent également des fonctions nouvelles ou additionnelles. L'entrepreneur n'est pas tenu de se conformer au présent paragraphe si la solution acquise par le Canada est toujours offerte par l'entrepreneur parallèlement aux nouveaux services offerts aux autres clients.

3.5 Option de déclassement. Si l'entrepreneur n'est pas en mesure de fournir les services avec des caractéristiques et des fonctionnalités non moins favorables, il doit en aviser le Canada par écrit en précisant les circonstances et les autres options possibles, notamment une réduction du prix. Si aucune autre option n'est acceptable pour le Canada, l'entrepreneur convient de consentir à la résiliation du contrat et de payer tous les coûts directs identifiables engagés par le Canada pour la migration et le stockage des données du Canada ainsi que pour le renouvellement des services de remplacement.

4. Service

4.1 Services de la solution

(a) **Logiciel-service.** L'entrepreneur fournira tous les services dont le Canada a besoin pour accéder à la solution et l'utiliser, tel que précisé l'appendice A.

(b) **Autorité.** L'entrepreneur déclare et garantit qu'il possède ou qu'il a obtenu et conservera pendant toute la durée du contrat tous les pouvoirs nécessaires, notamment les droits de propriété intellectuelle requis pour fournir les services conformément aux modalités du présent contrat.

(c) **Indemnisation.** Si quelqu'un allège que, en raison de l'accès du Canada à des services de solution SaaS ou de leur utilisation par le Canada, cette dernière porte atteinte aux droits de propriété intellectuelle, le Canada avisera rapidement le fournisseur par écrit de cette réclamation. Dans ces circonstances, ou si quelqu'un allègue que le fournisseur porte atteinte aux droits de intellectuelle associés à la solution SaaS de ce contrat :

Le fournisseur doit immédiatement prendre l'une des mesures suivantes :

(i) prendre toutes les mesures nécessaires pour acquérir les droit et être en mesure de continuer d'offrir les services de la solution au Canada, conformément au contrat;

(ii) modifier ou remplacer la partie qui porte prétendument atteinte pi la totalité de la solution SaaS, et continuer à fournir les services de la solution au Canada, conformément au contrat;

(iii) si les options ci-dessus ne sont pas viables, fournir un préavis écrit au sujet de la réclamation au Canada et proposer une solution SaaS « de rechange » aux termes de services d'une solution nouvelle ou provisoire, conformément au contrat; fournir les services de la solution nouvelle ou provisoire au même prix que les services de la solution concernée, et ce, pour la durée du contrat, indépendamment du prix commercial du fournisseur pour la solution SaaS de rechange ou de la plus grande fonctionnalité de la solution SaaS de rechange; et, à la demande du Canada, fournir de la formation sans frais supplémentaires sur l'utilisation de la solution SaaS de rechange;

(iv) fournir un préavis écrit au Canada afin de l'informer de la réalisation du contrat, y compris le nom requérant, la nature de la réclamation, le rôle présumé du fournisseur dans la violation alléguée relative à la solution SaaS et une confirmation de l'incapacité du fournisseur à continuer à fournir les services de la solution au Canada conformément au contrat. Pour permettre cette résiliation, le fournisseur doit fournir au Canada un accès accru à toute donnée du gouvernement du Canada utilisée ou conservée par l'entremise de la solution SaaS à des fins de récupération ou de migration, et rembourser entièrement toute partie du prix contractuel que le Canada a déjà versée au cours des 12 derniers mois, ou à partir de la date de la violation, selon le moment qui survient en premier.

Si le fournisseur omet de se conformer à la présente section dans un délai raisonnable, le fournisseur convient de rembourser le Canada pour tous les coûts que ce dernier peut avoir

déboursés pour régler la réclamation pour violation, y compris l'approvisionnement de services d'une nouvelle solution.

(d) **Accessibilité :** L'entrepreneur doit fournir un accès Web à la solution qui n'entrave pas la conformité aux normes d'accessibilité, tel que spécifié par la Norme sur l'accessibilité des sites Web : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=23601.

(e) **Octroi des droits d'utilisation**. L'entrepreneur accorde au Canada le droit d'accéder à la solution et de l'utiliser sur une base non exclusive et incessible, à partir d'un nombre illimité d'emplacements, d'appareils et d'environnements d'exploitation, au moyen d'une connexion sécurisée, sans fil, mobile ou autre, au moyen d'un navigateur Web ou d'une autre technologie de connexion qui pourrait devenir disponible.

(f) **Inclus**: L'entrepreneur déclare et garantit que les services comprennent

(i) hébergement et maintenance de la solution,

(ii) la fourniture de tous les services d'infrastructure de technologie de l'information accessoires et additionnels nécessaires,

(iii) une infrastructure technique conforme à toutes les normes de sécurité requises, permettant au Canada d'utiliser la solution pour traiter les données du client conformément à ses normes de sécurité exprimées, et

(iv) accès et utilisation sans entraves, quelle que soit la quantité de données créée, traitée ou stockée par la solution, le tout est inclus dans le prix.

(g) **Droits d'utilisation restreints.** Le Canada reconnaît qu'en fournissant les services, l'entrepreneur ne délivre aucun droit de propriété sur un produit logiciel, une composante de la solution ou une infrastructure utilisés par l'entrepreneur pour fournir les services, sauf dans les cas expressément prévus dans une autorisation de tâches. Le Canada ne fera sciemment pas les choses suivantes :

(i) distribuer, octroyer une licence, prêter ou vendre la solution;

(ii) porter atteinte aux mécanismes de sécurité de la solution ou les contourner;

(iii) retirer, modifier ou obscurcir tout avis de droit d'auteur, de marque commerciale ou tout autre avis de propriété figurant sur ou dans la solution.

(h) **Modalités applicables**. L'entrepreneur a indiqué, et le Canada reconnaît, que l'entrepreneur peut modifier unilatéralement, sans préavis à ses clients, y compris le Canada, les modalités commerciales selon lesquelles il offre sa solution. L'entrepreneur déclare et garantit qu'une telle modification n'entraînera pas des conditions moins favorables, notamment en ce qui concerne le prix, les niveaux de service et les recours, sans égard à tout avis contraire.

(i) **Modalités additionnelles.** Les parties conviennent que les modalités, y compris les avis par « clic » ou « fenêtre contextuelle », qui s'appliquent à l'offre commerciale de la solution par l'entrepreneur, y compris les outils de tiers ou l'infrastructure accessoire, ne s'appliquent pas à l'utilisation de la solution par le Canada si ces modalités sont en conflit avec les modalités expresses du présent contrat. Les modalités des outils tiers non spécifiés en tant que service ou solution dans le appendice A ne sont pas assujetties à cette section.

(j) **Offre commerciale de logiciel-service.** Le Canada reconnaît qu'il acceptera l'offre commerciale de logiciel-service de l'entrepreneur et déclare que, à moins que cela soit explicitement désigné comme travaux ou services à fournir en vertu du présent contrat, le Canada n'exige pas de développement personnalisé, de services de rechange, de niveaux de service, de fonctionnalités ou de caractéristiques.

(k) **Récupération des données:** L'entrepreneur accepte de rendre les données du Canada disponibles pendant au moins 90 jours après la fin du contrat afin de laisser au client suffisamment de temps pour migrer leurs données vers un nouvel environnement, sans frais supplémentaires pour le Canada.

5. Niveaux de service

L'*annexe D, Accords sur les niveaux de service*, contient les renseignements précis qui définissent les niveaux et les normes relatifs aux processus et aux attentes en matière de rendement pour les services devant être fournis en vertu du contrat, et doit être lue conjointement avec la section suivante.

5.1 Disponibilité. L'entrepreneur mettra le service à la disposition du Canada en stricte conformité avec la documentation sur la solution et l'annexe D, Accords sur les niveaux de service.

5.2 Crédits de service. L'entrepreneur accordera au Canada les crédits de service applicables s'il n'atteint pas les niveaux de disponibilité de la solution de temps de disponibilité définis à l'annexe D, Accords sur les niveaux de service.

5.3 Exclusions. L'entrepreneur précisera expressément toute exclusion des niveaux de disponibilité de la solution indiqués à l'annexe D, Accords sur les niveaux de service.

5.4 Services de soutien. L'entrepreneur fournira un soutien technique en stricte conformité avec l'annexe D, Accords sur les niveaux de service.

5.5 Acheminement au palier hiérarchique approprié. L'entrepreneur peut prévoir un processus de recours hiérarchique pour le règlement des différends, qui est décrit à l'annexe D, Accords sur les niveaux de service.

5.6 Pas d'infraction. L'entrepreneur garantit **qu'à sa connaissance**, rien dans la solution, ou dans l'utilisation de la solution par le Canada, ne constitue ou ne constituera une appropriation illicite de la propriété intellectuelle ou des autres droits d'un tiers ni ne les enfreindra.

6. Documentation

6.1 Documentation sur la solution. L'entrepreneur doit fournir au Canada, au moment de l'attribution du contrat, l'accès à la documentation sur la solution commercialement disponible. L'entrepreneur doit mettre à jour la documentation sur la solution à des conditions commercialement raisonnables.

6.2 Autres documents. L'entrepreneur doit fournir toute documentation nécessaire à l'exécution des travaux, ou y donner accès.

6.3 Droits de traduction. L'entrepreneur convient que le Canada peut traduire tout produit livrable écrit, y compris la documentation sur la solution ou les documents de formation, en anglais ou en français. L'entrepreneur reconnaît que toutes les traductions appartiennent au Canada et ce dernier n'a aucune obligation de les remettre à l'entrepreneur. Tous les documents qui sont traduits par le

Canada incluront l'avis de droit d'auteur ou de droit de propriété qui faisait partie du document original. L'entrepreneur ne peut être tenu responsable des erreurs techniques qui se produisent en raison d'une traduction faite par le Canada.

6.4 **Droits moraux**. À la demande du Canada, l'entrepreneur peut fournir une renonciation écrite permanente aux droits moraux, sous une forme acceptable pour le Canada, de la part de chaque auteur qui a contribué à la réalisation du produit écrit. Si l'entrepreneur n'est pas capable ou pas disposé à obtenir les renonciations demandées, l'entrepreneur convient d'indemniser le Canada de toutes les pertes et dépenses (y compris les frais juridiques) découlant de toute réclamation pour violation de droits moraux par un tiers fondée sur l'utilisation de la solution par le Canada.

6.5 **Documentation défectueuse.** Si, au cours de la période de garantie, le Canada avise l'entrepreneur d'un défaut ou d'une non-conformité dans une partie quelconque des documents fournis avec les travaux, l'entrepreneur doit corriger le défaut ou la non-conformité dès que possible et à ses propres frais. Le Canada peut fournir à l'entrepreneur des renseignements sur les défauts ou la non-conformité dans d'autres documents, y compris la documentation sur la solution, à titre d'information seulement.

