



Item Article	Description	Dest. Code Dest.	Inv. Code Fact.	Qty Qté	U. of I. U. de D.	Unit Price/Prix unitaire		Del. Offered Liv. offerte
						Destination	FOB/FAM Plant/Usine	
2	NPP Amendment 01	EN578	EN578	1	LOT	\$	\$	See Herein
3	NPP Amendment	EN578	EN578	1	LOT	\$	\$	See Herein
4	RFI and Draft RFSA	EN578	EN578	1	LOT	\$	\$	See Herein
6	NPP D	EN578	EN578	1	LOT	\$	\$	See Herein

DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA)

CONCERNANT

LES SOLUTIONS DE LOGICIELS-SERVICES

TABLE DES MATIÈRES

1.1	PRÉAMBULE.....	4
1.2	SOMMAIRE.....	6
1.3	APERÇU DU PROCESSUS D'ÉVALUATION DE SOUMISSIONS.....	7
1.4	EXIGENCES RELATIVES À LA SÉCURITÉ.....	8
1.5	COMPTE RENDU.....	8
1.6	TERMES-CLÉS.....	8
PARTIE 2 – INSTRUCTIONS À L'INTENTION DES FOURNISSEURS.....		9
2.1	INSTRUCTIONS, CLAUSES ET CONDITIONS UNIFORMISÉES.....	9
2.2	PRÉSENTATION DES SOUMISSIONS.....	10
2.3	PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – AVIS.....	11
2.4	DEMANDES DE RENSEIGNEMENTS – DEMANDE D'ARRANGEMENTS EN MATIÈRE D'APPROVISIONNEMENT.....	11
2.5	LOIS APPLICABLES.....	11
2.6	FOURNISSEURS.....	12
PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS.....		13
3.1	INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS.....	13
3.2	SECTION I : SOUMISSIONS TECHNIQUE.....	13
3.3	SECTION II : SOUMISSION FINANCIÈRE.....	15
3.4	SECTION III : ATTESTATIONS.....	16
3.5	SECTION IV : PROCESSUS CONTINU D'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT.....	16
PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION.....		17
4.1	PROCÉDURES D'ÉVALUATION.....	17
4.2	ÉVALUATION TECHNIQUE ET FINANCIÈRE.....	17
4.3	PROCESSUS D'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT.....	17
4.4	MÉTHODE DE SÉLECTION.....	18
4.5	VIABILITÉ FINANCIÈRE.....	18
PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES.....		19
5.1	ATTESTATIONS EXIGÉES AVEC L'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT.....	19
5.2	ATTESTATIONS PRÉALABLES À L'ÉMISSION D'UN ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT ET RENSEIGNEMENTS SUPPLÉMENTAIRES.....	ERROR! BOOKMARK NOT DEFINED.
PARTIE 6 – ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT.....		20
6.1	ARRANGEMENT.....	20
6.2	EXIGENCES RELATIVES À LA SÉCURITÉ.....	20
6.3	CLAUSES ET CONDITIONS UNIFORMISÉES.....	20
6.4	DURÉE DE L'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT.....	21
6.5	RESPONSABLES.....	21
6.6	UTILISATEURS DÉSIGNÉS.....	22
6.7	OCCASION DE QUALIFICATION CONTINUE.....	22
6.8	ORDRE DE PRIORITÉ DES DOCUMENTS.....	22
6.9	ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES.....	22
6.10	LOIS APPLICABLES.....	22
PARTIE 7 – SÉLECTION DES ENTREPRENEURS ET CLAUSES DU CONTRAT SUBSÉQUENT.....		23
7.1	POUVOIR ADJUDICATEUR ET LIMITES.....	23
7.2	SÉLECTION DE L'ENTREPRENEUR.....	23
7.3	PROCÉDURES DE DEMANDE DE SOUMISSIONS.....	23
7.4	CLAUSES DU CONTRAT SUBSÉQUENT.....	24

ANNEXE A – EXIGENCES DE QUALIFICATION	25
ANNEXE B – OBLIGATIONS EN MATIÈRE DE SÉCURITÉ ET PROTECTION DE LA VIE PRIVÉE	5
ANNEXE C – CATALOGUE DE SOLUTIONS DE LOGICIELS-SERVICES ET PRIX PLAFONDS	13
ANNEXE D – ACCORDS SUR LES NIVEAUX DE SERVICE (ANS).....	14
ANNEXE E – MODÈLE DE DEMANDE DE SOUMISSION POUR LOGICIELS-SERVICES	15
ANNEXE F – CLAUSES DU CONTRAT SUBSÉQUENT	30
ANNEXE G – PROCESSUS D'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT	31
ANNEXE H – CHAÎNE D'APPROVISIONNEMENT ET ACCORD DE NON-DIVULGATION	34
FORMULAIRES	35
FORMULAIRE 1 – FORMULAIRE DE PRÉSENTATION DES SOUMISSIONS	35
FORMULAIRE 2 - FORMULAIRE D'ATTESTATION DE L'ÉDITEUR DE LOGICIELS-SERVICES	37
FORMULAIRE 3 - FORMULAIRE D'AUTORISATION DE L'ÉDITEUR DE LOGICIELS-SERVICES	38
FORMULAIRE 4 - ATTESTATION AUX FINS DU PROGRAMME DE MARCHÉS RÉSERVÉS AUX ENTREPRISES AUTOCHTONES.....	39
FORMULAIRE 5 - LIST DE VÉRIFICATION DE L'EXHAUSTIVITÉ DE LA SOUMISSION	40
FORMULAIRE 6 - MODÈLE DE SOUMISSION SCI.....	40

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 première phase 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.

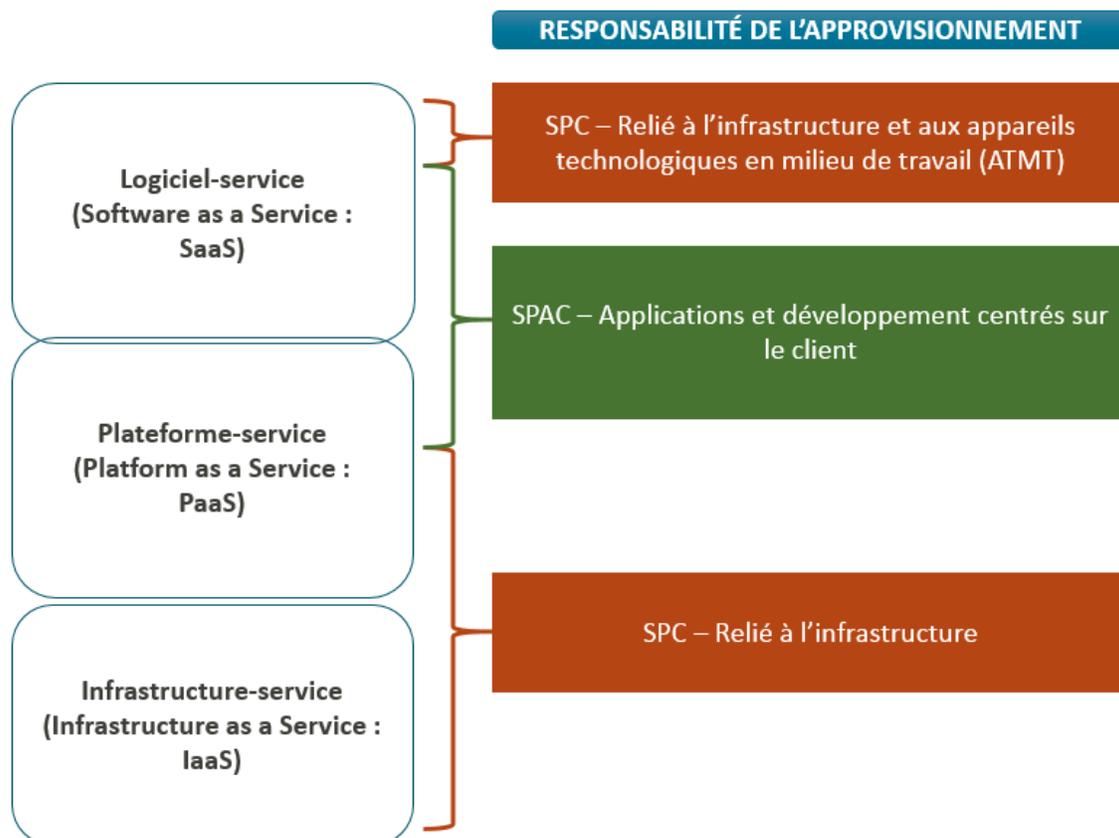
1.1.2 Organisation du GC pour assurer efficacement les achats des logiciels-services

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 (IaaS, PaaS).

Le rôle de SPAC en matière d'approvisionnement se situe principalement dans le domaine des applications logicielles et du développement (SaaS), 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 Exigences de sécurité, le Catalogue de logiciels-services et Prix plafond, les Accords sur les niveaux de service (ANS), et le Modèle de demande de soumission pour logiciels-services, clauses du contrat subséquent, processus d'intégrité de la chaîne d'approvisionnement et accord de non-divulgaration relatif à l'intégrité de la chaîne d'approvisionnement.

Remarque: Les mots en majuscules et les termes techniques utilisés dans la présente DAMA sont définis dans les Clauses du contrat subséquent - Appendix 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 de qualification des fournisseurs se déroulera comme suit:

Phase 1 : servira à évaluer les soumissions des fournisseurs proposant des solutions et de services-logiciels conformes aux exigences du Canada en matière de stockage et de traitement des informations Protégées B, comme indiqué à l'annexe A, Critères de qualification, Palier 2.

Phase 2 : servira à évaluer les soumissions des fournisseurs proposant des solutions et de services-logiciels 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, Qualifications requises, Palier 1.

Phase 3 : Les distributeurs à valeur ajoutée ne seront pris en compte que dans la phase 3.

Le Canada a l'intention de commencer à examiner les soumissions reçues au titre de la phase 1 le 17 juin 2019. Le Canada examinera d'abord les soumissions des fournisseurs de solutions et de services-logiciels hébergées par un fournisseur de services de services-logiciels «qualifié». Un fournisseur de services infonuagique «qualifié» a suivi le programme d'évaluation de la sécurité des TI des fournisseurs de services infonuagique ITS CCCS (<https://cyber.gc.ca/fr/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100>) et a satisfait à toutes les exigences de l'invitation de Services partagés Canada à se qualifier pour un véhicule d'approvisionnement en services d'informatique en nuage du gouvernement du Canada (Infonuagique GC) <https://achatsetventes.gc.ca/donnees-sur-l-approvisionnement/appels-d-offres/PW-18-00841719>. Les soumissions des fournisseurs dotés de

solutions et de services-logiciels qui ne sont pas hébergées par un fournisseur de services infonuagique «qualifié», y compris ceux des phases 2 et 3, seront examinées ultérieurement.

Le Canada se réserve le droit de modifier le processus d'évaluation des demandes et la séquence de hiérarchisation au sein et entre les phases ci-dessus à tout moment afin de répondre à ses besoins opérationnels.

1.4 Exigences relatives à la sécurité

La présente DAMA et les clauses du contrat subséquent comportent des exigences de sécurité, décrites en particulier à l'annexe A, Exigences de qualification et à l'annexe B - Obligations de sécurité et de confidentialité de la DAMA. 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, 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. Une soumission transmise 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.

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 assujéti 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 autorisés à proposer une soumission et à devenir un fournisseur en bonne et due forme. Les éditeurs de logiciels-services qui passent des marchés directement avec le Canada doivent soumettre le formulaire d'attestation de l'éditeur de logiciels-services (Formulaire 2).

b) Revendeurs de valeur ajouté en tant que fournisseurs: Les revendeurs de valeur ajouté sont éligibles à participer dans cette DAMA. Les revendeurs de valeur doivent soumettre le formulaire d'autorisation de l'éditeur de logiciels-services (Formulaire 3), attestant que le fournisseur a été autorisé à fournir les 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

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 claire 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).

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.

ANS qui s'appliquent à l'utilisation des Solutions de logiciels-services par le Canada 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 engagements en matière de niveau de service pour différentes Solutions de logiciels-services, il doit indiquer clairement la ou les Solutions de logiciels-services énumérées à l'annexe C – Catalogue de Solutions de logiciels-services et Prix Plafonds qui sont visées par les Accords sur les niveaux de service (ANS).

Les thèmes pouvant être traités dans les Accords sur les niveaux de service (ANS) de la Solution de logiciels-services peuvent inclure:

- A. la période durant laquelle le fournisseur offrira du soutien aux Clients;
- B. les coordonnées et les renseignements concernant la procédure pour accéder aux services de soutien;
- C. les procédures de résolution de problèmes;
- D. les temps de réponse;
- E. les procédures sur la façon et le moment de répondre à toutes les communications par téléphone, télécopieur ou courriel;
- F. la disponibilité du site Web de soutien pour les clients (par exemple: jour et nuit, 365 jours par an, 99.9 % du temps); et
- G. droits de maintenance (par exemple des correctifs, mises à jour majeures/mineures de presse, etc)

En soumettant une soumission en matière d'approvisionnement, le fournisseur reconnaît et accepte que toutes les modalités contenues dans l'annexe l'Annexe D - Accords sur les niveaux de service (ANS) de la Solution de logiciels-services visant à interpréter la DAMA, ou qui relèvent d'un sujet identique ou similaire ou en lien avec, les conditions contenues dans la DAMA et les clauses du contrat subséquent sont considérées comme nulles ou sans effet.

- (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 protection de la vie privée:** Les fournisseurs doivent se conformer aux obligations de sécurité et de confidentialité figurant à l'annexe B - Obligations en matière de sécurité et protection de la vie privée. Les fournisseurs doivent fournir les preuves écrites ou les documents de

certification attestant de leur conformité aux obligations en matière de sécurité et de confidentialité

- d) En présentant une soumission, le fournisseur reconnaît et accepte que toutes les autres conditions soumises dans le cadre de la soumission technique sont considérées comme nulles et ne font aucunement partie de l'AMA.

3.3 Section II : Soumission financière

- a) Dans la soumission financière, les fournisseurs doivent soumettre un catalogue de Solutions de logiciels-services comportant leurs prix commerciaux et rabais applicable en pourcentage ainsi que leurs prix ou tarifs applicables pour les services professionnels qui doivent être fournis par les fournisseurs, en plus de la ou des solutions logiciels-services proposées. La section Catalogue des solutions logiciels-services et des prix commerciaux de la soumission doit obligatoirement être soumise selon le modèle fourni dans en vertu du modèle fourni dans l'annexe C – Catalogue de Solutions de logiciels-services et de prix de la DAMA. Tous les documents de l'annexe C - Catalogue de Solutions de logiciels-services et de prix plafonds faisant partie de toutes les AMA émises dans le cadre de la présente DAMA seront utilisés pour créer un Catalogue de Solutions logiciels-services du GC. La soumission financière 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) Les renseignements suivants doivent figurer dans l'annexe C, Catalogue de Solutions de logiciels-services et de prix:
- (i) **N° 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:** 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) **Fournisseur de services d'infonuagiques :** Le fournisseur doit identifier le fournisseur de services infonuagiques (CSP) dont les services infonuagiques sont utilisés pour fournir au Canada la Solution de logiciel-service proposée.
 - (v) **Prix plafonds:** Le fournisseur doit soumettre les prix plafonds proposés à l'annexe C, Catalogue de Solutions de logiciels-services et prix plafonds. Les prix doivent respecter les conditions suivantes:
 - A. la tarification commerciale du fournisseur moins le pourcentage de rabais applicable
 - 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 entrez l'unité de mesure pour le logiciel-service, telle que «par utilisateur», «par entité», etc. et abonnement, durée;
 - (vii) **Rabais en pourcentage applicable:** Les fournisseurs doivent saisir le pourcentage de rabais qui sera appliqué aux prix unitaires commerciaux au plafond 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 qui seront utilisés dans la fonction de recherche pour aider les clients à repérer facilement des solutions de logiciels-services dans le catalogue qui répondent à leurs besoins.
- c) **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, indiquant l'escompte, en pourcentage, offert au Canada; ou
 - (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; ou
 - (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 soumettre des renseignements précis concernant chaque composante de la chaîne d'approvisionnement qu'ils proposent. Cette information est appelée (« Information sur la sécurité de la chaîne d'approvisionnement » ou « ISCA »), comme le précise la section 1.1 de l'**Annexe G, Processus d'intégrité de la chaîne d'approvisionnement**.
- (b) Les fournisseurs doivent soumettre l'information sur la sécurité de la chaîne d'approvisionnement dans le formulaire 6 - formulaire de soumission SCI. Le Canada utilisera cette information pour évaluer si, à son avis, la chaîne d'approvisionnement proposée par un soumissionnaire pourrait faire en sorte que la solution proposée par le soumissionnaire compromette ou serve à compromettre l'intégrité de la sécurité du matériel, des micrologiciels, des logiciels, des systèmes ou des renseignements lui appartenant, conformément à l'évaluation de l'ISCA décrite à l'**Annexe G, Processus d'intégrité de la chaîne d'approvisionnement**.
- (c) En soumettant ISCA, et compte tenu de cette opportunité à participer dans le processus d'acquisition, le fournisseur convient à se conformer aux conditions de l'accord de non-divulgence dans l'annexe X - Chaîne d'approvisionnement et accord de non-divulgence.

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

- a) 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 financière obligatoires sont les suivantes :

- (i) Solutions de logiciels-services et prix plafonds conformément aux paragraphes 3.3 (a) et (b);
et
- (ii) Référence(s) de prix conformément au paragraphe 3.3 (c).

4.3 Processus d'intégrité de la chaîne d'approvisionnement

Durant le processus de DAMA, la période de la chaîne d'approvisionnement et celle de contrat subséquent, l'autorité en matière de sécurité de la chaîne d'approvisionnement, comme identifié par le Canada, peut, sur la base du mandat en matière de la sécurité nationale consistant à protéger l'infrastructure informatique du Canada, évaluer les menaces, risques et vulnérabilités et de même pour le fournisseur SCI.

Le Canada évaluera si, à son avis, la chaîne d'approvisionnement du fournisseur crée la possibilité que la solution proposée par le soumissionnaire puisse compromettre ou soit utilisée pour compromettre l'intégrité de la sécurité de équipements, micro logiciels, logiciels, systèmes ou informations, conformément à la section 4 de l'annexe G, Processus d'intégrité de la chaîne d'approvisionnement.

Il est une condition préalable pour toute adjudication du contrat que le fournisseur doit satisfaire à l'évaluation de l'autorité en matière de sécurité de la chaîne d'approvisionnement

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 pour être déclaré recevable.

4.4 Viabilité financière

Clause du *Guide des CCUA* [S0030T](#) (2014-11-27) Viabilité financière.

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 fautive, 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 rejeté 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 et à l'annexe B - Obligations en matière de protection de la vie privée.

Remarque aux fournisseurs: Cette DAMA contient des exigences obligatoires à respecter pour la qualification. 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 incluses 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 :

Premier trimestre : du 1er avril au 30 juin;

Deuxième trimestre : du 1er juillet au 30 septembre;
Troisième trimestre : du 1er octobre au 31 décembre;
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 : A/Supply Team Leader

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

Les Terrasses de la Chaudière
10, rue Wellington, 4^{ème} 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 chaîne d'approvisionnement

L'autorité sur la sécurité de la chaîne d'approvisionnement pour le contrat est:

Nom: _____
Titre: _____
SSC : _____
Adress: _____
Telephone: _____
Courriel: _____

L'autorité sur la sécurité de la chaîne d'approvisionnement est le représentant de SSC et est responsable pour ce qui concerne au processus d'intégrité sur la chaîne 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 chaîne 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 F, Clauses du contrat subséquent;
- f) Annexe E, Modèle de demande de soumission pour logiciels-services;
- g) Annexe G, Processus d'intégrité de la chaîne d'approvisionnement; et
- h) Annexe H, Chaîne d'approvisionnement et accord de non-divulgence
- i) soumission du fournisseur daté du _____ (*insérer la date de la soumission*), (*si la soumission a été clarifiée ou modifiée, 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.

Annexe A – Exigences de qualification

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

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

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
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: (i) la gestion des comptes; (ii) la protection des frontières; (iii) la sauvegarde des actifs et du système d'information; iv) la gestion des incidents; (v) la surveillance du système; et (vi) 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); 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/nato/hq/nato_countries.htm .	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 : 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.