7. Travaux

7.1 Services professionnels

(a) **Services professionnels.** L'entrepreneur doit exécuter et fournir au Canada les services professionnels (les « travaux ») décrits dans une autorisation de tâches (AT).

(b) **Exécution des travaux; garantie.** L'entrepreneur déclare et garantit ce qui suit : i) il a les compétences pour exécuter les travaux; ii) il dispose de tout ce qui est nécessaire pour exécuter les travaux, y compris les ressources, les installations, la main-d'œuvre, la technologie, l'équipement et les matériaux; iii) il a les qualifications nécessaires, incluant les connaissances, les compétences, le savoir-faire et l'expérience, pour exécuter les travaux avec efficacité.

(c) **Rigueur des délais :** Il est essentiel que les travaux soient livrés au plus tard à la date indiquée dans l'autorisation de tâche.

7.2 Recours

(a) **Travaux.** Si à tout moment pendant la période de garantie, les travaux ne respectent pas les obligations de garantie, l'entrepreneur doit le plus tôt possible, à la demande du Canada, corriger à ses propres frais toute erreur ou tout défaut et apporter les modifications nécessaires aux travaux.

(b) **Documentation.** Si à tout moment pendant la période de garantie, le Canada découvre un défaut ou une non-conformité dans une partie des travaux, l'entrepreneur doit le plus tôt possible corriger à ses propres frais le défaut ou la non-conformité.

(c) **Droit du Canada à un recours.** Si l'entrepreneur ne s'acquitte pas d'une obligation prévue dans le présent contrat dans un délai raisonnable après avoir reçu un avis, le Canada aura le droit de remédier ou de faire remédier aux travaux défectueux ou non conformes aux frais de l'entrepreneur. Si le Canada ne souhaite pas corriger ou remplacer les travaux défectueux ou non conformes, le prix contractuel sera réduit de façon équitable.

7.3 Sous-traitance

(a) **Conditions de sous-traitance.** L'entrepreneur peut sous-traiter l'exécution des travaux, mais seulement si (i) l'entrepreneur obtient le consentement écrit préalable de l'autorité contractante, (ii) le sous-traitant est lié par les termes du présent contrat, et (iii) l'entrepreneur demeure responsable envers le Canada pour tous les travaux effectués par le sous-traitant.

(b) **Exceptions au consentement de sous-traitance.** L'entrepreneur n'est pas tenu d'obtenir le consentement de l'autorité contractante à l'égard des contrats de sous-traitance expressément autorisés dans le contrat. L'entrepreneur peut également, sans le consentement de l'autorité contractante : (i) acheter des produits courants « Off-the-shelf » en vente libre dans le commerce, ainsi que des articles et des matériaux produits par des fabricants dans le cours normal de leurs affaires; (ii) sous-traiter tous les services accessoires qui seraient normalement sous-traités dans l'exécution des travaux; et (iii) permettre à ses sous-traitants à tout échelon d'effectuer des achats ou de sous-traiter comme le prévoient les alinéas (i) et (ii).

7.4 Retard justifiable

(a) **Sans la responsabilité.** L'entrepreneur n'est pas responsable des retards d'exécution ni de l'inexécution due à des causes au-delà de son contrôle qui ne pouvaient raisonnablement être prévues ou évitées par des moyens raisonnablement accessibles à l'entrepreneur, pourvu que l'entrepreneur avise l'autorité contractante du retard ou de la probabilité du retard dès qu'il en prend connaissance (ce qu'on appelle « **retard justifiable** »).

(b) **Avis**. L'entrepreneur doit de plus informer l'autorité contractante, dans les quinze (15) jours ouvrables, de toutes les circonstances liées au retard et soumettre à l'approbation de l'autorité contractante un plan de redressement clair qui détaille les étapes que l'entrepreneur propose de suivre afin de réduire au minimum les conséquences de l'événement qui a causé le retard.

(c) **Livraison et dates d'échéance** : Toute date de livraison ou autre date qui est directement touchée par un retard justifiable fera l'objet d'un report raisonnable dont la durée n'excédera pas la durée du retard justifiable.

(d) **Non-responsabilité des coûts pour le Canada :** Le Canada ne sera pas responsable des frais engagés par l'entrepreneur ou l'un de ses sous-traitants ou mandataires par suite d'un retard justifiable, sauf lorsque celui-ci est attribuable à l'omission du Canada de s'acquitter de l'une de ses obligations en vertu du contrat.

7.5 Droits et recours

7.5.1 Les droits sont cumulatifs

Tous les droits et recours prévus dans le contrat ou par la loi sont cumulatifs et non exclusifs.

7.5.2 Résiliation pour manquement

(a) **Avis de manquement.** L'autorité contractante peut transmettre à l'entrepreneur un avis écrit de résiliation pour manquement de tout ou partie du contrat. L'avis indiquera la violation, les circonstances pertinentes, le délai proposé, les travaux ou les services touchés (en cas de résiliation partielle), les exigences relatives à un plan d'action, les services de transition ou de

migration nécessaires, et la date effective de la résiliation. L'avis indiquera également si le Canada conserve d'autres réclamations de dommages-intérêts.

(b) **Conformité du fournisseur.** L'entrepreneur doit respecter les exigences en matière d'assurance prévues dans l'avis.

(c) **Violation totale.** Si, de l'avis raisonnable du Canada, le manquement de l'entrepreneur est une violation totale ou substantielle du contrat, le Canada peut immédiatement résilier le contrat au moyen d'un préavis. Par souci de clarté, l'avis du Canada peut être fondé sur les circonstances, y compris, sans toutefois s'y limiter :

(i) le non-respect d'une obligation contractuelle substantielle par l'entrepreneur;
(ii) le fait que l'entrepreneur semble irréfutablement ne pas être en mesure de respecter une obligation contractuelle substantielle en raison de facteur hors de son contrôle, ce qui inclut une insolvabilité réelle ou apparente, l'omission répétée de produire des produits livrables acceptables en vertu du présent contrat ou de contrats similaires avec le Canada;
(iii) des violations non corrigées multiples ou répétées d'une obligation contractuelle intermédiaire par l'entrepreneur;
(iv) un manquement de l'entrepreneur qui a des répercussions négatives sur les activités du gouvernement.

(d) **Autre manquement**

(i) Si les manquements de l'entrepreneur ne sont pas des violations totales, le Canada déterminera le délai dans lequel l'entrepreneur doit corriger le manquement et peut exiger un plan d'action.
(ii) Si, en réponse à l'avis, l'entrepreneur indique son incapacité ou son manque de volonté à corriger le manquement, le Canada peut résilier le contrat pour manquement immédiatement.
(iii) Si le contrat (y compris les autorisations de tâches individuelles) précise qu'un manquement particulier ne permettra aucun délai, le Canada peut résilier le contrat pour manquement immédiatement sans fournir la possibilité de corriger le manquement.

(e) Le Canada n'est pas tenu d'aviser l'entrepreneur des manquements. Les parties conviennent que le Canada peut choisir de ne pas utiliser de processus de préavis officiel ou de prolonger le délai imparti à l'entrepreneur, et que cela pourra considérer comme une renonciation de la part du Canada à certains droits ou une acceptation du manquement de l'entrepreneur par le Canada.

(f) Si le Canada résilie le contrat pour manquement, le Canada ne paiera que pour les travaux ou services complétés livrés et acceptés avant la date de la résiliation. Le Canada ne paiera aucun montant qui dépasse la valeur des travaux ou services acceptés.

7.5.3 Résiliation pour raisons de commodité

(a) **Avis de résiliation.** L'autorité contractante peut transmettre au fournisseur un avis écrit de résiliation pour raisons de commodité de tout le contrat ou d'une partie du contrat. L'avis indiquera la violation, la date effective de la résiliation, les travaux ou les services touchés (en cas de résiliation partielle), et les services de transition ou de migration nécessaires. L'entrepreneur doit se conformer aux exigences prévues par l'avis, y compris continuer à effectuer ou à livrer des services ou des travaux qui ne sont pas touchés par la résiliation.

(b) L'entrepreneur convient de rembourser immédiatement au Canada la portion de toute avance non liquidée à la date de la résiliation.

(c) Si, en vertu du paragraphe a), le Canada résilie :

a. **les travaux,** le Canada paiera à l'entrepreneur les coûts raisonnables liés à la résiliation des travaux engagés par l'entrepreneur, excluant particulièrement les coûts liés à la cessation d'emploi d'employés, à moins que l'entrepreneur établissent que ces coûts découlent d'obligations légales;

b. **les services.**

i. pour les services d'abonnement payés par avance chaque mois, le Canada renoncera à son droit de réclamer la partie non liquidée d'une avance à la date de la résiliation; et

ii. pour les services d'abonnement annuel, ou comportant des périodes contractuelles définies, et incluant des paiements annuels faits par avance, le Canada renoncera à son droit de réclamer la partie d'une avance qui n'est pas liquidée le dernier jour du mois suivant la date de la résiliation,

(d) Les parties conviennent que ces montants représentent une estimation authentique des dommages liquidés qu'encourrait l'entrepreneur en raison d'une résiliation précoce du contrat, et qu'il ne s'agit pas d'une pénalité.

7.6 Services professionnels : Services de transition

(a) **Migration.** L'entrepreneur convient qu'en raison de la nature des services stipulés au contrat, le Canada peut exiger qu'ils soient fournis sans interruption. Avant la transition vers le nouvel entrepreneur ou au Canada, l'entrepreneur devra fournir toute l'information et la documentation opérationnelle, techniques, conceptuelles et de configuration nécessaires à la transition, dans la mesure où il ne s'agit pas de renseignements confidentiels de l'entrepreneur. L'entrepreneur déclare et garantit qu'il n'entravera pas, directement ou indirectement, l'accès du Canada aux données du Canada ou leur transfert.

(b) **Services de migration et de transition.** L'entrepreneur convient que, si le Canada demande des services de migration ou de transition pendant la période précédant la fin de la durée du contrat, il aidera diligemment le Canada à faire la transition entre le présent contrat et le nouveau contrat ou à faire migrer les données du Canada à l'environnement du nouveau fournisseur. Il convient que les services décrits ci-dessous ne donneront lieu à aucuns frais autres que ceux qui sont prévus dans la base de paiement.

7.7 Inspection et acceptation des travaux

(a) **Inspection par le Canada :** Tous les travaux sont soumis à l'inspection et à l'acceptation par le Canada. L'inspection et l'acceptation des travaux par le Canada ne relèvent pas l'entrepreneur de sa responsabilité à l'égard des défectuosités ou des autres manquements aux exigences du contrat. Le Canada aura le droit de rejeter tout travail non conforme aux exigences du contrat et d'exiger une rectification ou un remplacement aux frais de l'entrepreneur.