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	Besoin	Obligation de démontrer la conformité au niveau 1
O3	Installations des centres de données	<p>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.</p> <p>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-sr/international-fra.html de SPAC, tel qu'il est mis à jour de temps à autre.</p>	<p>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.</p>
		<p>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 récupération préventive en matière de sécurité physique.</p> <p>Cette description doit inclure, à tout le moins, les éléments qui suivent :</p> <ul style="list-style-type: none"> a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, qui sont suffisamment dispersées 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; 	<p>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 de la section XX, Exigences relatives aux installations du centre de données. Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> 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 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. <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O4	Sécurité du personnel	<p>f) l'accompagnement des visiteurs et la surveillance de leur activité;</p> <p>g) la tenue des registres de vérification de l'accès physique;</p> <p>h) le contrôle et la gestion des dispositifs d'accès physique;</p> <p>i) l'application des mesures de protection des données du GC à d'autres lieux de travail (p. ex., les sites de télétravail); et</p> <p>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.</p>	
	Sécurité du personnel	<p>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.</p> <p>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 :</p> <p>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;</p> <p>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;</p> <p>c) le processus relatif à la sensibilisation et à la formation en matière de sécurité dans le cadre de l'intégration à</p>	<p>Le fournisseur doit présenter une documentation démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences de la relatives à la sécurité du personnel.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>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.</p> <p>b) Les exigences relatives à la sécurité du personnel, 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 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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O5	Assurance d'une tierce partie	<p>l'emploi et lorsque les rôles des employés et des sous-traitants changent;</p> <p>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</p> <p>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.</p> <p>Le logiciel-service doit être conçu et développé pour assurer la sécurité du logiciel-service public commercial proposé, y compris la mise en œuvre de politiques, de procédures et de contrôles de sécurité de l'information.</p>	<p>Le fournisseur doit présenter une documentation au Canada démontrant la façon dont le fournisseur du logiciel-service public commercial respecte les exigences relatives l'assurance d'une tierce partie. La conformité doit être démontrée par la présentation d'au moins une des certifications de l'industrie énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants.</p> <p>Le fournisseur doit présenter les certifications suivantes de l'industrie afin de démontrer la conformité du service proposé :</p> <p>1) l'une des certifications suivantes :</p> <p>i) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences,</p> <p>ii) contrôle de l'organisation des services (SOC) de l'AICPA – rapports des SOC 2 de type II;</p> <p>2) 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).</p> <p>Chaque rapport de certification et d'évaluation fourni doit :</p> <p>a) être valide à la date de clôture de la soumission,</p> <p>b) 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,</p> <p>c) indiquer la date ou l'état de la certification actuelle,</p> <p>d) comprendre la liste des biens, de l'infrastructure du fournisseur et des emplacements de service dans le cadre du rapport de certification,</p> <p>e) indiquer les emplacements et les services offerts par le fournisseur proposé. Si la méthode déterminée est utilisée pour exclure les</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoins	Obligation de démontrer la conformité au niveau 1
O6	Gestion de la chaîne d'approvisionnement	<p>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.</p> <p>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.</p> <p>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 logiciel-service qui ont été proposés par le fournisseur.</p> <p>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.</p>	<p>organisations de services en sous-traitance, comme l'hébergement de centres de données, le rapport d'évaluation de l'organisation sous-traitante doit être inclus, et</p> <p>f) être délivré par un tiers indépendant qualifié au titre de l'AICPA ou de CPA Canada ou du régime de certification ISO, et respecter la norme ISO/IEC 17020 relativement aux systèmes de gestion de la qualité.</p> <p>Remarque :</p> <ul style="list-style-type: none"> • 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. <p>Le fournisseur doit fournir une liste de documentation des sous-processes 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-processus; (ii) l'identification des activités de périmètre qui seraient réalisées par le sous-processus; et (iii) le ou les emplacements où le sous-processus effectuerait les activités requises pour prendre en charge les services.</p> <p>1) Pour le SaaS, le contractant doit démontrer que l'aaS/PaaS est mis à profit par ces services:</p> <p>a) Les sous-processus des fournisseurs ont été évalués conformément par le programme CCCS; et</p> <p>b) Le fournisseur respecte les obligations de sécurité des sous-processus et/ou des sous-traitants énoncés dans les exigences pendant toute la durée du contrat.</p> <p>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.</p>
O7	Gestion des risques de la chaîne d'approvisionnement	<p>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</p>	<p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O8	Gestion de l'accès privilégié	<p>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.</p>	<p>Pour être jugée conforme, la documentation fournie doit démontrer la conformité du fournisseur à l'une des trois normes suivantes :</p> <ol style="list-style-type: none"> 1. ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur (parties 1 à 4); <p>ou</p> <ol style="list-style-type: none"> 2. publication spéciale 800-161 du NIST – <i>Supply Chain Risk Management Practices for Federal Information Systems and Organizations</i> (pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes d'information et organisations du fédéral); <p>ou</p> <ol style="list-style-type: none"> 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 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.
		<p>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 :</p> <ol style="list-style-type: none"> 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) ayant un identifiant, une authentification et une autorisation uniques; 	<p>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 :</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ol style="list-style-type: none"> 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. <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
		<p>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 :</p> <ul style="list-style-type: none"> 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); <p>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);</p> <p>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;</p> <p>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;</p> <p>i) adhérer aux principes du moindre privilège et du besoin de savoir pour accorder l'accès aux services et aux renseignements;</p> <p>j) contrôler l'accès aux objets stockés et aux politiques d'autorisation granulaires pour autoriser ou limiter l'accès;</p> <p>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;</p> <p>l) mettre en place un processus automatisé pour effectuer une vérification périodique de la création, de la</p>	

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
		<p>modification, de l'activation, de la désactivation et de la suppression de comptes, au minimum; et</p> <p>m) révoquer, en cas de cessation d'emploi, les authenticateurs et les justificatifs d'accès associés au personnel de service.</p>	

ID de l'exigence obligatoire	Sous-catégorie	Besoins	Obligation de démontrer la conformité au niveau 1
O9	<p>Fédération de l'identité</p>	<p>Fédération de l'identité</p> <p>Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment :</p> <ul style="list-style-type: none"> 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 authenticateurs 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. 	<p>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.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O10	Protection des points d'extrémité	<p>Protection des points d'extrémité</p> <p>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.</p>	<p>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.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>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.</p> <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O11	Développement sécurisé	<p>Développement sécurisé</p> <p>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.</p>	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Développement sécurisé.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>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.</p> <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoins	Obligation de démontrer la conformité au niveau 1
O12	Gestion à distance du fournisseur	<p>Gestion à distance des fournisseurs</p> <p>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:</p> <p>(a) Mettre en œuvre des mécanismes d'authentification multifacteurs 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);</p> <p>(b) Employer un algorithme cryptographique approuvé par le CSTC pour protéger la confidentialité des sessions d'accès à distance;</p> <p>(c) acheminez tous les accès à distance via des points de contrôle d'accès contrôlés, surveillés et vérifiés;</p> <p>(d) déconnecter ou désactiver rapidement les connexions de gestion à distance ou d'accès à distance non autorisées;</p> <p>(e) Autoriser l'exécution à distance de commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.</p>	<p>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.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>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.</p> <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoins	Obligation de démontrer la conformité au niveau 1
O13	<p>Fuite d'information</p>	<p>Fuite d'information</p> <p>1) Le fournisseur doit fournir au Canada un document décrivant le processus qu'il suit pour répondre à un 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 des principaux fournisseurs de services 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 :</p> <p>a) un processus d'identification du renseignement précis impliqué dans la contamination d'un actif ou d'un système;</p> <p>b) un processus visant à isoler et à éradiquer un renseignement ou un système contaminé;</p> <p>c) un processus d'identification des renseignements ou des systèmes pouvant avoir été subseqüemment contaminés et de toute autre mesure prise pour empêcher la propagation de la contamination.</p> <p>2) Le fournisseur doit transmettre au Canada un processus d'intervention en cas de fuite d'information à jour, et ce, chaque année ou après toute modification apportée au processus de gestion de ces incidents.</p>	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fuite d'information.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>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.</p> <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O14	Protection Cryptographique	<p>Protection cryptographique</p> <p>Le fournisseur doit fournir au Canada un document décrivant le processus suivi pour répondre à une protection cryptographique de l'information.</p> <p>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;</p> <p>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-isp40111);</p> <p>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/), dans un 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</p> <p>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.</p>	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection Cryptographique.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>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.</p> <p>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.</p> <p>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.</p>

ID de l'exigence obligatoire	Sous-catégorie	Besoin	Obligation de démontrer la conformité au niveau 1
O15	Séparation des données	<p>Le fournisseur doit, pour les deux pays, 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:</p> <ul style="list-style-type: none"> 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. 	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences.</p>

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).

2. 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: (i) la gestion des comptes; (ii) la protection des frontières; (iii) la sauvegarde des actifs et du système d'information; (iv) la gestion des incidents; (v) la surveillance du système; et (vi) 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.	<p>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.</p> <p>1) Pour être jugés conformes, les documents doivent comporter les éléments suivants :</p> <p>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 compte principal du GC utilisés pour établir l'environnement infonuagique du GC.</p> <p>b) Pour les exigences, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur de logiciel-service commercialement disponible propose 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</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O3	Isolation de la protection des données	<p>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 :</p> <ul style="list-style-type: none"> a) un centre de données situé physiquement au Canada; b) un centre de données qui répond à toutes les exigences de sécurité et certifications énoncées dans les exigences relatives aux installations des centres de données. <p>Exigences relatives aux installations des centres de données:</p> <p>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 l'ISG-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).</p> <p>Cela comprend au minimum :</p>	<p>de référence dans la réponse, y compris le titre du document, ainsi que les numéros de page et de paragraphe.</p> <p>c) 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.</p> <p>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.</p> <p>Pour être jugés conformes, les documents doivent comporter les éléments suivants :</p> <ul style="list-style-type: none"> 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 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. <p>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.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O4	Séparation des données	<p>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;</p> <p>b) l'utilisation adéquate des supports de TI;</p> <p>c) le contrôle de la maintenance des systèmes d'information et de leurs composants pour protéger leur intégrité et assurer leur disponibilité continue;</p> <p>d) le contrôle de l'accès aux dispositifs de sortie des systèmes d'information pour empêcher l'accès non autorisé aux données du Canada;</p> <p>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;</p> <p>f) l'escorte des visiteurs et la surveillance de leurs activités;</p> <p>g) la tenue de registres de vérification de l'accès physique;</p> <p>h) le contrôle et la gestion des dispositifs d'accès physique;</p> <p>i) l'application de mesures de protection des données du Canada à d'autres lieux de travail (p. ex., les sites de télétravail);</p> <p>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.</p>	
		<p>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:</p>	<p>Le fournisseur doit fournir une documentation démontrant que le fournisseur des services proposés se conforme aux exigences.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O5	Protection des données	<p>(a) la séparation entre l'administration interne du fournisseur et les ressources utilisées par ses clients; et</p> <p>(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.</p> <p>Le fournisseur du logiciel-service commercialement disponible 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 de redondance, à l'intérieur des frontières géographiques du Canada.</p> <p>Cela comprend les éléments suivants :</p> <p>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;</p> <p>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;</p> <p>c) garantir l'impossibilité de trouver les données d'un client précis sur les supports physiques;</p> <p>d) utiliser le cryptage pour veiller à ce qu'aucune donnée ne soit inscrite sur le disque de manière non cryptée.</p> <p>Remarque à l'attention des fournisseurs :</p> <p>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</p>	<p>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.</p> <p>Pour être jugés conformes, les documents doivent comporter les éléments suivants :</p> <p>a) des captures d'écran du centre de données disponibles dans lesquelles les centres de données canadiens figurent sur la liste de la disponibilité;</p> <p>b) une liste ou une carte indiquant l'emplacement géographique des centres de données au Canada.</p> <p>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.</p> <p>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.</p>
O6	Installations des centres de données	<p>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,</p>	<p>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.</p> <p>Pour être jugés conformes, les documents doivent comporter les éléments suivants :</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		<p>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:</p> <ul style="list-style-type: none"> 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 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. 	<p>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.</p> <p>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.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O7	Sécurité du personnel	<p>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 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.</p> <p>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 :</p> <ul style="list-style-type: none"> 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 données du GC ou de dommage à la fiabilité des services d'infonuagique hébergeant les actifs et données du GC. 	<p>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.</p> <p>Pour être jugés conformes, les documents doivent comporter les éléments suivants :</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p>
O8	Assurance d'une tierce partie	<p>Le logiciel sous forme de service commercialement disponible doit être conçu et élaboré pour garantir la sécurité du logiciel-service commercialement disponible proposé et comprendre la mise en œuvre de politiques et de procédures sur la sécurité de l'information et de mesures de contrôle de la sécurité.</p> <p>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</p>	<p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		<p>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.</p> <p>La conformité sera validée et vérifiée par le biais du processus d'évaluation du Centre canadien de cyber sécurité (CCCS), du fournisseur de services cloud (CSP), de la sécurité des technologies de l'information (TI) (ITSM.50.100) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux).</p> <p>Tout fournisseur ayant participé au processus doit fournir une documentation confirmant qu'il a terminé le processus d'intégration avec (i) une copie du rapport d'évaluation complété le plus récent fourni par CCCS; et (ii) une copie du dernier rapport de synthèse fourni par CCCS. Cela accélérera le processus de qualification et ne demandera pas au fournisseur de démontrer la conformité</p> <p>Pour lancer le processus d'intégration, le fournisseur doit contacter le service clientèle de CCCS pour recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire relative au programme d'évaluation informatique du CSP.</p>	<p>Le fournisseur doit fournir chacune des certifications suivantes de l'industrie pour démontrer sa conformité :</p> <ol style="list-style-type: none"> 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. <p>Chaque certification ou rapport d'évaluation doit :</p> <ol style="list-style-type: none"> a) être valide à la date de clôture de la demande de soumissions; 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. <p>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 compléter les allégations de certifications ci-dessus, afin de démontrer la conformité au Profil des mesures de sécurité pour les services de la TI du GC</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O9	Programme d'évaluation de la sécurité des TI	<p>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.</p>	<p>fondés sur l'informatique en nuage pour les renseignements classés Protégé B, intégrité moyenne et disponibilité moyenne (PBMM).</p> <p>Remarque :</p> <ul style="list-style-type: none"> Des certifications doivent être fournies pour toutes les parties des services proposés. Les certifications doivent être accompagnées de rapports d'évaluation.
		<p>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.</p> <p>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.</p> <p>La mise en correspondance des mesures de sécurité doit inclure :</p> <p>le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage;</p> <p>la certification de l'industrie en matière d'assurance par un tiers;</p> <p>la mise en correspondance entre le Profil des mesures de sécurité pour les services de TI du GC fondés sur l'informatique en nuage et la certification de l'industrie en matière d'assurance de tiers.</p>	