(b) **Procédures d'acceptation** : Sauf disposition contraire du contrat, les procédures d'acceptation sont les suivantes :

(i) Une fois les travaux sont terminés, l'entrepreneur doit en aviser l'autorité technique par écrit, avec copie à l'autorité contractante, en se référant à la présente disposition du contrat et en demandant l'acceptation des travaux;

(ii) Le Canada disposera de 30 jours à compter de la réception de l'avis pour effectuer son inspection (la « **période d'acceptation** »).

(c) **Défauts et soumission à nouveau des produits livrables :** Si le Canada découvre un défaut durant la période d'acceptation, l'entrepreneur devra le régler le plus tôt possible et aviser le Canada par écrit une fois les travaux terminés, après quoi le Canada aura le droit d'inspecter à nouveau les travaux avant leur acceptation, et la période d'acceptation recommencera. Si le Canada détermine qu'un produit livrable est incomplet ou déficient, il n'est pas tenu de désigner tous les articles manquants ou tous les défauts avant de rejeter le produit livrable.

(d) **Accès aux lieux :** L'entrepreneur doit permettre aux représentants du Canada, en tout temps durant les heures de travail, d'accéder à tous les lieux où toute partie des travaux est exécutée. Les représentants du Canada peuvent procéder à leur gré à des examens et à des vérifications. L'entrepreneur doit fournir toute l'aide, les locaux, tous les échantillons, pièces d'essai et documents que les représentants du Canada peuvent raisonnablement exiger pour l'exécution de l'inspection. L'entrepreneur doit expédier lesdits échantillons et pièces d'essai à la personne ou à l'endroit indiqué par le Canada.

(e) **Inspection de la qualité par l'entrepreneur :** L'entrepreneur doit inspecter et approuver toute partie des travaux avant de le soumettre pour acceptation ou livraison au Canada. Tous les produits livrables soumis par l'entrepreneur doivent être d'une qualité professionnelle, exempts d'erreurs typographiques et autres erreurs, et conformes aux normes les plus élevées de l'industrie.

(f) **Registre des inspections :** L'entrepreneur doit tenir un registre des inspections à la fois précis et complet qu'il doit mettre à la disposition du Canada, sur demande. Les représentants du Canada peuvent tirer des copies et des extraits des registres pendant l'exécution du contrat et pendant une période maximale de trois ans après la fin du contrat.

(g) **Rétroaction informelle :** À la demande de l'entrepreneur, le Canada peut fournir une rétroaction informelle avant que tout produit livrable ne soit officiellement soumis pour acceptation. Toutefois, cela ne doit pas être utilisé comme une forme de contrôle de la qualité des travaux de l'entrepreneur. Le Canada n'est pas tenu de fournir une rétroaction informelle.

8. Autorisation de tâches (AT) (clause facultative à utiliser lorsque des services professionnels sont requis)

Les services professionnels de l'entrepreneur en vertu du présent contrat doivent être réalisés sur demande, au moyen d'une autorisation de tâches (AT).

8.1 Forme et contenu de l'AT. Une AT contiendra a) le numéro du contrat et le numéro de l'AT, b) les détails des activités et des ressources requises, c) une description des produits livrables, d) un calendrier indiquant les dates d'achèvement des principales activités ou les dates de soumission des produits livrables, e) les exigences de sécurité et f) les coûts.

8.2 Réponse de l'entrepreneur à l'AT. L'entrepreneur doit fournir au Canada, dans la période mentionnée dans l'AT, le coût estimatif total proposé pour l'exécution du travail et une répartition des coûts, établie conformément aux honoraires. L'entrepreneur ne sera pas payé pour la préparation ni

la présentation d'une réponse, ni pour la fourniture d'autres renseignements requis pour la préparation et l'attribution officielle de l'AT.

8.3 Limite de l'AT et pouvoirs d'attribuer des AT de façon officielle. Pour être attribuée de façon officielle, une AT doit être signée par l'autorité canadienne concernée comme indiqué dans le présent contrat. Tous les travaux effectués par l'entrepreneur sans avoir reçu une AT valide seront effectués à ses propres risques.

8.4 Rapports d'utilisation périodique. L'entrepreneur doit compiler et tenir à jour des données sur les services fournis au gouvernement fédéral, conformément aux AT approuvées attribuées dans le cadre du présent contrat.

8.5 Regroupement d'AT pour des raisons administratives. Le présent contrat peut être modifié à l'occasion afin de tenir compte de l'ensemble des AT valides attribuées à ce jour et de consigner les travaux réalisés dans le cadre de ces AT à des fins administratives.

9 Base de paiement

Remarque: Cet article sera ajusté à l'attribution du contrat pour inclure la base et la méthode de paiement soumises par l'entrepreneur à l'annexe D, Accords sur les niveaux de service ou à la soumission gagnante.

9.1 Abonnement. En ce qui concerne les services, y compris l'accès à la solution et son utilisation, la documentation sur la solution, les services de soutien et les services d'infrastructure de technologie de l'information accessoires et additionnels requis (tous les services décrits dans le présent contrat qui ne sont pas des travaux), le Canada doit payer les prix détaillés à l'annexe C – Catalogue de Solutions de logiciels-services et Prix Plafonds, ou dans la soumission de l'entrepreneur, le cas échéant.

9.2 Services professionnels fournis dans le cadre d'une autorisation de tâches. En ce qui concerne les services professionnels demandés par le Canada, conformément à une autorisation de tâches attribuée de façon officielle, le Canada paiera à l'entrepreneur, à terme échu, jusqu'à concurrence du prix maximum pour l'AT, les heures réellement travaillées ainsi que tout produit livrable subséquent / prix ferme énoncé dans l'autorisation de tâches, aux taux quotidiens fermes tout compris indiqués à l'annexe C – Catalogue de Solutions de logiciels-services et Prix Plafonds ou dans la soumission de l'entrepreneur, le cas échéant, les taxes sont extra.

9.3 Frais de soutien sur place. Si le Canada l'approuve à l'avance, l'entrepreneur recevra les taux de main-d'œuvre horaires ou quotidiens précisés dans le contrat, ainsi que les frais de déplacement et de subsistance raisonnables et appropriés engagés par l'entrepreneur dans le cadre des services sur place. Les frais de déplacement et de subsistance ne seront remboursés que conformément aux indemnités de repas et de véhicule particulier prévues dans la Directive sur les voyages du Conseil national mixte, telle que modifiée de temps à autre. Tous ces frais pré approuvés devront être facturés au Canada comme frais distincts.

9.4 Attestation du prix. L'entrepreneur atteste que le prix proposé n'est pas supérieur au plus bas prix demandé à tout autre client, y compris à son meilleur client, pour une qualité et une quantité semblable de biens, de services ou les deux.

10. Paiement

10.1 Factures

(a) **Présentation des factures**. L'entrepreneur doit présenter des factures pour les services et la livraison des travaux, le cas échéant.

(b) **Exigences de facturation**. Les factures doivent être soumises au nom de l'entrepreneur et doivent contenir :

(i) la date, le nom et l'adresse du ministère client, les numéros d'articles ou de référence, les livrables ou la description des travaux, le numéro du contrat, le numéro de référence du client (NRC), le numéro d'entreprise – approvisionnement (NEA) et le ou les codes financiers;

(ii) des renseignements sur les dépenses (comme le nom des articles et leur quantité, l'unité de distribution, le prix unitaire, les tarifs horaires fermes, le niveau d'effort et les sous-contrats, selon le cas) conformément à la base de paiement, excluant les taxes applicables;

(iii) les taxes applicables doivent être indiquées sur une ligne distincte avec les numéros d'enregistrement correspondants des autorités fiscales, et tous les éléments qui sont détaxés, exonérés ou auxquels les taxes applicables ne s'appliquent pas doivent être désignés comme tels sur toutes les factures;

(iv) les déductions correspondant à la retenue de garantie, s'il y a lieu;

(v) le report des totaux, s'il y a lieu.

(c) **Taxes**

(i) **Paiement des taxes**. Les taxes applicables seront payées par le Canada conformément aux dispositions de l'article sur la présentation des factures. Il incombe à l'entrepreneur de facturer les taxes applicables selon le taux approprié, conformément aux lois en vigueur. L'entrepreneur accepte de remettre aux autorités fiscales concernées le montant de taxes applicables versées ou exigibles.

(ii) **Retenue pour les non-résidents**. Le Canada doit retenir 15 % du montant à payer à l'entrepreneur pour des services rendus au Canada si l'entrepreneur n'est pas un résident du Canada, à moins que ce dernier obtienne une exonération valide de l'Agence du revenu du Canada. Le montant retenu sera conservé dans un compte pour l'entrepreneur à l'égard de toute dette fiscale exigible par le Canada.

(d) **Certification des factures**. L'entrepreneur atteste que la facture correspond aux travaux qui ont été livrés et qu'elle est conforme au contrat.

10.2 Période de paiement. Le Canada paiera le montant non contesté de la facture de l'entrepreneur dans les 30 jours suivant sa réception. Dans l'éventualité où une facture n'est pas dans une forme

et un contenu acceptables, le Canada en avisera l'entrepreneur et le délai de paiement de 30 jours débutera à la réception d'une facture conforme.

10.3 Intérêts sur les paiements en retard. Le Canada versera à l'entrepreneur des intérêts simples, au taux moyen majoré de 3 % par an, sur toute somme en souffrance, à partir du premier jour où la somme est en souffrance jusqu'au jour qui précède la date de paiement inclusivement, à condition que le Canada soit responsable du retard de paiement à l'entrepreneur. Le Canada ne versera pas d'intérêts sur les paiements anticipés qui sont en souffrance.

10.4 Mode de paiement

(a) Le Canada paiera l'entrepreneur pour les services soit à l'avance, soit à terme échu, conformément à l'annexe D, Accords sur les niveaux de service applicable. Lorsque le paiement est effectué à l'avance, la période de paiement anticipé ne dépasse pas 12 mois. Le paiement anticipé n'empêche pas le Canada d'exercer un recours à l'égard de ce paiement ou de la prestation des services.

(b) Si le Canada conteste une facture pour quelque raison que ce soit, il réglera à l'entrepreneur la tranche de la facture non contestée, à la condition que les articles non contestés soient indiqués distinctement sur la facture et que leur paiement soit exigible. Dans le cas des factures contestées, elles ne seront réputées reçues aux fins de la section 7.3 qu'une fois le litige réglé.

10.5 Limite des dépenses. Le Canada ne paiera pas l'entrepreneur pour tout changement à la conception, toute modification ou interprétation des travaux, à moins que ces changements à la conception, ces modifications ou ces interprétations n'aient été approuvés par écrit par l'autorité contractante avant d'être intégrés aux travaux.

10.6 Paiement électronique des factures. L'entrepreneur accepte d'être payé à l'aide des instruments de paiement électronique suivants :

(a) carte d'achat Visa;

(b) carte d'achat MasterCard;

(c) dépôt direct (national et international);

(d) échange de données informatisé;

(e) virement télégraphique (international seulement);

(f) système de transfert de paiements de grande valeur (plus de 25 millions de dollars).

11. Exigences en matière d'assurances.

L'entrepreneur est responsable de décider s'il doit s'assurer pour remplir ses obligations en vertu du contrat et pour se conformer aux lois applicables. Toute assurance contractée et maintenue par l'entrepreneur est aux frais de ce dernier et pour son bénéfice et sa protection. Elle ne dégage pas l'entrepreneur de sa responsabilité en vertu du contrat, ni ne la diminue.

12. Limitation de responsabilité

12.1 Responsabilité de première partie

(a) Exécution du contrat : L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par l'exécution ou l'inexécution du contrat par l'entrepreneur.

(b) Fuite de données: L'entrepreneur est entièrement responsable de tous les dommages subis par le Canada, causés par une infraction à la sécurité ou un manquement à l'obligation de confidentialité entraînant la consultation ou la divulgation non autorisées de dossiers, de données ou de renseignements appartenant au Canada ou à un tiers.

(c) Limitation par incident : Sous réserve de la clause suivante, quel que soit le fondement ou la nature de la réclamation, la responsabilité totale par incident de l'entrepreneur n'excédera pas la valeur cumulative des factures liées au contrat au cours des douze (12) mois précédant l'incident.

(d) Aucune limitation: La limitation de responsabilité susmentionnée de l'entrepreneur ne s'applique pas :

(i) à toute inconduite volontaire ou à tout acte répréhensible délibéré;

(ii) à tout manquement aux obligations relatives à la garantie.

12.2 Responsabilité de tierce partie : Chaque partie convient qu'elle est pleinement responsable des dommages qu'elle cause à un tiers dans le cadre du contrat, que la réclamation soit déposée par le tiers auprès du Canada ou de l'entrepreneur, ou des deux. Le montant de la responsabilité sera celui précisé dans l'accord conclu entre les parties ou déterminé par la cour. Les parties conviennent de se rembourser mutuellement tout paiement versé à un tiers en lien avec les dommages causés par l'autre partie et de rembourser rapidement leur part de responsabilité.

13. Dispositions générales

13.1 Lois applicables. Le présent contrat sera interprété et régi selon les lois en vigueur en [PROVINCE].

13.2 Survie. Les obligations des parties concernant la confidentialité, les déclarations et les garanties prévues dans le contrat ainsi que les dispositions qu'il est raisonnable de présumer, en raison de la nature des droits et des obligations, qu'elles devraient rester en vigueur, demeurent applicables malgré l'expiration du contrat ou sa résiliation.

13.3 Divisibilité. Si une disposition de ce contrat est déclarée inexécutable par un tribunal faisant autorité, le reste de ce contrat reste en vigueur.

13.4 Renonciation. Le défaut ou la négligence par une partie d'appliquer les droits en vertu du présent contrat ne sera pas considéré comme une renonciation à ses droits.

13.5 Aucun pot-de-vin. L'entrepreneur déclare qu'aucun pot-de-vin, cadeau, bénéfice ou autre avantage n'a été ni ne sera payé, donné, promis ou offert, directement ou indirectement, à un représentant ou à un employé du Canada ni à un membre de sa famille, en vue d'exercer une influence sur l'attribution ou la gestion du contrat.

13.6 Honoraires conditionnels. L'entrepreneur atteste qu'il n'a pas versé ni convenu de verser, directement ou indirectement, et convient de ne pas verser, directement ou indirectement, des honoraires conditionnels en rapport avec la soumission, la négociation ou l'obtention du contrat à toute personne autre qu'un employé de l'entrepreneur remplissant les fonctions habituelles liées à son poste. Dans le présent article, « honoraires conditionnels » signifie tout paiement ou autre forme de rémunération qui est subordonnée au degré de succès ou calculée en fonction du degré de succès obtenu dans la sollicitation, la négociation ou l'obtention du contrat, et « personne » signifie tout particulier qui est tenu de fournir au registraire une déclaration en vertu de l'article 5 de la *Loi sur le lobbying*, 1985, ch. 44 (4e suppl.).

13.7 Sanctions internationales.

(a) Les Canadiens et les Canadiennes et les ressortissants canadiens à l'étranger sont liés par les sanctions économiques imposées par le Canada. En conséquence, le gouvernement du Canada ne peut accepter la livraison d'aucun bien ou service provenant, directement ou indirectement, d'un ou plusieurs pays ou personnes assujettis à des sanctions économiques.

(b) Le fournisseur ne doit livrer au gouvernement du Canada aucun bien ni aucun service assujetti à des sanctions économiques.

(c) L'entrepreneur doit se conformer aux modifications apportées aux règlements imposés pendant la période du contrat. L'entrepreneur doit immédiatement aviser le Canada s'il est dans l'impossibilité d'exécuter le contrat à la suite de l'imposition de sanctions à un pays ou à une personne ou de l'ajout de biens ou de services à la liste des biens ou des services sanctionnés. Si les parties ne peuvent alors s'entendre sur un plan de redressement, le contrat sera résilié pour des raisons de commodité, conformément à la section 18.2.

13.8 Dispositions relatives à l'intégrité – Contrat. La *Politique d'inadmissibilité et de suspension* (la « Politique ») et toutes les directives incorporées par renvoi à l'invitation à soumissionner à sa date de clôture sont intégrées au contrat et en font partie intégrante. L'entrepreneur doit se conformer aux dispositions de la politique et des directives; celles-ci se trouvent sur le site internet de Travaux publics et Services gouvernement Canada sous *Politique d'inadmissibilité et de suspension*.

13.9 Code de conduite pour l'approvisionnement – Contrat. L'entrepreneur accepte de se conformer au *Code de conduite pour l'approvisionnement* et d'être lié par celui-ci pendant la durée du contrat.

13.10 Code régissant les conflits d'intérêts et code de valeurs et d'éthique de la fonction publique. L'entrepreneur reconnaît que les personnes qui sont assujetties aux dispositions de la *Loi sur les conflits d'intérêts*, 2006, ch. 9, art. 2, du Code régissant la conduite des titulaires de charge publique en ce qui concerne les conflits d'intérêts et l'après-mandat, du Code de valeurs et d'éthique de la fonction publique ou tout autre code de valeur et d'éthique en vigueur au sein d'organismes spécifiques ne peuvent bénéficier directement du contrat.

13.11 Pouvoirs

Autorité contractante

L'autorité contractante dans le cadre du contrat est :

Nom :

Titre :

Organisation :

Traiter :

Téléphone :

Courriel :

L'autorité contractante doit recevoir une copie de la facture pour le dossier et l'examen du Canada.

L'autorité contractante est responsable de la gestion du contrat, et toute modification du contrat doit être autorisée, par écrit, par l'autorité contractante. L'entrepreneur ne doit pas effectuer de travaux dépassant la portée du contrat ou des travaux qui n'y sont pas prévus à la suite de demandes ou d'instructions verbales ou écrites de toute personne autre que l'autorité contractante.

Responsable technique

Le responsable technique pour le contrat est :

Nom :

Titre :

Organisation :

Traiter :

Téléphone :

Télécopieur :

Courriel :

Le responsable technique représente le ministère ou l'organisme pour lequel les travaux sont exécutés conformément au contrat. Il s'occupe de toutes les questions liées au contenu technique des travaux prévus au contrat. Il est possible de discuter des questions techniques avec le responsable technique; cependant, ce dernier n'est pas habilité à autoriser des modifications à la portée des travaux. Ces changements peuvent être effectués uniquement au moyen d'une modification au contrat émise par l'autorité contractante.

Personne-ressource administrative du client

Personne-ressource administrative du client :

Nom :

Titre :

Organisation :

Traiter :

Téléphone :

Télécopieur :

Courriel :

La personne-ressource administrative du client doit recevoir la facture originale. Toutes les demandes de renseignements relatives aux demandes de paiement doivent être adressées à la personne-ressource *administrative du client.*

Représentant de l'entrepreneur

Le représentant de l'entrepreneur est :

Nom :

Titre :

Téléphone :

Télécopieur :

Courriel :

Octroi de mandataire

L'entrepreneur avise le Canada et ce dernier reconnaît qu'il a l'intention de désigner l'un de ses partenaires autorisés comme agent autorisé (l '"agent autorisé") pour remplir certaines obligations contractuelles pour le compte de l'entrepreneur pendant la durée du contrat, comme défini dans la section Portée ci-dessous.

L'entrepreneur désigne son partenaire autorisé ***(à compléter lors de l'attribution du contrat)*** en tant qu'agent autorisé en vertu du contrat.

Le contact de l'agent autorisé est:

Prénom:
Titre:
Téléphone:
Facsimilé:
Adresse e-mail:

L'entrepreneur accepte de fournir à l'autorité contractante un avis écrit de 30 jours à l'avance de l'un des éléments suivants:

(i) le remplacement de tout partenaire autorisé en tant qu'agent agréé,

(ii) toute modification de l'étendue des pouvoirs délégués à l'agent autorisé, et

(iii) la résiliation de l'agent autorisé.

L'entrepreneur accepte, à la demande de l'autorité contractante, de retirer ou de remplacer immédiatement l'agent autorisé. Le retrait ou le remplacement de l'agent autorisé s'ajoute à tout autre recours que le Canada peut invoquer. Une violation par un agent autorisé est une violation par l'entrepreneur lui-même.

13.12 Portée du pouvoir de l'agent

Le contractant déclare que l'agent autorisé désigné est autorisé à traiter pour le compte du contractant des transactions liées à la fourniture des biens et services dans le cadre du contrat, dans les limites suivantes: négociation des prix, fourniture des informations de facturation, facturation, fourniture de services de rapport de consommation et réception Paiement.

L'entrepreneur accepte que, sur preuve du paiement, tout paiement effectué par le Canada à l'agent autorisé sera considéré comme un paiement à l'entrepreneur lui-même. Cette relation de mandat (par laquelle l'agent autorisé s'acquitte de ses obligations contractuelles pour le compte de l'entrepreneur) ne modifie pas, ne diminue ou ne modifie aucune des responsabilités de l'entrepreneur en vertu du contrat. L'entrepreneur accepte et comprend qu'il est de la seule responsabilité de s'assurer que tous ses agents autorisés se conforment aux conditions du contrat. Si l'agent autorisé ne se conforme pas aux conditions, il doit, sur notification écrite de l'autorité contractante, remplissez et remplissez immédiatement ces obligations sans frais supplémentaires pour le Canada.