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O10	Gestion de la chaîne d'approvisionnement	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>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 :</p> <ul style="list-style-type: none"> (i) des sous-traitants du fournisseur; (ii) des sous-traitants de sous-traitants du fournisseur en aval de la chaîne; iii) toute filiale. <p>Le fournisseur doit remplir le formulaire 6 - Modèle de soumission SCI tel que fourni dans la présente DAMA.</p> <p>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.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O11	Gestion des risques de la chaîne d'approvisionnement	<p>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.</p>	<p>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.</p> <p>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.</p> <ol style="list-style-type: none"> 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. <p>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.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O12	Confidentialité	<p>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:</p> <p>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.</p> <p>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.</p>	<p>Pour démontrer la conformité à la certification, le fournisseur doit fournir:</p> <p>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</p> <p>b) Une copie du rapport d'évaluation ISO 27018 de logiciels-services commercialement disponible et de services et de services cloud.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O13	Confidentialité par conception	<p>Le fournisseur doit démontrer qu'il:</p> <ul style="list-style-type: none"> a) met en œuvre un cycle de vie de développement logiciel conforme à la norme ISO 27032 et et met en œuvre la confidentialité par la conception ; b) est conforme au cadre de gestion de la confidentialité et aux exigences de la politique spécifiées dans la norme ISO 29100; et c) Adhère à la confidentialité dès la conception des 7 principes fondamentaux (voir https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf). 	<p>Le fournisseur doit fournir une documentation démontrant que le fournisseur des services proposés se conforme aux exigences.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
O14	Gestion d'accès privilégié	<p>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 :</p> <ul style="list-style-type: none"> a) gérer et surveiller l'accès privilégié aux services d'infonuagique pour s'assurer que toutes les interfaces de service dans un environnement à locaux 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 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; 	<p>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 :</p> <p>Pour être jugés conformes, les documents doivent comporter les éléments suivants :</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au palier 2
		<p>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;</p> <p>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;</p> <p>j) mettre en place des contrôles d'accès aux objets stockés et des politiques d'autorisation granulaires pour autoriser ou limiter l'accès;</p> <p>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;</p> <p>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</p> <p>m) révoquer, en cas de cessation d'emploi, les authentifiants et les justificatifs d'accès associés au personnel chargé des services.</p>	

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
O15	Fédération de l'identité	<p>Fédération de l'identité</p> <p>Le fournisseur doit permettre au Canada de soutenir l'intégration de l'identité fédérée. Pour ce faire, il doit notamment :</p> <ul style="list-style-type: none"> 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 authenticateurs 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. 	<p>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.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p>
O16	Protection des points d'extrémité	<p>Protection des points d'extrémité</p> <p>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.</p>	<p>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.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <ul style="list-style-type: none"> b) 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. <p>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</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
O17	Développement sécurisé	<p>Développement sécurisé</p> <p>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.</p>	<p>documents mentionnés, leur titre et les numéros de page et de paragraphe.</p> <p>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.</p> <p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Développement sécurisé.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>c) 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.</p> <p>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.</p> <p>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.</p>
O18	Gestion à distance du fournisseur	<p>Gestion à distance des fournisseurs</p> <p>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:</p> <p>(a) Mettre en œuvre des mécanismes d'authentification multi-facteurs pour authentifier les utilisateurs d'accès distant,</p>	<p>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.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>a) les documents sur le système ou la documentation technique décrivant et détaillant les mesures de sécurité, y compris les</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
		<p>conformément au ITSP.30.031 V2 du CST (ou versions ultérieures) (https://www.cse-cst.gc.ca/fr/node/1842/html/26717);</p> <p>(b) Employer un algorithme cryptographique approuvé par le CSTC pour protéger la confidentialité des sessions d'accès à distance;</p> <p>(c) acheminez tous les accès à distance via des points de contrôle d'accès contrôlés, surveillés et vérifiés;</p> <p>(d) déconnecter ou désactiver rapidement les connexions de gestion à distance ou d'accès à distance non autorisées;</p> <p>(e) Autoriser l'exécution à distance de commandes privilégiées et l'accès à distance aux informations relatives à la sécurité.</p>	<p>politiques, processus et procédures mis en œuvre pour la protection de la fédération de l'identité.</p> <p>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.</p> <p>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.</p>
O19	Fuite d'information	<p>Fuite d'information</p> <p>a) Le fournisseur doit fournir au Canada un document décrivant le processus qu'il suit pour répondre à un 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</p> <p>b) ii) à une autre pratique exemplaire des principaux fournisseurs de services 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 : un processus d'identification du renseignement précis impliqué dans la contamination d'un actif ou d'un système;</p> <p>c) un processus visant à isoler et à éradiquer un renseignement ou un système contaminé;</p> <p>d) un processus d'identification des renseignements ou des systèmes pouvant avoir été subsequment contaminés et de toute autre mesure prise pour empêcher la propagation de la contamination.</p> <p>c) Le fournisseur doit transmettre au Canada un processus d'intervention en cas de fuite d'information à jour, et ce, chaque année ou après toute modification apportée au processus de gestion de ces incidents.</p>	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Fuite d'information.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>b) 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.</p> <p>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.</p> <p>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.</p>

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 1
O20	Protection Cryptographique	<p>Protection cryptographique</p> <p>Le fournisseur doit fournir au Canada un document décrivant le processus suivi pour répondre à une protection cryptographique de l'information.</p> <p>e) 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;</p> <p>f) 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.40.11 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-itsp4011);</p> <p>g) 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/), dans un 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</p> <p>h) 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</p>	<p>Le fournisseur doit fournir une documentation démontrant la façon dont le fournisseur des services proposés se conforme aux exigences de la Protection Cryptographique.</p> <p>Pour être jugée conforme, la documentation fournie doit inclure :</p> <p>c) 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.</p> <p>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.</p> <p>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.</p>

Annexe B – Obligations en matière 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

- a. 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 biens et les actifs d'information, comme suit :
 - (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 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; et
 - (iii) Chaque vérification sera effectuée par un vérificateur tiers qualifié et 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 17 020 sur les systèmes de management de la qualité à la sélection et aux frais du fournisseur.
- b. Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être communiqué au Canada. Le rapport de vérification doit indiquer clairement toutes les constatations importantes faites par le vérificateur externe. 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 constatation négative découlant de ces rapports et (ii) fournir au Canada, sur demande, des rapports d'étape sur la mise en œuvre dans les dix (10) jours ouvrables du gouvernement fédéral.

6. Interface de programmation d'application (API)

Le fournisseur 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.
- c) Pour la solution logiciel-service, le fournisseur doit fournir des API qui permettent:
 - (i) d'interroger des données inactives dans des applications de la solution logiciel-service; et
 - (ii) 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 (Palier 1 et 2) 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, et en utilisant des algorithmes et des certificats cryptographiques pris en charge, comme le décrit 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;
- b) Fournit une protection des données en transit entre les microservices et les applications utilisées au sein des Services;
- c) Utiliser des certificats correctement configurés dans les connexions TLS conformément aux directives du CST.
- d) Désactiver les protocoles vulnérables connus, comme toutes les versions de Secure Sockets Layer (SSL) (p. ex. SSLv2 et SSLv3) et toutes les versions antérieures de TLS (p. ex. TLS 1.0 et TLS 1.1), conformément à la norme ITSP.40.062 du CST, ainsi que les modes de chiffrement vulnérables connus (p. ex. RC4 et 3DES); et
- e) 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.

8. 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 autorisée 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.).

9. 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.

10. 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 télémessure, 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.

11. 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.

12. 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;

- b) 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.
 - (i) 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.

13. 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.

14. Respect de la vie privée

- (1) Le fournisseur doit démontrer à travers le rapport d'évaluation par la partie indépendante et le rapport d'audit qui :
 - (a) limite la création, collection, réception, gestion, d'accès, possession, d'envoi, divulgation et disposition de l'information personnelle, et permettre uniquement dans la mesure de la nécessité pour exécuter le travail et,
 - (b) mis en place des processus et des contrôles de sécurité actualisés tels que les contrôles de gestion des accès, la sécurité des ressources humaines, la cryptographie et la sécurité physique, opérationnelle et des communications, afin de préserver l'intégrité, la confidentialité et l'exactitude de toutes les informations et données, ainsi que des métadonnées, quel que soit leur format.
- (2) 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 compter 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. Cela est également nécessaire pour garantir que les informations, les données et les métadonnées peuvent être utilisées comme preuves convaincantes devant un tribunal.

15. Agent de protection de la vie privée

- (1) Dans les 10 jours suivant l'émission de l'arrangement en matière d'approvisionnement, le fournisseur doit fournir au Canada les informations permettant d'identifier une personne, en tant qu'agent de la protection de la vie privée, qui agira en tant que représentant de l'entrepreneur pour toutes les questions liées aux informations personnelles et aux enregistrements. 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 – Catalogue de Solutions de logiciels-services et Prix Plafonds

Remarque à l'intention du fournisseur : Ce formulaire doit être rempli et joint à la soumission du fournisseur dans le cadre de DAMA.

LISTE DE PRODUITS ET PRIX PLAFOND										
N° d'article	N° de pièce de la Solution de logiciels-services	Nom de la Solution de logiciels-services	Nom de l'éditeur de logiciel	Fournisseur de services infonuagiques	Prix unitaire plafonné	Unité de mesure	Remise en pourcentage applicable	Langues	Information sur la Solutions de logiciels-services	Mots-clés / tags
	(inscrire le numéro de pièce utilisé pour identifier la Solution de logiciels-services)	(indiquer le nom commercial utilisé pour identifier la Solution de logiciels-services)	(inscrire le nom de l'éditeur de logiciel qui possède les droits de propriété intellectuelle de la Solution de logiciels-services)	(identifier le fournisseur de services infonuagiques (CSP) dont les services infonuagiques sont utilisés pour fournir la Solution de logiciels-services)	(Inscrire le prix unitaire plafonné en \$CAN)	(entrez l'unité de mesure pour le logiciel-service, telle que «par utilisateur», «par entité», etc. et abonne ment, durée)	(entrez le pourcentage de réduction qui sera appliqué aux prix unitaires plafonds pour la durée de l'arrangement)	(Inscrire la langue de la Solution de logiciels-services, p. ex, français, anglais)	(Inscrire une adresse de site Web affichant cette information)	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
1										
2										
3										

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

Seules les modalités présentées dans la soumission font partie de l'arrangement en matière d'approvisionnement (AMA). Les fournisseurs peuvent soumettre leurs ententes de niveau de service (ENS) sous forme d'adresses URL. Les fournisseurs peuvent mettre à jour leurs ENS sur une base continue, à condition que les changements ne correspondent pas à une diminution du niveau de service fourni. Lorsqu'un fournisseur désire ajouter un nouveau produit ou service de SaaS à l'AMA, les ENS doivent être soumises à nouveau au responsable de l'AMA aux fins d'approbation avant d'être intégrées à l'AMA. Les modalités intégrées par renvoi avec une adresse URL ou un fichier « Lisez-moi », ou par un autre moyen, ne font pas partie de l'AMA à moins d'être inscrites intégralement dans l'annexe D relatif aux ENS.