Le présent contrat de licence a été signé par les parties

[NOM DE L'ENTREPRENEUR]	[AUTHORITE CONTRACTANTE]
Par:	Par:
Nom:	Nom:
Titre:	Titre:

APPENDICE A – LIVRABLES (estimation des besoins)

1. TABLE 1 – LISTE DES LIVRABLES INITIALES

Table 1 - LISTE DES LIVRABLES INITIALES							
Numéro d'article	**Nom du produit du fournisseur** (Voir appendice C)	**Numéro de pièce du fournisseur** (Voir appendice C)	**Unité de mesure** (Voir appendice C)	**Période**	Qté	**Prix unitaire**	**Prix calculé**
1							
...							
						Sub-Total:	$0.00

2. TABLE 2 - LISTE DES LIVRABLES OPTIONNELS *(si applicable)*

Table 2 - LISTE DES LIVRABLES INITIALES							
Numéro d'article	**Nom du produit du fournisseur** (Voir appendice C)	**Numéro de pièce du fournisseur** (Voir appendice C)	**Unité de mesure** (Voir appendice C)	**Période**	Qté	**Prix unitaire**	**Prix calculé**
1							
...							
						Sub-Total:	$0.00

APPENDICE B – DÉFINITIONS ET INTERPRÉTATIONS

Dans la présente entente, à moins que le contexte ne l'indique autrement, les termes ci-après ont les acceptions suivantes :

TERMES	DÉFINITIONS
« Accord sur les niveaux de service (ANS) »	Contrat entre un fournisseur de services (interne ou externe) et l'utilisateur final qui définit le niveau de service attendu du fournisseur de services.
« Appareil »	Désigne tout équipement muni d'une unité centrale (CPU), d'une mémoire de grande capacité, d'unités d'entrée-sortie comme un clavier et un écran, et comprend les serveurs, les postes de travail, les ordinateurs portatifs, les assistants numériques personnels et l'équipement informatique mobile.
« Autorité contractante »	Désigne la personne désignée comme tel dans le contrat, ou dans un avis à l'entrepreneur, pour représenter le Canada dans l'administration du contrat;
« Biens »	Toutes les ressources en matière de technologies de l'information auxquelles le fournisseur a accès ou les ressources de cette nature qu'il utilise ou gère pour assurer la prestation et la livraison des services décrits dans la présente entente (y compris, non exclusivement, toutes les ressources technologiques se trouvant aux points de services du fournisseur, ou encore, dans un centre de données, un réseau, un dispositif de stockage, des serveurs, des plateformes de virtualisation, des systèmes d'exploitation, des inter-logiciels et des applications du fournisseur ou d'un sous-traitant de celui-ci).
« Canada », « Couronne », « Sa Majesté » ou « l'État »	Désignent Sa Majesté la Reine du chef du Canada, représentée par le ministre des Travaux publics et des Services gouvernementaux, et toute autre personne dûment autorisée à agir au nom de ce dernier ou, s'il y a lieu, un ministre compétent à qui le ministre des Travaux publics et des Services gouvernementaux a délégué ses pouvoirs, fonctions ou attributions et toute autre personne dûment autorisée à agir au nom de ce ministre;.
« Client »	Désigne le ministère ou l'organisme pour lequel les travaux sont exécutés.
« Contrat »	Désigne les articles de convention, les présentes conditions générales, toutes conditions générales, appendices, annexes et tout autre document

	intégré par renvoi, tous tels que modifiés de temps à autre avec le consentement des parties.
« Coût »	Désigne le coût établi conformément aux Principes des coûts contractuels 1031-2 en vigueur à la date de la demande de soumissions ou, s'il n'y a pas eu de demande de soumissions, à la date du contrat.
« Date de paiement »	Désigne la date que porte le titre négociable tiré par le Receveur général du Canada afin de payer une somme exigible en vertu du contrat.
« Disponibilité du logiciel »	Désigne le pourcentage de minutes au cours d'un mois pendant lequel le logiciel est opérationnel.
« Documentation du logiciel »	Désigne l'ensemble des manuels, livrets, guides d'utilisation et autres documents écrits en langage humain intelligible que l'entrepreneur doit fournir au Canada conformément au contrat et qui sera utilisée conjointement avec le logiciel.
« Données du Canada »	Les informations ou les données, peu importe leur forme ou leur format : (A) communiquées par des membres du personnel, des clients, des partenaires, des participants d'une coentreprise, des concédants de licence ou des fournisseurs du Canada, ou se rapportant à ceux-ci; (B) communiquées par des utilisateurs finaux des services ou se rapportant à ceux-ci; (C) recueillies, utilisées ou traitées par les services, ou stockées pour ceux-ci, à savoir, directement ou indirectement : (i) communiquées au fournisseur ou à ses sous-traitants par le Canada ou les utilisateurs finaux ou au nom de ceux-ci; (ii) auxquelles le fournisseur ou ses sous-traitants peuvent avoir accès, de façon intentionnelle ou accidentelle; (iii) se trouvant sur un quelconque bien ou sur un autre réseau, système ou matériel utilisé ou géré pour le Canada par le fournisseur pour les services et les services du fournisseur, y compris l'infrastructure du fournisseur; (iv) générées, développées, acquises ou obtenues autrement par le fournisseur, l'un de ses sous-traitants ou un sous-traitant ultérieur dans le cadre de la prestation des services, y compris toute l'information dérivée de cette information et toutes les métadonnées faisant partie de cette information ou s'y rapportant. Il est entendu que les « données du Canada » comprennent la totalité de l'information et des données stockées ou traitées par l'entremise des services, des biens ou de l'infrastructure du fournisseur.
« Données du Client »	Signifie (i) toutes les données fournies au contractant par le client ou à sa demande en relation avec la solution et (ii) tout le contenu que le contractant développe et livre au client, et que le client accepte, conformément au présent contrat.
« Dossier »	Tout exemplaire papier ou des données sous forme lisible par machine comprenant des renseignements personnels ou des données du Canada.

« Droits d'utilisation »	Signifie l'octroi de l'accès et l'utilisation d'une solution, parfois appelés licence d'abonnement.
« Éditeur de logiciel-service »	Signifie l'entité qui possède, opère, maintient et distribue les solutions logiciel-service.
« En souffrance »	S'entend d'une somme qui demeure impayée le lendemain du jour où elle est devenue exigible en vertu du contrat.
« Entrepreneur »	Désigne la personne, l'entité ou les entités dont le nom figure au contrat pour fournir au Canada les services et/ou les travaux.
« Erreur logique »	Désigne toute instruction ou tout énoncé présent ou absent dans le code du logiciel qui, par sa présence ou son absence, empêche le logiciel de fonctionner conformément aux spécifications.
« Fournisseur »	La personne ou entité (ou, pour le cas du groupement, les personnes ou entités) présentant une soumission en réponse a à la demande d'arrangements en matière d'approvisionnement (DAMA) délivrée par le Canada. Il ne sous-entend pas à inclure sa société mère, ses sociétés affiliées, filiales ou ses sous-traitants.
« Fournisseur de services d'infonuagique (« FSI ») »	Signifie entité qui possède, opère et maintient l'infrastructure physique sur laquelle la solution est hébergé et à travers laquelle la solution est distribué. Un FSI peut aussi être l'éditeur de service-logiciel dans la mesure où ils hébergent et distribuent leurs propres solutions ou celles de tiers.
« Fuite d'information »	Incidents dans lesquels un renseignement est placé accidentellement dans un bien ou un système n'ayant pas l'autorisation de le traiter (p. ex. ITSG-33, IR-9).
« Incident de sécurité »	Anomalie observable ou mesurable se rapportant à un bien et entraînant ou pouvant entraîner : (A) une violation des politiques de sécurité du Canada, d'une mesure de sécurité en particulier, des politiques ou des procédures de sécurité du fournisseur ou d'un de ses sous-traitants, ou de toute exigence des présentes obligations en matière de sécurité ou des obligations en matière de protection de la vie privée; (B) l'accès aux justificatifs d'un membre du personnel autorisé, aux justificatifs des utilisateurs finaux ou à des renseignements, ainsi que la modification ou l'exfiltration de ceux-ci, le tout sans autorisation.
« Infonuagique »	Modèle qui permet, de façon omniprésente, pratique et à la demande, l'accès réseau à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et

	services) qui peuvent rapidement être fournies et mises à jour tout en exigeant très peu d'efforts de gestion ou de contacts avec le fournisseur de services.
« Infrastructure du fournisseur »	Toute infrastructure fournie par le fournisseur ou un sous-traitant ultérieur de celui-ci qui est nécessaire à l'utilisation continue et au maintien des services.
« Infrastructure IaaS »	Infrastructure gérée par le fournisseur (ou un sous-traitant du fournisseur) dans l'objectif d'offrir un service IaaS (p. ex. centre de données, réseautage, stockage, serveurs, plateforme de virtualisation). Cela comprend également les systèmes, le matériel et les logiciels servant à gérer, à exploiter et à offrir une infrastructure IaaS.
« Infrastructure PaaS »	Infrastructure gérée par le fournisseur (ou un sous-traitant du fournisseur) dans l'objectif d'offrir un service PaaS (p. ex. centre de données, réseautage, stockage, serveurs, plateforme de virtualisation, système d'exploitation, intergiciel, Runtime). Cela comprend également les systèmes, le matériel et les logiciels servant à gérer, à exploiter et à offrir une infrastructure PaaS.
« Infrastructure SaaS »	Infrastructure gérée par le fournisseur (ou un sous-traitant du fournisseur) dans l'objectif d'offrir un service SaaS (p. ex. centre de données, réseautage, stockage, serveurs, plateforme de virtualisation, système d'exploitation, intergiciel, Runtime, données, applications). Cela comprend également les systèmes, le matériel et les logiciels servant à gérer, à exploiter et à offrir une infrastructure SaaS.
« jour ouvrable du gouvernement fédéral »	Est défini comme étant du lundi au vendredi, de 8 h à 16 h, heure normale de l'Est, excluant les jours fériés observés par le Canada.
« Lieu de prestation du service »	Toute installation ou tout site ou endroit que le fournisseur ou qu'un sous-traitant ultérieur du fournisseur possède, loue, fournit ou occupe autrement et à partir duquel le fournisseur ou tout sous-traitant ultérieur du fournisseur fournit des services.
« Logiciel » Programme	Informatique, micro logiciel, routine, code, instruction, script, macro, programmation d'application ou autre interface, outil, définition de l'affichage d'un document, bibliothèque d'objets, outil logiciel ou autre instruction ou ensemble d'instructions à suivre pour du matériel ou un autre logiciel, que ce soit en code source ou en code objet, exprimé dans un seul ou dans la totalité des langages, y compris des interfaces programme-homme intégrées, SQL et d'autres langages d'interrogation, langage HTML et d'autres langages de balisage informatiques.