Aucune modalité n'est censée abréger ou proroger les délais pour introduire une action pour violation, une action en responsabilité délictuelle, ou d'autres actions de tout type.

Annexe E – Modèle de demande de soumission pour logiciels-services

TABLE DES MATIÈRES

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX	16
1.1 INTRODUCTION	16
1.2 SOMMAIRE	16
1.3 COMPTE RENDU.....	17
1.4 AUTORITÉ CONTRACTANTE	17
PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES	18
2.1 INSTRUCTIONS, CLAUSES ET CONDITIONS UNIFORMISÉES	18
2.2 PRÉSENTATION DES SOUMISSIONS.....	20
2.3 DEMANDES DE RENSEIGNEMENTS – EN PÉRIODE DE SOUMISSION	20
2.4 LOIS APPLICABLES	21
2.5 AMÉLIORATIONS APPORTÉES AU BESOIN PENDANT LA DEMANDE DE SOUMISSIONS.....	21
PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS	22
3.1 INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS.....	22
PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION	24
4.1 PROCÉDURES D'ÉVALUATION.....	24
4.2 MÉTHODE DE SÉLECTION	24
PARTIE 5 – ATTESTATIONS ET RENSEIGNEMENTS SUPPLÉMENTAIRES	26
5.1 ATTESTATIONS EXIGÉES AVEC LA SOUMISSION	26
5.2 ATTESTATIONS PRÉALABLES À L'ATTRIBUTION DU CONTRAT	26
ANNEXE « X » - ÉNONCÉ DES TRAVAUX OU BESOIN	27
ANNEXE « X » - BASE DE PAIEMENT	27
ANNEXE « X » - LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ	27
ANNEXE « X » - INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE	27
ANNEXE « X » - PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – ATTESTATION	28

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 assujéti à tous les accords commerciaux énoncés dans la clause, sinon modifier cet article en conséquence.

1.2.2 Ce besoin est assujéti 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 assujéti 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.

1.2.12 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

Intégrer les modifications ci-dessous lorsque le service Connexion postal est offert pour la transmission électronique des soumissions par les soumissionnaires et que les instructions uniformisées 2003 sont incorporées par renvoi dans la demande de soumissions et en font partie intégrante.

Les instructions uniformisées 2003 sont modifiées comme suit :

- l'article 08, Transmission par télécopieur ou par le service Connexion postal, est modifié comme suit :
le sous-article 2. est entièrement supprimé et remplacé par ce qui suit :

2. Connexion postal

- a. Sauf indication contraire dans la demande de soumissions, les soumissions peuvent être transmises à l'aide du service Connexion postal offert par la Société canadienne des postes.
 - (i) SPAC, région de la capitale nationale : La seule adresse de courriel acceptable avec Connexion postal 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 postal 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 postal, 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 postal 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 postal. Les demandes d'ouverture de conversation Connexion postal reçues après cette date pourraient rester sans réponse.
- c. Si le soumissionnaire envoie un courriel demandant le service Connexion postal 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 postal. La conversation du service Connexion postal 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 postal 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 postal. 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 postal.
- g. Dans le cas des transmissions par le service Connexion postal, 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 postal;
 - (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 postal.
- h. L'Unité de réception des soumissions enverra un accusé de réception des documents de la soumission au moyen de la conversation Connexion postal, 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 postal 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 postal.
- j. Une soumission transmise par le service Connexion postal 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 postal 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 postal, tel qu'indiqué dans les instructions uniformisées 2003 ou pour envoyer des soumissions au moyen d'un message Connexion postal si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postal. »

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 postal)

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 postal, tel qu'indiqué dans les instructions uniformisées 2003, ou pour envoyer des soumissions au moyen d'un message Connexion postal si le soumissionnaire utilise sa propre licence d'utilisateur du service Connexion postal.

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 postal 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 postal et celui de la copie papier, le libellé de la copie électronique transmise par le service Connexion postal 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 fautive, 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

Insérer les paragraphes suivants pour les besoins formulés au nom d'un ministère ou d'un organisme assujéti au Programme de contrats fédéraux : (consulter l'Annexe 5.1 du Guide des approvisionnements). (Voir aussi la Partie 7 – Clauses du contrat subséquent).

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 assujéti 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 assujéti 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 X – PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – ATTESTATION

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 défaut, si une attestation est jugée fautive, 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. Le défaut de se conformer à toute demande ou exigence imposée par le Canada peut également rendre la soumission non recevable ou constituera un défaut en vertu du contrat.

Pour de plus amples 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](#).

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

Remplir les sections A et B.

A. Cochez seulement l'un des énoncés suivants :

- 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;
 - A5.1. Le soumissionnaire atteste qu'il a conclu un Accord pour la mise en oeuvre de l'équité en matière d'emploi valide et en vigueur avec le Programme du travail de EDSC.

OU

- A5.2. Le soumissionnaire atteste qu'il a soumis l'Accord pour la mise en oeuvre de l'équité en matière d'emploi (LAB1168) au Programme du travail de EDSC. Comme il s'agit d'une condition préalable à l'attribution du contrat, remplissez le formulaire intitulé Accord pour la mise en oeuvre de l'équité en matière d'emploi (LAB1168), signez-le en bonne et due forme et transmettez-le aux responsables du Programme du travail de EDSC.

B. Cochez seulement l'un des énoncés suivants :

- 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 intitulée Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation. (Consultez la section sur les coentreprises des instructions uniformisées)

Annexe F – Clauses du contrat subséquent
(voir en attachement)

Annexe G – Processus d'intégrité de la chaîne d'approvisionnement

1. Exigences relatives à la présentation des soumissions (obligatoires à la date de clôture de la demande de soumissions)

Les soumissionnaires doivent joindre à leur soumission, au plus tard à la date de clôture de la demande de soumissions, l'ISCA suivante :

1.2.1 Liste des produits informatiques: Les fournisseurs doivent identifier les solutions SaaS sur lesquelles les données du Canada seraient transmises et / ou stockées, qui seront utilisées et / ou installées pour exécuter toute partie des travaux et / ou des services décrits dans le contrat subséquent, en ce qui concerne chaque solution SaaS, en complétant le modèle de soumission du formulaire 6-SCI fourni dans la DAMA, qui comprend les informations suivantes:

a) **Nom OEM:** Entrez le nom du fabricant de l'équipement d'origine (OEM) du produit commandé.

b) **Numéro OEM DUNS:** Entrez le numéro DUNS du fabricant OEM. Le système de numérotation universelle des données (DUNS) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer le pointage de crédit d'une entreprise. Si la société ne possède pas de numéro DUNS ou si vous ne parvenez pas à vous en procurer un, veuillez compléter les informations demandées sous «C - Informations sur la propriété». Les informations sur la propriété comprennent les 5 premiers, en pourcentage, les investisseurs et les propriétaires de l'entreprise. Les noms fournis aux investisseurs et aux propriétaires doivent être ceux qui figurent dans les documents d'investissement ou de propriété de la société en question.

c) **Nom du produit:** entrez le nom du fabricant OEM pour le produit.

d) **Numéro de modèle:** Entrez le modèle OEM et / ou le numéro de version du produit.

e) **URL du produit:** entrez l'URL de la page Web du fabricant pour le produit.

f) **Informations sur la vulnérabilité:** Saisissez les informations concernant les 5 derniers problèmes de sécurité signalés concernant le produit. Si le fabricant OEM publie ces informations sur le site Web CVE, indiquez les numéros CVE séparés par des points-virgules (;). Si le fabricant OEM ne publie pas ces informations sur le site Web de CVE, vous devrez lui demander directement des informations sur les failles de sécurité et les fournir au Centre canadien de la cybersécurité. Si tel est le cas pour un produit particulier, entrez "voir les informations jointes" dans le champ Informations sur la vulnérabilité et incluez le ou les noms de fichier dans la colonne d'informations supplémentaires fournissant les informations de vulnérabilité requises

1.2.2 Informations sur la propriété: les fournisseurs doivent identifier le fabricant d'origine du (des) produit (s) ou service (s) commandé (s), ainsi que le nom de tout fournisseur (c.-à-d. Sous-traitants (particuliers ou entreprises), entrepreneurs de sous-traitants (particuliers ou entreprises) tout au long de la chaîne, revendeurs, distributeurs, sous-traitants, etc.) du ou des produits ou services commandés.

Cette liste doit identifier tous les tiers pouvant exécuter toute partie des travaux, qu'il s'agisse de sous-traitants pour le fournisseur ou de sous-traitants pour sous-traitants du fournisseur tout au long de la chaîne. Tout sous-traitant pouvant accéder aux données du Canada doit être identifié. Aux fins de cette exigence, un tiers qui est simplement un fournisseur de biens pour le fournisseur, mais qui n'exécute aucune partie des travaux, n'est pas considéré comme un sous-traitant. Les sous-traitants incluent, par exemple, des techniciens qui pourraient être déployés ou assurer la maintenance de la solution du fournisseur. Si le fournisseur ne prévoit pas faire appel à des sous-traitants pour exécuter une partie quelconque des travaux, il est demandé au fournisseur de l'indiquer dans sa réponse.

Les fournisseurs sont priés de fournir leurs informations sur le formulaire [insérer]. Il est demandé aux fournisseurs d'indiquer leur nom légal sur chaque page, d'insérer un numéro de page ainsi que le nombre total de pages. Les fournisseurs sont également invités à insérer une ligne distincte pour chaque sous-traitant et des lignes supplémentaires, le cas échéant.

Pour chacune des entités répertoriées, indiquez:

a) **Numéro OEM DUNS:** Entrez le numéro DUNS du fabricant OEM. Le système de numérotation universelle des données (DUNS) est un numéro unique à neuf chiffres attribué à chaque emplacement physique d'une entreprise. Il s'agit d'une norme mondiale utilisée pour déterminer le pointage de crédit

d'une entreprise. Si la société ne possède pas de numéro DUNS ou si vous ne parvenez pas à vous en procurer un, renseignez les informations demandées sous «C - Informations sur la propriété». Les informations sur la propriété comprennent les 5 premiers, en pourcentage, les investisseurs et les propriétaires de l'entreprise. Les noms fournis aux investisseurs et aux propriétaires doivent être ceux qui figurent dans les documents d'investissement ou de propriété de la société en question.

b) **Pays / Nationalité:** le pays dans lequel une personne répertoriée a sa nationalité principale ou le pays dans lequel une personne morale est enregistrée.

c) **Lien vers le site Web d'entreprise:** pour chaque nom OEM ou nom de fournisseur, propriété, investisseurs et dirigeants énumérés ci-dessus, indiquez un URI / URL aux informations prenant en charge les revendications répertoriées dans chacun des champs.