« Nuage public »	Signifie que l'infrastructure cloud est mise à disposition pour une utilisation ouverte par le grand public. Il peut être détenu, géré et exploité par une entreprise, un universitaire ou un organisme gouvernemental, ou une combinaison de ces derniers. Il existe dans les locaux du fournisseur de cloud.
« Offert sur le marché »	Un produit ou un service que le public peut utiliser ou consommer et qui n'exige aucune modification ni aucun entretien pendant son cycle de vie.
« Partie »	Signifie le Canada, l'entrepreneur ou tout autre signataire du contrat; « parties » signifie l'ensemble d'entre eux.
« Prix du contrat »	Désigne le montant indiqué dans le contrat et devant être payé à l'entrepreneur pour l'exécution des travaux prévus, sans tenir compte des taxes applicables.
« Produit livrable » ou « produits livrables »,	Lorsqu'ils sont utilisés de façon générique, désigne toute partie distincte des travaux à exécuter pour le Canada.
« Registre des incidents de sécurité »	Tout incident, avis ou alerte qu'un dispositif, un système ou un logiciel peut techniquement produire en ce qui concerne son état, ses fonctions et ses activités. Les registres des incidents de sécurité ne se limitent pas aux dispositifs de sécurité; ils s'appliquent à tous les dispositifs, systèmes et logiciels ayant techniquement la capacité de produire des registres sur les incidents pouvant être utilisés dans les enquêtes sur la sécurité, les vérifications et les activités de surveillance. Voici une liste non exhaustive d'exemples de systèmes pouvant produire des registres des incidents de sécurité : pare-feu, systèmes de prévention d'intrusion, routeurs, commutateurs, filtrage de contenu, registres du flux de trafic d'un réseau, réseaux, services d'authentification, services de répertoire, protocoles DHCP, systèmes DNS, plateformes matérielles, plateformes de virtualisation, serveurs, systèmes d'exploitation, serveurs Web, bases de données, applications, pare-feu à couche application (couche 7).
« Renseignements »	La totalité des données du Canada, ce qui peut comprendre des renseignements personnels; s'entend de tout élément de données individuel des données du Canada.
« Renseignements personnels »	Renseignements, quels que soient leur forme et leurs supports, concernant un individu identifiable, au sens de l'article 3 de la Loi sur la protection des renseignements personnels. Il s'agit, par exemple, des renseignements relatifs à la race, à l'origine nationale ou ethnique, à la religion, à l'âge, à la situation de famille, à l'adresse, à l'éducation ainsi que les renseignements relatifs au dossier médical, au casier judiciaire, aux opérations financières et les antécédents professionnels. Les renseignements personnels comprennent aussi tout numéro ou symbole qui est propre à une personne, comme son numéro d'assurance sociale.

	Définition tirée du site Web des lois sur la justice du gouvernement du Canada: https://laws-lois.justice.gc.ca/fra/lois/P-21/section-3.html.
« Revendeur de valeur ajoutée (RVA) »	Signifie le fournisseur qui est la filiale, partenaire, revendeur de valeur ajoutée ou autres distributeurs de solution de logiciel-service. RVA ne signifie pas l'éditeur ou fournisseur du logiciel-service, ou le fournisseur de services d'infonuagique (« FSI ») qui est à la fois le fournisseur du logiciel-service entité ou personne autre que le fournisseur de services d'infonuagique qui présente une soumission en tant qu'un fournisseur ayant ses droits et obligations dans le cadre de demande d'arrangements en matière d'approvisionnement (DAMA).
« Services »	Signifie : (a) accorder des droits d'utilisation sur les applications logicielles («solution (s)») identifiées au appendice fournies à une ou à plusieurs solutions fournies ou hébergées par l'entrepreneur; (b) fournir la documentation de la solution; (c) assurer la maintenance, la mise à niveau et la mise à jour de la ou des solutions; (d) gérer les incidents et les défauts pour s'assurer que la ou les solutions fonctionnent aux niveaux de service applicables.
« Services de démarrage rapide »	Désigne la formation essentielle sur les meilleures pratiques, l'architecture, le déploiement, l'intégration de la conception opérationnelle, l'évolutivité et l'utilisation d'une solution dans l'environnement du GC.
« Service IaaS »	Composantes d'une infrastructure de services axées sur le client et gérées par le Canada (en tant que client) (p. ex. systèmes d'exploitation, intergiciels, Runtime, données, applications, administration).
« Services infonuagiques publics »	Les services infonuagiques publics font référence à un bassin partagé de modèles de services d'infonuagique configurables, offerts promptement et avec souplesse aux utilisateurs, à leur demande et en libre-service; ces services sont assurés par Internet depuis les serveurs du fournisseur, plutôt que depuis les serveurs installés dans l'établissement d'une entreprise. Les services infonuagiques publics ne comprennent pas les éléments suivants : (a) services gérés; (b) services de formation; (c) services infonuagiques privés ou offerts sur place; et

	(d) services professionnels ou services de consultation dépassant la portée des services de soutien publics habituellement offerts sur le marché.
« Service PaaS »	Désigne la capacité offerte au consommateur de se déployer sur l'infrastructure cloud ou des applications acquises créées à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur.
« Services publics et Approvisionnement Canada » ou « Travaux publics et Services gouvernementaux Canada »	s'entendent du ministère des Travaux publics et des Services gouvernementaux, comme énoncé dans la Loi sur le ministère des Travaux publics et des Services gouvernementaux.
« Solution » ou « solution de logiciel-service (« SaaS ») »	Désigne une application logicielle livrée selon un modèle de distribution de logiciels-service dans lequel un fournisseur de services applicatifs ou un fournisseur de services infonuagique met à la disposition des clients des applications logicielles hébergées de manière centralisée sur Internet, permettant ainsi l'accès à la solution mise à jour et actualisée, services de support technique, infrastructure de technologie de l'information sécurisée physiquement et électroniquement, inclus dans le service d'abonnement.
« Soumission »	Désigne les documents que le fournisseur soumet en réponse à la DAMA.
« Sous-traitant »	Toute personne à qui le fournisseur confie en sous-traitance la prestation des services du fournisseur, en tout ou en partie.
« Sous-traitant ultérieur »	Personne physique ou morale, autorité publique, organisme ou autre organisation effectuant le traitement des données personnelles au nom d'un contrôleur des données, le Canada.
« spécifications »	Désigne la description des exigences essentielles, fonctionnelles ou techniques liées aux travaux prévus au contrat, y compris les procédures permettant de déterminer si les exigences ont été respectées.
« Système »	Toute combinaison de matériel et de logiciel, y compris toute ligne de communication ou tout périphérique réseau servant à assurer la liaison entre cette combinaison de matériel et de logiciel se rapportant aux services.
« Taux d'escompte »	S'entend du taux d'intérêt fixé de temps en temps par la Banque du Canada qui représente le taux minimum auquel elle consent des avances à court terme aux membres de l'Association canadienne des paiements.

« Taux moyen »	Désigne la moyenne arithmétique simple du taux d'escompte en vigueur chaque jour, à 16 h, heure de l'Est, pour le mois civil immédiatement antérieur à la date de paiement.
« Taxes applicables »	S'entend de la taxe sur les produits et services (TPS), de la taxe de vente harmonisée (TVH) et de toute taxe provinciale, payable par le Canada, selon la loi, comme la taxe de vente du Québec (TVQ) en date du 1er avril 2013.
« Travaux »	Tous les efforts déployés pour produire un produit livrable ou pour accomplir ou fournir un service que le fournisseur doit offrir aux termes du contrat.
« Utilisateur »	Désigne toute personne autorisée par le client à utiliser le logiciel en vertu du contrat. Pour les besoins du présent contrat, le terme comprend tout employé, mandataire ou entrepreneur autorisé à utiliser le logiciel.
« Utilisateur final »	Le terme "utilisateur final" désigne le consommateur d'un bien ou d'un service.

APPENDICE C – OBLIGATIONS EN MATIÈRE DE SÉCURITÉ

Obligations en matière de sécurité

Les obligations du fournisseur contenues dans les présentes Obligations de sécurité doivent être transférées par le fournisseur aux Sous-traitants du Fournisseur, dans la mesure applicable à chaque Sous-traitant du fournisseur, étant donné la nature des services qu'il fournit au fournisseur.

1. Gestion du changement

(a) Le fournisseur doit, pendant toute la durée du Marché, prendre toutes les mesures nécessaires, par l'entremise des Procédures de gestion du changement de mettre à jour et de maintenir les exigences en matière de sécurité au besoin pour se conformer aux pratiques de sécurité des normes de l'industrie, pourvu que si ces modifications peuvent raisonnablement être apportées sans ressources additionnelles, le fournisseur doit les effectuer sans frais additionnel pour le Canada (c.-à-d. au moyen d'un ordre de modification à coût nul).

(b) Le fournisseur doit accepter d'informer le Canada de toutes les améliorations qui pourraient avoir une incidence sur les services dans le contrat, y compris les améliorations techniques, administratives ou tout autre type d'améliorations. Le fournisseur accepte d'offrir toutes les améliorations qu'il offre à ses clients en général dans le cadre de son service régulier, sans appendice pour le Canada.

2. Reconnaissance

Les parties reconnaissent que :

(a) Tous les biens et les actifs d'information sont assujettis à ces obligations en matière de sécurité.

(b) Nonobstant toute autre disposition de la présente annexe, les parties partagent la responsabilité de l'élaboration et du maintien des politiques, des procédures et des contrôles de sécurité relatifs aux biens et aux actifs d'information.

3. Transfert et récupération des données

Le fournisseur (palier 1 et 2) doit, à la demande du Canada :

(a) Extraire toutes les ressources d'information en ligne, presque en ligne et hors ligne, y compris, mais sans s'y limiter, les bases de données, le stockage d'objets et de fichiers, les configurations de systèmes, les journaux d'activités infonuagiques, le code source hébergé dans un dépôt de codes Canada, et des configurations de réseau permettant au client d'utiliser ces instructions pour migrer d'un environnement à un autre;

(b) Transfert sécurisé de tous les actifs d'information, y compris les métadonnées, dans un format lisible et utilisable par machine acceptable pour le Canada, conformément aux Lignes directrices sur les formats de fichier à utiliser pour transférer des ressources documentaires à valeur continue de Bibliothèque et Archives Canada (https://www.bac-lac.gc.ca/fra/services/gestion-ressources-documentaires-gouvernement/lignes-directrices/Pages/lignes-directrices-formats-fichier-transferers-ressources-documentaires.aspx).