- a. **Diagrammes de réseau :** Un ou plusieurs diagrammes de réseau conceptuels montrant la totalité du réseau proposé pour la réalisation des travaux décrits dans la présente demande de soumissions. Les diagrammes de réseau doivent uniquement comprendre les portions du réseau du soumissionnaire (et de ceux de ses sous-traitants) sur lesquelles les données du Canada seraient transmises dans le cadre de l'exécution de tout contrat subséquent. À tout le moins, le diagramme doit illustrer ce qui suit :
- i. les principaux nœuds suivants servant à la prestation de services dans le cadre de tout contrat subséquent :
 1. les points de service;
 2. le réseau de base;
 3. le ou les réseaux de sous-traitants (préciser le nom du sous-traitant qui figure sur la liste des sous-traitants);
 - ii. les interconnexions entre les nœuds, s'il y a lieu;
 - iii. toute interconnexion entre les nœuds et Internet;
 - iv. pour chaque nœud, un renvoi au produit qui sera déployé dans ce nœud, à l'aide du numéro d'article de la liste des produits de TI.
- b. **Liste des sous-traitants :** Le soumissionnaire doit remettre une liste de tous les sous-traitants qui pourraient participer à l'exécution d'une partie des travaux (cela comprend les sous-traitants qui lui sont affiliés ou liés) dans le cadre de tout marché attribué. Au minimum, la liste doit inclure ce qui suit :
- i. le nom du sous-traitant;
 - ii. l'adresse du siège social du sous-traitant;
 - iii. la partie des travaux que réaliserait le sous-traitant;
 - iv. le ou les lieux où le sous-traitant réaliserait les travaux.

2. Évaluation de l'information sur la sécurité de la chaîne d'approvisionnement :

2.1 Le Canada déterminera si, à son avis, les informations sur la sécurité de la chaîne logistique créent la possibilité que la solution du fournisseur puisse compromettre ou être utilisée pour compromettre la sécurité des équipements, micrologiciels, logiciels, systèmes ou informations du Canada.

2.2 Dans le cadre de son évaluation:

(a) Le Canada peut demander au fournisseur toute information supplémentaire dont il a besoin pour effectuer une évaluation de sécurité complète des informations de sécurité de la chaîne logistique. Le fournisseur disposera de 2 jours ouvrables (ou d'une période plus longue, si l'autorité de sécurité de la chaîne d'approvisionnement le spécifie par écrit) pour fournir les informations nécessaires au Canada. Si ce délai n'est pas respecté, la réponse sera disqualifiée.

(b) Le Canada peut utiliser les ressources du gouvernement ou les consultants pour effectuer l'évaluation et peut contacter des tiers pour obtenir des informations complémentaires. Le Canada peut utiliser n'importe quel renseignement, qu'il soit inclus dans la réponse ou provenant d'une autre source, qu'il juge souhaitable de mener une évaluation complète des renseignements sur la sécurité de la chaîne logistique.

2.3 Si, de l'avis du Canada, un aspect quelconque de l'information sur la sécurité de la chaîne logistique, s'il est utilisé dans une solution, risque de compromettre ou d'être utilisé comme compromettant la sécurité des équipements, micrologiciels, logiciels, systèmes ou informations du Canada:

(a) Le Canada informera le fournisseur par écrit (par courrier électronique) et identifiera le ou les aspects de l'information sur la sécurité de la chaîne d'approvisionnement qui sont sujets à préoccupation ou qui ne peuvent pas être évalués (par exemple, les futures versions proposées des produits ne peuvent pas être traitées). évalué). Toute information

supplémentaire que le Canada pourrait être en mesure de fournir au fournisseur au sujet de ses préoccupations sera déterminée en fonction de la nature des préoccupations. Dans certaines situations, pour des raisons de sécurité nationale, le Canada pourrait ne pas être en mesure de fournir des informations supplémentaires au fournisseur; Par conséquent, dans certaines circonstances, le fournisseur ne connaîtra pas les raisons sous-jacentes des préoccupations du Canada en ce qui concerne un produit, un sous-traitant ou un autre aspect de ses informations sur la sécurité de la chaîne d'approvisionnement.

(b) L'avis donnera au fournisseur une occasion de soumettre des informations révisées sur la sécurité de la chaîne logistique dans les 10 jours civils suivant le jour où la notification écrite du Canada est envoyée au fournisseur (ou sur une période plus longue spécifiée par écrit par la chaîne logistique. Autorité de sécurité).

(c) Si le fournisseur soumet les informations révisées sur la sécurité de la chaîne d'approvisionnement dans le délai imparti, le Canada procédera à une deuxième évaluation. Si le Canada détermine que certains aspects des informations de sécurité de la chaîne d'approvisionnement révisées du fournisseur pourraient compromettre ou servir à compromettre la sécurité de l'équipement, des micrologiciels, des logiciels, des systèmes ou des informations du Canada, aucune autre possibilité de révision des informations de sécurité de la chaîne d'approvisionnement ne sera fournie. la réponse sera disqualifiée.

2.4 En participant à ce processus, le fournisseur reconnaît que la nature de la technologie de l'information est telle que de nouvelles vulnérabilités, y compris des failles de sécurité, sont constamment identifiées. En outre, le fournisseur reconnaît que l'évaluation de la sécurité effectuée par le Canada n'entraîne pas l'évaluation de la solution proposée. Par conséquent:

(a) une qualification en vertu de la présente DAMA ne constitue pas une approbation du fait que les produits ou autres informations inclus dans les informations de sécurité de la chaîne logistique satisfont aux exigences de la demande de soumissions ultérieure ou de tout contrat subséquent ou autre instrument pouvant être attribué en tant que résultat de toute demande de soumissions ultérieure;

(b) la qualification en vertu de la présente DAMA ne signifie pas que des informations identiques ou similaires sur la sécurité de la chaîne d'approvisionnement seront évaluées de la même manière pour les besoins futurs;

(c) à tout moment au cours du processus de demande de soumissions subséquent, le Canada peut informer un fournisseur que certains aspects de ses informations sur la sécurité de la chaîne d'approvisionnement font désormais l'objet de préoccupations en matière de sécurité. À ce stade, le Canada en informera le défendeur et donnera au fournisseur l'occasion de réviser ses informations sur la sécurité de la chaîne d'approvisionnement, en utilisant le même processus que celui décrit ci-dessus.

d) au cours de l'exécution d'un contrat ultérieur, si le Canada a des préoccupations concernant certains produits, conceptions ou sous-traitants initialement inclus dans les informations sur la sécurité de la chaîne logistique, les conditions de ce contrat régiront le processus de traitement de ces préoccupations.

2.5 Tous les fournisseurs seront informés par écrit s'ils sont ou non qualifiés en vertu de la présente DAMA pour passer à la prochaine étape du processus d'approvisionnement.

2.6 Tout fournisseur qualifié en vertu de la présente DAMA sera tenu de proposer une solution cohérente avec la version finale de l'information sur la sécurité de la chaîne d'approvisionnement qu'il a soumise avec sa réponse à la présente DAMA (révision seulement conformément au paragraphe ci-dessous). Sauf en vertu du paragraphe ci-dessous, aucun produit alternatif ou supplémentaire ni aucun sous-traitant ne peuvent être proposés dans la solution du fournisseur. Ceci est une exigence obligatoire de ce processus de sollicitation. La solution proposée lors de toute demande de soumissions ultérieure ne doit pas nécessairement contenir tous les produits dans les informations finales sur la sécurité de la chaîne d'approvisionnement.

2.7 Une fois qu'un fournisseur a été qualifié en réponse à la présente DAMA, aucune modification n'est autorisée dans les informations sur la sécurité de la chaîne logistique, sauf dans des circonstances exceptionnelles déterminées par le Canada. Étant donné qu'on ne peut pas prévoir toutes les circonstances exceptionnelles, on peut déterminer si des changements peuvent être apportés et le processus régissant ces changements sera déterminé par le Canada au cas par cas.

Annexe H – Chaîne d’approvisionnement et accord de non-divulagation

Entente de non-divulagation

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

- (a) 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.
- (b) 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.
- (c) 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.
- (d) 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.
- (e) Le soumissionnaire est conscient qu’un manquement à cette entente de non-divulagation 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-divulagation 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.
- (f) La présente entente de non-divulagation demeure en vigueur indéfiniment.

FORMULAIRES

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 <i>[voir la clause 2008 des instructions uniformisées]</i>	
Liste des membres du conseil d'administration <i>[Les fournisseurs sont priés d'indiquer les noms de l'ensemble des membres du conseil d'administration dans l'entreprise.]</i>	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 <i>(indiquer le niveau et la date d'attribution)</i>	
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 <i>(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].)</i>	
Entreprise canadienne <i>(Les fournisseurs doivent indiquer s'ils sont canadiens.)</i>	

<p>Entreprise écologique <i>[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.]</i></p>	
<p>Approvisionnement écologique <i>Les fournisseurs doivent s'engager à fournir des produits qui respectent l'environnement.)</i></p>	
<p>Attestation du fournisseur que les Solutions de logiciels-services sont disponibles dans le commerce <i>[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.]</i></p>	
<p>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 :</p> <ol style="list-style-type: none"> 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. 	
<p>Signature du représentant autorisé du fournisseur</p>	

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 _____

N° de téléphone du fondé de signature de l'éditeur de
Logiciels-services _____

N° 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 B – Obligations en matière de sécurité et protection de la vie privée

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) N° d'article, inclus pour chaque produit.

- c) **N° 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) la période durant laquelle le fournisseur offrira du soutien en regard des logiciels-services; PAGE # _____
- b) les coordonnées et renseignements concernant la procédure pour accéder aux services de soutien; PAGE # _____
- c) les procédures de résolution de problèmes; PAGE # _____
- d) les temps de réponse; PAGE # _____
- e) les procédures sur la façon et le moment de répondre à toutes les communications par téléphone, télécopieur ou courriel; PAGE # _____
- f) la disponibilité du site Web de soutien pour les utilisateurs du Canada (par exemple: jour et nuit, 365 jours par an, 99 % du temps); PAGE # _____
- g) Droits de maintenance (correctifs, mises à jour, versions majeure/mineure, etc.) PAGE # _____

Annexe G – Processus d'intégrité de la chaîne d'approvisionnement

.....

Nom du représentant autorisé du fournisseur :

Signature du représentant autorisé du fournisseur (date):

**Formulaire 6 – Formulaire de soumission de SCI
(voir l'attachement)**

Clauses du contrat subséquent relatives au logiciels-services

1. EXIGENCE	3
2 DURÉE, RÉILIATION ET RENOUVELLEMENT AUTOMATIQUE	4
3 SOLUTION	5
4 SERVICE	6
5 NIVEAUX DE SERVICE.....	7
6 DOCUMENTATION	8
7 TRAVAUX	8
8 AUTORISATION DE TÂCHES (AT) (CLAUSE FACULTATIVE À UTILISER LORSQUE DES SERVICES PROFESSIONNELS SONT REQUIS).....	11
9 BASE DE PAIEMENT	12
10 PAIEMENT	12
11 EXIGENCES EN MATIÈRE D'ASSURANCES.....	14
12 LIMITATION DE RESPONSABILITÉ	14
13 DISPOSITIONS GÉNÉRALES	15
APPENDICE A – LIVRABLES.....	19
APPENDICE B – DÉFINITIONS ET INTERPRÉTATIONS	20
APPENDICE C – OBLIGATIONS EN MATIÈRE DE SÉCURITÉ	26
PPENDICE D - OBLIGATIONS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE	30
APPENDICE E – EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:	32
APPENDICE F – EXIGENCE RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEURS ÉTRANGERS	33
APPENDICE G – PROCESSUS D'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT	39
APPENDICE H – FORMULAIRE D'AUTORISATION DE TÂCHES	48

Solution de logiciel-service

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 :

- i) la trousse de formation et de services Guide de démarrage rapide (« GDR »);
- ii) les services de mise en œuvre;
- iii) les services de formation;
- iv) les services d'épuration, de migration et de transition des données;
- v) 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 payé 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.

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 assujéti à un règlement juridique sur les autorisations de dépenses financières.
- d) **Avis de renouvellement automatique.** 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 à l'autorité technique avant l'expiration de la durée du contrat.
- e) **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.
- f) **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.

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.** 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 propriété intellectuelle par un tiers fondée sur l'utilisation de la solution par le Canada.
- 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.

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 que rien dans la solution, ou dans l'utilisation de la solution par le Canada, 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 Droit de résiliation. Si un tel événement empêche l'exécution du contrat pendant plus de 30 jours civils, l'autorité contractante peut alors choisir de résilier l'AT ou une partie ou la totalité du présent contrat sans qu'il y ait faute, ce qui signifie qu'aucune des parties ne sera responsable envers l'autre relativement au retard justifiable ou à la résiliation subséquente, et le Canada ne sera responsable que du paiement des services reçus à la date effective de la résiliation.

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 défauts 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.

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

Remarque au fournisseur. SPAC et SSC 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 PSPC et SSC 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 au 4 ci-dessous.

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 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.

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 (4^e suppl.).

13.7 Sanctions internationales.

1. 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](#).
2. Le fournisseur ne doit livrer au gouvernement du Canada aucun bien ni aucun service assujetti à des sanctions économiques.
3. 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 :

Le présent contrat de licence a été signé par les parties.

[NOM DE L'ENTREPRENEUR]

[AUTORITÉ CONTRACTANTE]

Par :

Par :

Nom :

Nom :

Titre :

Titre :

APPENDICE A – LIVRABLES

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 :

« 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.

« 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 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, micrologiciel, 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.

« 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;

« 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.

« 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 leur support, 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.

« Responsable du traitement » Personne physique ou morale, autorité publique, organisme ou autre organisation effectuant le traitement des données personnelles au nom du Canada, conformément aux directives de celui-ci.

« 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)

« 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).

« Service PaaS » Composantes d'une infrastructure de services axées sur le client et gérées par le Canada (en tant que client) (p. ex. données, applications, administration).

« Service SaaS » Composantes d'un service axées sur le client et gérées par le Canada (en tant que client) (p. ex. administration).

« Services » signifie :

1. 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;
2. fournir la documentation de la solution;
3. assurer la maintenance, la mise à niveau et la mise à jour de la ou des solutions;
4. gérer les incidents et les défauts pour s'assurer que la ou les solutions fonctionnent aux niveaux de service applicables;

« 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 :

- services gérés;
- services de formation;
- services infonuagiques privés ou offerts sur place;
- services professionnels ou services de consultation dépassant la portée des services de soutien publics habituellement offerts sur le marché.

« 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.

« 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.

« 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.

« 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 final » Toute personne, ou tout processus système agissant au nom d'une personne, que le Canada autorise à accéder aux services.

« 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.

« 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.

« 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;

« 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 1^{er} avril 2013;

« travaux » désigne tous les services professionnels que l'entrepreneur doit effectuer, livrer ou exécuter.

« 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;

APPENDICE C – OBLIGATIONS EN MATIÈRE DE SÉCURITÉ

Transfert des obligations en matière de sûretés

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

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).

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 tous les fichiers en ligne, pseudo-direct et hors ligne;
- (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 déclassification des supports d'information électroniques (CSTC ITSG-06).

a)

- 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 (Palier 1 ET 2)**

- 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)
- (iii) faire de son mieux pour prévenir les attaques au moyen de mesures de sécurité comme les protections contre le refus de service;
- (iv)
- (v) faire de son mieux pour détecter les attaques, les incidents de sécurité et autres événements anormaux;
- (vi)
- (vii) détecter l'utilisation et l'accès non autorisés à tous les services, données et composants pertinents aux services IaaS, PaaS ou SaaS du Canada;
- (viii)
- (ix) 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;
- (x)
- (xi) répondre aux menaces et aux attaques contre les services du fournisseur, les contenir et veiller à la récupération;
- (xii)
- (xiii) 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 (Palier 1 ET 2)**

- 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;
- b) 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 (PALIERS 1 ET 2)**

- 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 déféctuosité 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 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>). 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-feux, 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.

Le fournisseur doit de plus :

1. 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;
2. 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 (PALIERS 1 ET 2)

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 (PALIERS 1 ET 2)

- a) Le fournisseur doit fournir une liste de sous-traitants auxquels il pourrait faire appel pour exécuter n'importe quelle partie des travaux en fournissant le service au Canada. La liste doit comprendre les renseignements suivants : (i) le nom du sous-traitant; (ii) la description des travaux qui seraient exécutés par le sous-traitant; et (iii) les emplacements où le sous-traitant exécuterait les travaux.
- b) Le fournisseur doit fournir une liste des sous-traitants dans les dix jours suivant la date d'entrée en vigueur du contrat. Le fournisseur 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. Le fournisseur doit aider le Canada à mener les vérifications visant les sous-traitants dans les dix jours ouvrables.

11. Gestion des risques de la chaîne d'approvisionnement

Dans les 30 jours suivant l'attribution du contrat, l'entrepreneur doit fournir un plan de gestion des risques de la chaîne d'approvisionnement (PGRCA) mis à jour, évalué et validé de manière indépendante par un tiers indépendant certifié selon le régime de certification de l'AICPA ou de CPA Canada ou de l'ISO. Le plan PGRCA doit être fourni au Canada sur une base annuelle, ou sur demande, ou immédiatement après tout changement important du plan PGRCA.

PPENDICE D - OBLIGATIONS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

1. Audit de conformité

- a) Dans le cas où le Canada doit effectuer des audits de sécurité, des inspections et / ou examiner toute information appendiceaire (par exemple, documentation, description de protection des données, architecture de données et descriptions de sécurité) conformément à la section 12.1, les deux parties conviennent de négocier une solution en bonne foi et de considérer à la fois la raison d'être de la demande du Canada et les processus et protocoles de l'entrepreneur.
- b) Dans les 30 jours suivant la demande de l'autorité contractante, l'entrepreneur doit faire appel à un tiers pour effectuer un audit de la protection de la vie privée ou fournir la preuve qu'il ne génère pas, ne collecte, n'utilise pas, ne stocke ou ne divulgue pas d'informations personnelles additionnelles, telles que définies par Le Canada, autre que les données du client telles que définies par l'entrepreneur, ne possède pas spécifiquement de données à caractère personnel dans les données de support (collectées dans des journaux (par exemple, des données de télémétrie telles que les en-têtes et le contenu d'un message électronique).

2. 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 / réplique hors site) dans un document Word ou Excel.

3. 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>). / dcpia) 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.

4. 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:
- 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
- d) 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.

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) Appendice E - EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN

(b) Appendice F - EXIGENCE RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEURS ÉTRANGERS

APPENDICE E – EXIGENCE EN MATIÈRE DE SÉCURITÉ POUR ENTREPRENEUR CANADIEN:

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, ainsi qu'une cote de protection des documents approuvée au niveau PROTÉGÉ B, délivrées par la Secteur de la Sécurité Industrielle (SSI) de **Services publics et approvisionnement Canada (SPAC)**.
2. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens PROTÉGÉS, ou à des établissements de travail dont l'accès est réglementé, doivent TOUS détenir une cote de sécurité du personnel valable au niveau SECRET, ou FIABILITE, comme requis par le guide de sécurité, délivrée ou approuvée par la SSI de SPAC.
3. L'entrepreneur NE DOIT PAS utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données et(ou) de production au niveau PROTÉGÉ jusqu'à ce que l'autorisation écrite a été émise par l'autorité en matière de sécurité pour le ministère ou agence du client. Lorsque cette autorisation aura été délivrée, ces tâches pourront être exécutées au niveau PROTÉGÉ A et B compris un lien électronique au niveau PROTÉGÉ A et B.
4. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de la SSI de SPAC.
5. L'entrepreneur ou l'offrant doit se conformer aux dispositions des documents suivants :
 - a) de la Liste de vérification des exigences relatives à la sécurité et directive de sécurité (s'il y a lieu), reproduite ci-joint à l'Annexe _____;
 - b) le *Manuel de la sécurité industrielle* (dernière édition);
 - c) Site Web du SSI : Exigences de sécurité des contrats du gouvernement du Canada, veuillez visitez <https://www.tpsgc-pwgsc.gc.ca/esc-src>

VEUILLEZ NOTER : Il y a des niveaux multiples de contrôle de sécurité du personnel associé avec ce dossier. Dans ce cas, un guide de sécurité doit être ajouté à la LVERS afin de clarifier ces contrôles de sécurité. Le guide de sécurité est habituellement généré par l'autorité de projet et/ou l'autorité de sécurité de l'organisation

APPENDICE F – EXIGENCE RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEURS ÉTRANGERS

L'Autorité désignée en matière de sécurité pour le Canada (ADS canadien) pour les questions industrielles au Canada est la Direction de la sécurité industrielle internationale (DSII), Secteur de la sécurité industrielle (SSI), Services publics et approvisionnement Canada (SPAC). L'ADS canadien est chargée d'évaluer la conformité des soumissionnaires aux exigences en matière de sécurité pour l'**entrepreneur/sous-traitant** étrangers. Les exigences en matière de sécurité suivantes s'appliquent à l'**entrepreneur/sous-traitant** étranger destinataire, incorporés ou autorisés à faire des affaires dans un état autre que le Canada et qui assurent la prestation de services décrites dans l'énoncé des travaux ultérieur et s'ajoute aux exigences de confidentialité et de sécurité de l'appendice B et l'appendice C.