4. Disposition des dossiers et remise des dossiers au Canada

(a) Le fournisseur (palier 1 et 2) doit, sur demande, éliminer ou réutiliser en toute sécurité les ressources (p. ex. l'équipement, le stockage des données, les fichiers et la mémoire) qui contiennent des actifs d'information et s'assurer que les données précédemment stockées ne peuvent être traitées par d'autres clients après leur diffusion. Cela touche toutes les copies des actifs d'information qui sont créées aux fins de disponibilité accrue et de reprise après sinistre. L'élimination ou la réutilisation des ressources par le fournisseur doit être harmonisée à l'un des documents suivants : (i) Manuel d'utilisation du Programme national de sécurité industrielle (DoD 5220.22-M6); (ii) Lignes directrices pour l'assainissement des supports (NIST SP 800-88); ou (iii) Effacement et dé-classification des supports d'information électroniques (CSTC ITSG-06).

(b) Le fournisseur doit fournir des preuves démontrant qu'il a réussi à effacer, à purger ou à détruire toutes les ressources, selon le cas, et qu'il est en mesure d'empêcher le rétablissement de tout système, de toute capacité (logiciel ou processus), de toute donnée ou de toute information retirés ou détruits après leur retrait de l'instance du Canada.

5. Surveillance continue

(a) Le fournisseur doit continuellement gérer, surveiller et maintenir la posture de sécurité de tous les biens, de l'infrastructure du fournisseur et des emplacements de service pendant toute la durée du contrat, et s'assurer que les services fournis au Canada sont conformes aux présentes obligations en matière de sécurité. Dans le cadre de l'obligation, l'entrepreneur doit:

(i) surveiller activement et continuellement les menaces et les vulnérabilités pesant sur les actifs, l'infrastructure du fournisseur, les emplacements de service ou les actifs d'information;

(ii) faire de son mieux pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le refus de service;

(iii) faire de son mieux pour détecter les attaques, les incidents de sécurité et autres événements anormaux;

(iv) détecter l'utilisation et l'accès non autorisés à tous les services, données et composants

pertinents aux services IaaS, PaaS ou SaaS du Canada;

(v) gérer et appliquer les correctifs et les mises à jour liés à la sécurité de manière opportune et systématique afin d'atténuer les vulnérabilités et de remédier à tout problème signalé publiquement dans les services ou les bibliothèques que les services utilisent, et fournir des avis préalables liés aux correctifs conformément aux engagements convenus relatifs au niveau de service;

(vi) répondre aux menaces et aux attaques contre les services du fournisseur, les contenir et veiller à la récupération; et

(vii) au besoin, prendre des contre-mesures proactives, y compris, des mesures préventives et d'intervention permettant d'atténuer les menaces.

(b) Les services de l'entrepreneur doivent permettre de copier les données des applications (IaaS, PaaS et SaaS) et le trafic réseau (IaaS et PaaS) du gouvernement du Canada dans les services infonuagiques hébergés et de les acheminer vers un emplacement prédéterminé (dans le nuage ou dans les locaux du gouvernement).

(c) Les services de l'entrepreneur doivent permettre au Canada de déployer et d'utiliser des logiciels de sécurité pour assurer la surveillance avancée et l'atténuation des cyber-menaces pour les services du Canada à l'échelle de l'hôte géré par le gouvernement et de la couche réseau, pour les composants gérés par le Canada seulement.

6. Notifications

(a) Le fournisseur doit fournir :

(i) une notification rapide de toute interruption qui peut avoir une incidence sur la disponibilité et le rendement du service (comme convenu entre les parties et indiqué dans l'énoncé de travail ou l'entente sur les niveaux de service [ENS]);

(ii) des bilans réguliers au sujet des procédures de restauration des services à un état opérationnel selon les ENS et les exigences en matière de disponibilité du système convenues, sous forme d'alertes transmises avant et après la mise en œuvre;

(iii) des alertes, des avis et des directives de sécurité liés au système d'information, par courriel, pour les vulnérabilités qui constituent une menace pour les services.

7. Intervention en cas d'incident de sécurité

(a) Si le fournisseur prend connaissance d'une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée des données ou l'accès accidentel ou illégal aux données du client ou des données personnelles du client pendant le traitement par le fournisseur (chacun étant un « incident de sécurité »), le fournisseur doit rapidement et sans tarder (i) informer le Canada de cet incident de sécurité; (ii) mener une enquête et fournir des renseignements détaillés sur cet incident de sécurité; (iii) prendre les mesures raisonnables pour atténuer les effets et les dommages découlant de l'incident de sécurité.

(b) Le fournisseur doit alerter et aviser promptement le Canada (par téléphone et par courriel) de toute compromission, de toute violation ou de toute preuve comme (i) un incident de sécurité,

(ii) une défectuosité liée à la sécurité d'un actif, (iii) l'accès irrégulier ou non autorisé à un actif, (iv) la copie à grande échelle d'un actif d'information ou (v) toute autre activité illégale recensée par le fournisseur, portant ce dernier à croire de manière raisonnable que le risque de compromission, d'atteinte à la sécurité ou à la vie privée est ou pourrait être imminent, ou si les mesures de protection existantes ont cessé de fonctionner, au cours de la période suivante (tous les jours, 24 heures par jour, 365 jours par année), et sans tarder, dans tous les cas, dans les 24 heures.

(c) Le fournisseur doit collaborer avec le Canada au confinement, à l'éradication et à la récupération des incidents de sécurité conformément au processus d'intervention en cas d'incident de sécurité du fournisseur et au Plan de gestion des événements de cyber sécurité du gouvernement du Canada (PGEC GC) (https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html). Notamment :

(i) ne permettre qu'aux représentants désignés du Canada :

1. de demander et de recevoir des renseignements liés à l'incident de sécurité et à tout actif d'information compromis (y compris, données des utilisateurs, journaux d'événements du système et de sécurité, saisies de paquets du réseau ou de l'hôte, journaux de composants de sécurité comme des systèmes de détection et de prévention d'intrusion et des pare-feu, etc.), dans un format non chiffré, à des fins de réalisation d'enquêtes;

2. d'assurer le suivi de l'état d'un événement signalé lié à la sécurité de l'information ou d'un incident de sécurité.

(ii) d'appuyer les efforts d'enquête du Canada dans le cas de toute compromission des utilisateurs ou des données du service relevé.

(d) Le fournisseur doit de plus :

(i) tenir un registre des violations de la sécurité comprenant une description de la violation de la sécurité, la durée, les conséquences de la violation, le nom de la personne ayant signalé la violation, et la personne à qui la violation a été signalée, et la procédure pour récupérer les données ou le service; et

(ii) assurer le suivi ou permettre au Canada d'assurer le suivi des divulgations d'actifs et de renseignements, y compris les données qui ont été divulguées, à qui, et à quel moment.

8. Preuve électronique et mises en suspens pour raisons juridiques

Le fournisseur doit (et doit, dans la mesure où cela s'applique compte tenu de la nature des services sous-traités fournis par chaque sous-traitant du fournisseur, exiger des sous-traitants qu'ils prennent des mesures raisonnables pour) s'assurer que les services offrent des fonctions de communication de la preuve électronique et de mises en suspens pour raisons juridiques pour les journaux des événements de sécurité afin de permettre au Canada de mener rapidement et efficacement des enquêtes de sécurité et de répondre aux demandes des tribunaux en matière de mises en suspens pour raisons juridiques.

9. Mise à l'essai de l'évaluation de sécurité

Le fournisseur doit disposer d'un processus qui permet au Canada d'effectuer une analyse de vulnérabilité ou un essai de pénétration non perturbateur et non destructif visant la partie canadienne des composantes du service dans l'environnement du fournisseur.

10. Sous-traitants

(a) L'entrepreneur doit fournir une liste de sous-traitants auxquels il pourrait faire appel pour exécuter n'importe quelle partie des services infonuagiques en fournissant la solution au Canada. La liste doit comprendre les renseignements suivants : i) le nom du sous-traitant; ii) la détermination des activités de qui seraient accomplies par le sous-traitant; et iii) le pays (ou les pays) où le sous-traitant exécuterait les activités requises pour appuyer les services infonuagiques publics.

(b) L'entrepreneur doit fournir une liste des sous-traitants dans les dix jours suivant la date d'attribution du contrat. L'entrepreneur doit aviser le Canada (en mettant à jour le site Web et en fournissant au client un mécanisme lui permettant d'obtenir un avis lié à cette mise à jour) au sujet de tout nouveau sous-traitant au moins 14 jours avant de fournir aux sous-traitants l'accès aux données du client ou aux données personnelles.

11. Gestion des risques de la chaîne d'approvisionnement

(a) L'entrepreneur doit prendre des mesures de sécurité pour atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI en vue de préserver la confiance en ce qui concerne la sécurité des sources des systèmes d'information et les composants de TI servant à offrir les logiciels-services. En font notamment partie la conception et la mise en œuvre de contrôles visant à atténuer et à contenir les risques liés à la sécurité des données par une séparation adéquate des tâches, un accès établi selon les fonctions des utilisateurs et un accès qui suit le principe du privilège minimal pour tout le personnel au sein de la chaîne d'approvisionnement.

(b) L'entrepreneur doit adopter une approche pour la gestion des risques de la chaîne d'approvisionnement, ce qui comprend la préparation d'un plan de gestion des risques de la chaîne d'approvisionnement qui concorde avec l'une des pratiques exemplaires suivantes décrites aux ID des exigences obligatoires O7 du palier 1 (Gestion des risques de la chaîne d'approvisionnement) et O11 du palier 2 de l'annexe A, Exigences de qualification :

(i) ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4);

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

(iii) Contrôle de sécurité ITSG-33 pour SA-12 lorsque les garanties de sécurité définies sont documentées dans un plan de gestion des risques liés à la chaîne d'approvisionnement.

(c) Dans les 90 jours suivant l'attribution du contrat, l'entrepreneur doit :

(a) Fournir un compte rendu indiquant que l'approche et le plan de gestion des risques liés à la chaîne d'approvisionnement ont été évalués indépendamment et validés par un tiers indépendant certifié selon les exigences de l'AICPA, de CPA Canada ou du régime de certification ISO.

OU

(b) Fournir au Canada une copie du plan de gestion des risques liés à la chaîne d'approvisionnement sur une base annuelle ou sur demande.

Dans le cas où l'entrepreneur est un éditeur de logiciels-services ayant recours à un fournisseur d'infrastructures-services approuvé par le gouvernement du Canada déjà conforme aux ID d'exigence obligatoire O7 du palier 1 et O11 du palier 2 de l'annexe A, Exigences de qualification, Gestion des risques liés à la chaîne d'approvisionnement dans les 90 jours suivant l'attribution du contrat, ledit éditeur doit fournir une liste de produits de technologie de communication de l'information (TCI) qui décrit l'équipement de TCI déployé dans l'environnement dudit fournisseur pour une évaluation de l'intégrité de la chaîne d'approvisionnement. Cette évaluation de l'intégrité de la chaîne d'approvisionnement sera effectuée au plus tôt tous les trois ans.

12. Processus d'intégrité de la chaîne d'approvisionnement en cours

(a) Les parties reconnaissent que, dans le cadre du présent contrat, le Canada considère la sécurité comme un facteur crucial et qu'une évaluation continue des logiciels-services sera nécessaire tout au long de la période visée par le contrat.

(b) Les parties reconnaissent que le Canada se réserve le droit d'examiner le logiciel-service natif de tout entrepreneur, en tout ou en partie, en tout temps, par souci d'intégrité de la chaîne d'approvisionnement. Cette reconnaissance n'oblige pas l'entrepreneur à participer à l'évaluation de l'intégrité de la chaîne d'approvisionnement.

(c) Tout au long du contrat, l'entrepreneur doit transmettre au Canada des renseignements sur toute violation des données du réseau de l'entrepreneur dont il a connaissance, qui amène a) un accès illégal au contenu du Canada emmagasiné sur le matériel informatique ou dans les installations de l'entrepreneur ou b) un accès non autorisé à ce matériel ou à ces installations lorsque, dans un cas comme dans l'autre, cet accès provoque une perte, une divulgation ou une modification du contenu du Canada relativement au transfert de propriété ou aux logiciels-services prévus par le présent contrat, qui compromettrait l'intégrité, la confidentialité, le contrôle des accès, la disponibilité, l'uniformité ou les mécanismes de vérification du système, des données ou des applications du Canada.

13. Changement de contrôle

(a) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle affectant l'entrepreneur (soit à l'entrepreneur lui-même, soit à l'un de ses parents, jusqu'au propriétaire final) peut être préjudiciable à la sécurité nationale, le Canada peut résilier le contrat sur une «Sans faute» en fournissant un avis à l'entrepreneur dans les 90 jours civils suivant la réception de l'avis de l'entrepreneur concernant le changement de contrôle. Le Canada ne sera pas tenu de fournir ses raisons de résilier le CONTRAT en relation avec le changement de contrôle, si le Canada détermine à sa discrétion que la divulgation de ces raisons pourrait elle-même porter atteinte à la sécurité nationale.

(b) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle affectant un sous-traitant (que ce soit le sous-traitant lui-même ou l'un de ses parents, jusqu'au propriétaire final) peut être préjudiciable à la sécurité nationale, le Canada avisera l'entrepreneur par écrit. de sa détermination. Le Canada ne sera pas tenu de motiver sa décision si le Canada détermine à sa discrétion que la divulgation de ces raisons pourrait elle-même porter atteinte à la sécurité nationale. L'entrepreneur doit, dans les 30 jours civils suivant la réception de la décision du Canada, prendre des dispositions pour qu'un autre sous-traitant, acceptable pour le Canada, fournisse la partie des services cloud fournie par le sous-traitant existant (ou l'entrepreneur doit livrer cette partie des services cloud lui-même). Si l'entrepreneur ne le fait pas dans ce délai, le Canada sera en droit de résilier le contrat sans faute en fournissant un avis à l'entrepreneur dans les 120 jours civils suivant la réception de l'avis original de l'entrepreneur concernant le changement de contrôle.

(c) Dans le présent article, la résiliation sans faute signifie qu'aucune des parties ne sera responsable envers l'autre à l'égard du changement de contrôle et de la résiliation qui en résulte, et le Canada ne sera responsable que du paiement des services reçus. jusqu'à la date effective de la résiliation.

(d) Malgré ce qui précède, le droit du Canada de résilier sans faute ne s'appliquera pas aux circonstances dans lesquelles il y a une réorganisation interne qui n'affecte pas la propriété de la société mère ultime ou de la société mère de l'entrepreneur ou du sous-traitant , selon le cas; autrement dit, le Canada n'a pas le droit de résilier le CONTRAT en vertu du présent article lorsque l'entrepreneur ou le sous-traitant continue, en tout temps, d'être contrôlé, directement ou indirectement, par le même propriétaire final.

APPENDICE D - OBLIGATIONS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

1. Demandes de propriété des données et de confidentialité

(a) Les données du client, y compris toutes les informations personnelles (PI), seront utilisées ou autrement traitées uniquement pour fournir les services, y compris à des fins compatibles avec la fourniture des services. L'entrepreneur ne doit en aucun cas utiliser ou traiter de données Canada ou en tirer des informations à des fins publicitaires ou à des fins commerciales similaires. Entre les parties, le client conserve tous les droits, titres et intérêts relatifs aux données du client. L'entrepreneur n'acquiert aucun droit dans les données du Canada, autres que les droits que le client accorde à l'entrepreneur pour fournir la solution au client.

(b) Toutes les données que l'entrepreneur stocke, héberge ou traite au nom du Canada demeurent la propriété du Canada. À la demande de l'autorité contractante, l'entrepreneur doit fournir des enregistrements de données personnelles dans les cinq jours ouvrables du gouvernement fédéral (ou sept jours ouvrables du gouvernement fédéral s'il est nécessaire de les récupérer à partir d'une sauvegarde / réplication hors site) dans un document Word ou Excel.

2. Aider à la réalisation de l'évaluation des incidences sur la vie privée au Canada

À la demande du responsable technique, l'entrepreneur doit aider le Canada à créer une évaluation des facteurs relatifs à la vie privée conformément à la Directive du Conseil du Trésor sur l'évaluation des facteurs relatifs à la vie privée (https://www.statcan.gc.ca/fra/about/pia) en aidant le Canada à fournir les documents justificatifs, y compris une EFVP fondamentale pour le Canada fournie par l'entrepreneur. L'entrepreneur accepte de fournir ce soutien dans les dix jours ouvrables suivant une demande ou dans un délai convenu par les parties en fonction de la complexité de la demande présentée par le Canada.

3. Atteinte à la vie privée

(a) L'entrepreneur doit alerter et informer promptement le responsable technique (par téléphone et par courriel) de toute compromission, violation ou tout élément de preuve la laissant croire raisonnablement que le risque de compromission, ou de violation, est imminent, ou pourrait l'être, ou si les garanties existantes ont cessé de fonctionner, pendant la période suivante (7 jours x 24 heures x 365 jours) et dans les limites des engagements de niveau de service détaillés dans l'Annexe D applicable - Accords sur les niveaux de service.

(b) Si l'entrepreneur prend connaissance d'une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des données sur le client ou à des informations personnelles lors du traitement par l'entrepreneur (chacun étant un «incident de sécurité»), le contractant doit promptement et sans retard indu:

(i) je. informer le Canada de l'incident de sécurité;

(ii) enquêter sur l'incident de sécurité et fournir au Canada des informations détaillées sur l'incident de sécurité; et

(iii) prendre des mesures raisonnables pour atténuer les effets et minimiser les dommages résultant de l'incident de sécurité.

(c) L'entrepreneur doit:

(i) Conserver un registre des violations de la sécurité avec une description de la violation, la période, les conséquences de la violation, le nom du journaliste et le destinataire de la violation, ainsi que la procédure de récupération des données; et

(ii) Suit ou permet au Canada de suivre les divulgations de données du Canada, y compris les données qui ont été divulguées, à qui et à quelle heure.

APPENDICE E – FORMULAIRE D'AUTORISATION DE TÂCHES

FORMULAIRE D'AUTORISATION DE TÂCHE (AT)					
Entrepreneur		**Numéro de contrat :**			
No d'engagement		**Code financier :**			
No d'autorisation de tâche (modification):		**Date d'émission :**	**Réponse au plus tard le :**		
1. Énoncé des travaux (activités, attestations et livrables)					
Voir ci-joint l'énoncé des travaux et les attestations requises.					
2. Période des services :	**De** (DATE) :		**À** (DATE) :		
3. Emplacement des travaux :					
4. Exigences de déplacement :					
5. Exigences linguistiques :					
6. Autres conditions/contraintes :					
7. Niveau d'attestation de sécurité exigé pour le personnel de l'entrepreneur :					
8. Réponse de l'entrepreneur :					
CATÉGORIE ET NOM DE LA RESSOURCE PROPOSÉE	**NUMÉRO DE DOSSIER DE SÉCURITÉ DE SPAC**	**TAUX QUOTIDIEN**	**NOMBRE ESTIMATIF DE JOURS**	**COÛT TOTAL**	

FORMULAIRE D'AUTORISATION DE TÂCHE (AT)				
			Coût estimatif	
			Taxes applicables	
			Total du coût de main-d'œuvre	
			Total des frais de déplacement et de subsistance	
			Prix ferme ou prix maximum de l'AT	
Signature de l 'entrepreneur				
Nom, titre et signature de la personne autorisée à signer au nom de **l'entrepreneur** (en caractères d'imprimerie) _____			Signature: _____ Date: _____	
Approval – Signing Authority Approbation - Pouvoir de signature				

FORMULAIRE D'AUTORISATION DE TÂCHE (AT)	
Signatures (client) Nom, titre et signature de la personne autorisée à signée : Responsable technique : _____ Date: _____	**Signatures (SPAC)** Autorité contractante [1]: _____ Date: _____
[1] Signature requise pour les projets d'une valeur de _____ $ ou plus, taxes applicables comprises.	
Vous êtes tenu de vendre à sa Majesté la Reine du Chef du Canada, conformément aux modalités établies ou mentionnées dans la présente ou ci-jointes, les services énumérés dans les présente et dans les documents ci-joints, aux prix établis.	

APPENDICE F – LVERS RELATIVE AUX LOGICIELS-SERVICES

(Insérer s'il y a lieu)

Remarque à l'intention des entrepreneurs : Des niveaux de sécurité différents ou supplémentaires peuvent s'appliquer aux clients qui utilisent l'AMA ou à leurs exigences de travail, comme les cotes de sécurité des fournisseurs ou des ressources de ceux-ci. Si un contrat attribué dans le cadre d'un AMA comporte des niveaux de sécurité différents ou supplémentaires, ceux-ci seront inclus à l'appendice I (LVERS) et à l'appendice J (Guide de classification) du contrat.

APPENDICE G – GUIDE DE CLASSIFICATION DE SÉCURITÉ

(Insérer s'il y a lieu)

Remarque à l'intention des entrepreneurs : Des niveaux de sécurité différents ou supplémentaires peuvent s'appliquer aux clients qui utilisent l'AMA ou à leurs exigences de travail, comme les cotes de sécurité des fournisseurs ou des ressources de ceux-ci. Si un contrat attribué dans le cadre d'un AMA comporte des niveaux de sécurité différents ou supplémentaires, ceux-ci seront inclus à l'appendice I (LVERS) et à l'appendice J (Guide de classification) du contrat.