1. **L'entrepreneur/Le sous-traitant** étranger destinataire doit être dans un pays de l'Union européenne, dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité et un protocole d'entente bilatérale ou multinationale. Le programme de sécurité a des ententes en matière de sécurité et protocole d'entente bilatérale ou multinationale avec les pays mentionnés au site de SPAC suivant: <http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html>.
2. **L'entrepreneur/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution du **contrat/sous-traitance**, tenir une équivalence à une vérification d'organisation désignée (VOD), délivrée par l'ADS canadien comme suit :
 - i. **L'entrepreneur/Le sous-traitant** étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence.
 - ii. **L'entrepreneur/Le sous-traitant** étranger destinataire ne doit pas entreprendre les travaux, fournir les services ou assurer toute autre prestation tant que l'Administration désignée en matière de sécurité au Canada (ADS canadien) n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le **contrat/sous-traitance**. L'ADS canadien donne cette confirmation par écrit à l'**entrepreneur/au sous-traitant** étranger destinataire. Un Formulaire d'attestation remis par l'ADS canadien à l'**entrepreneur/au sous-traitant** étranger destinataire permettra de confirmer la conformité et l'autorisation de fournir les services prévus.
 - iii. **L'entrepreneur/Le sous-traitant** étranger destinataire proposé doit identifier l'agent de sécurité du contrat (ASC) autorisé et un agent remplaçant de sécurité d'entreprise (ARSE) (le cas échéant) qui sera responsable du contrôle des exigences de sécurité, telles qu'elles sont définies dans le **contrat/sous-traitance**. Cette personne sera désignée par le président-directeur général ou par un cadre supérieur clé de l'entreprise étrangère destinataire proposée. Les cadres supérieurs clés comprennent les propriétaires, les agents, les directeurs, les cadres et les partenaires occupant un poste qui leur permettrait d'avoir une influence sur les politiques ou les pratiques de l'organisation durant l'exécution du **contrat/sous-traitance**.
 - iv. **L'entrepreneur/Le sous-traitant** étranger destinataire n'autorisera pas l'accès à des renseignements/biens de niveau **PROTÉGÉ du Canada**, sauf à son personnel ayant été évalué conformément à la définition et aux pratiques énoncées dans la Norme relative au filtrage de sécurité du Conseil du Trésor (<https://www.tbssct.gc.ca/pol/doc-fra.aspx?id=28115>) ou à l'utilisation de mesures équivalentes acceptables établies par l'entrepreneur dans leur documentation accessible au public, et comme convenu par le ASC canadien, notamment:, sous réserve des conditions suivantes:
 - a. Le personnel à un besoin de savoir pour l'exécution du **contrat/sous-traitance**;

- b. Le personnel a fait l'objet d'une vérification du casier judiciaire valide, avec des résultats favorables, d'une agence gouvernementale reconnue ou d'une organisation du secteur privé dans **leur pays**, ainsi qu'une vérification d'antécédents, validé par l'ADS canadien.
 - c. **L'entrepreneur/Le sous-traitant** étranger destinataire doit s'assurer que le personnel consente à la divulgation du casier judiciaire et antécédents à l'ADS canadien et d'autres fonctionnaires du gouvernement canadien, si demandé; et
 - d. Le Gouvernement du Canada se réserve le droit de refuser l'accès aux renseignements/ biens de niveau **CANADA PROTÉGÉ à l'entrepreneur/au sous-traitant** étranger destinataire pour cause.
3. Le gouvernement du Canada se réserve le droit de refuser l'accès à des informations/actifs au niveau **CANADA PROTÉGÉ** ou produit par un **entrepreneur/sous-traitant étranger** destinataire pour un motif valable.
 4. Les renseignements/biens de niveau **CANADA PROTÉGÉ** fournis ou produits dans le cadre **du contrat/sous-traitance** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:
 - a. L'ADS canadien atteste par écrit que le sous-traitant étranger destinataire a obtenu l'accès aux renseignements/biens de niveau **CANADA PROTÉGÉ** par l'intermédiaire de l'ADS canadien;
 - b. L'ADS canadien donne son autorisation écrite lorsque l'autre sous-traitant étranger destinataire est situé dans un autre pays.
 5. **L'entrepreneur/Le sous-traitant** étranger destinataire **NE DOIT PAS** emporter de renseignements/ biens de niveau **CANADA PROTÉGÉ** hors des établissements de travail visés, et **l'entrepreneur/ sous-traitant** étranger destinataire doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.
 6. **L'entrepreneur/Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements/biens de niveau **CANADA PROTÉGÉ** pour répondre à des besoins distincts de l'exécution du **contrat/sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'ADS canadien.
 7. **L'entrepreneur/Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution du **contrat/sous-traitance** tenir une équivalence à une autorisation de détenir des renseignements (ADR) de **CANADA PROTÉGÉ A et B**.
 8. **Les contrats de sous-traitance comportant des exigences de sécurité NE DOIVENT PAS être attribués sans l'autorisation écrite préalable de la DSA canadienne.**
 9. **L'entrepreneur/Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité.
 10. **Propriété des renseignements personnels et des dossiers**
 Pour exécuter les services et / ou les travaux, **l'entrepreneur / sous-traitant** destinataire étranger et / ou collectera des informations personnelles de tiers. L'entrepreneur / sous-traitant destinataire étranger reconnaît qu'il n'a aucun droit sur les renseignements personnels ou les dossiers et que le Canada est propriétaire des dossiers. Sur demande, l'entrepreneur ou le sous-traitant destinataire étranger doit mettre immédiatement à la disposition du Canada tous les renseignements personnels et tous les dossiers dans un format acceptable par le Canada.

11. Utilisation des informations personnelles

L'entrepreneur / sous-traitant étranger destinataire accepte de créer, collecter, recevoir, gérer, accéder, utiliser, conserver et éliminer les informations personnelles et les enregistrements uniquement pour exécuter les services et / ou les travaux conformément au contrat / sous-contrat.

12. Cueillette des renseignements personnels

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

1. les renseignements personnels sont recueillis au nom du Canada et lui seront transmis;
2. les usages qui seront faits des renseignements personnels recueillis;
3. que 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;
4. les conséquences, s'il en est, du refus de fournir les renseignements;
5. que l'intéressé au droit d'accéder à ses renseignements personnels et d'y apporter des corrections;
6. les renseignements personnels feront partie d'un fichier de renseignements personnels particulier (au sens de la Loi sur la protection des renseignements personnels), et fournir à l'individu de l'information concernant l'institution fédérale qui gère le fichier de renseignements personnels, si l'autorité contractante a fourni ces renseignements à l'entrepreneur/au sous-traitant étranger destinataire.

(1) L'entrepreneur, ses sous-traitants 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 en vertu d'un contrat passé avec le Canada.

(2) Si l'autorité contractante l'exige, l'entrepreneur /le sous-traitant étranger destinataire 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/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.

(3) Si, lors de la cueillette de renseignements personnels auprès d'un individu, l'entrepreneur/le sous-traitant étranger destinataire sait ou soupçonne que cet individu n'est pas en mesure de consentir à la divulgation et à l'utilisation de ses renseignements personnels, l'entrepreneur/le sous-traitant étranger destinataire doit demander des directives à l'autorité contractante.

13. Exactitude, confidentialité et intégrité des renseignements personnels

L'entrepreneur/Le sous-traitant étranger destinataire doit veiller à ce que les renseignements personnels soient les plus exacts, complets et à jour que possible. Pour ce faire, l'entrepreneur/le sous-traitant étranger destinataire doit, au minimum:

- a) ne pas utiliser de données d'identification personnelle (par ex., le numéro d'assurance sociale, le numéro de passeport, le numéro d'identificateur client unique) pour lier de nombreuses bases de données qui comprennent des renseignements personnels;
- b) isoler les dossiers des renseignements et des dossiers de **l'entrepreneur/du sous-traitant** étranger destinataire;
- c) ne donner l'accès aux renseignements personnels et aux dossiers qu'à ceux qui le requièrent aux fins d'exécution 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/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 d'exécution des travaux. **L'entrepreneur/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) tenir un registre de toutes les demandes faites par un individu 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 un individu ou par le Canada au nom d'un individu);
- g) joindre une note à tout dossier qu'un individu a demandé de corriger, mais que **l'entrepreneur/le sous-traitant** étranger destinataire a décidé, pour quelque raison que ce soit, de ne pas corriger. Lorsque cela se produit, l'entrepreneur doit immédiatement informer l'autorité contractante de la correction demandée et des raisons de **l'entrepreneur/le sous-traitant** étranger destinataire de ne pas l'effectuer. Si l'autorité contractante demande que la correction soit effectuée, **l'entrepreneur/le sous-traitant** étranger destinataire a l'obligation du faire;
- h) tenir un registre de la date et de l'auteur de la dernière mise à jour de chaque dossier;
- i) maintenir un journal de vérification électronique qui enregistre tous les accès et les tentatives d'accès des dossiers électroniques. Le journal de vérification doit être dans un format qui peut être lu par **l'entrepreneur/le sous-traitant** étranger destinataire et le Canada en tout temps;
- j) sécuriser et contrôler l'accès à tout renseignement personnel.

14. Protection des renseignements personnels

L'entrepreneur/Le sous-traitant étranger destinataire doit protéger les renseignements personnels à tout moment en prenant toutes les mesures raisonnablement nécessaires pour les protéger et en protéger l'intégrité et la confidentialité. Pour ce faire, l'entrepreneur/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 autre mécanisme de contrôle) soit requis pour accéder au système ou à la base de données où sont stockés les renseignements personnels;
- b) s'assurer que les mots de passe ou autres moyens d'accès aux renseignements personnels ne sont fournis qu'aux individus qui le requièrent aux fins d'exécution des travaux;
- c) ne pas confier à un tiers (y compris un affilié) le stockage des renseignements personnels sans l'autorisation préalable et écrite de l'autorité contractante;
- d) protéger les bases de données ou les systèmes informatiques qui emmagasinent les renseignements personnels contre un accès externe de manière à protéger les renseignements très protégés et de nature délicate;
- 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 demandées par le Canada de temps à autre;
- g) aviser immédiatement l'autorité contractante de toute infraction (p. ex. un accès, un usage ou une divulgation non autorisé de renseignements) ou de tout incident pouvant mettre en danger la sécurité ou l'intégrité des dossiers, des systèmes ou des installations ou des renseignements personnels sont conservés. Si une infraction se produit, l'entrepreneur ou le sous-traitant devra immédiatement prendre toutes les mesures raisonnables nécessaires pour limiter l'étendue des impacts possibles ou pour résoudre le problème et empêcher celui-ci de se reproduire. Le Canada peut exiger de l'entrepreneur qu'il prenne des mesures précises pour régler le problème et éviter qu'il se reproduise, et pourrait invoquer les dispositions de la présente entente en lien avec la suspension ou la résiliation du contrat pour manquement.

15. Obligations réglementaires

L'entrepreneur/Le sous-traitant étranger destinataire 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.R.C.1985, ch. A-1, et de la [Loi sur la Bibliothèque et les Archives du Canada](#), L.C. 2004, ch.11. L'entrepreneur /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 toute autre loi qui entre en vigueur lorsqu'il y a lieu.

L'entrepreneur/Le sous-traitant étranger destinataire reconnaît que les obligations dont il doit s'acquitter en vertu du contrat 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/le sous-traitant étranger destinataire estime que l'une ou l'autre des obligations du contrat l'empêche de s'acquitter de ses obligations en vertu de ces lois, il doit immédiatement informer l'autorité contractante de la disposition du contrat et de l'obligation de la loi qu'il considère comme contradictoires.

16. 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/le sous-traitant étranger destinataire doit immédiatement informer l'autorité contractante afin de lui permettre de participer aux procédures pertinentes.

16. Plaintes ou demandes d'accès

Le Canada et l'entrepreneur/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, 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 et mutuellement de son dénouement.

17. Exception

Les obligations énoncées dans ces articles 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/le sous-traitant étranger destinataire ou de tout sous-traitant, agent ou représentant de l'entrepreneur ou des employés.

18. Vérification

Le Canada peut vérifier en tout temps la conformité de l'entrepreneur/le sous-traitant étranger destinataire aux articles relatifs à la protection des renseignements personnels. À la demande de l'autorité contractante, l'entrepreneur/le sous-traitant étranger destinataire doit donner au Canada (ou à son représentant autorisé) l'accès à ses locaux et aux renseignements personnels et dossiers en tout temps jugé raisonnable. Si le Canada découvre un problème durant la vérification, l'entrepreneur/le sous-traitant étranger destinataire doit le corriger immédiatement à ses frais.

APPENDICE G – PROCESSUS D'INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

1. Processus continu d'intégrité de la chaîne d'approvisionnement

1.1 Processus d'intégrité de la chaîne d'approvisionnement : Les parties reconnaissent que le processus d'intégrité de la chaîne d'approvisionnement est un élément clé du processus d'approvisionnement ayant mené à l'attribution du présent contrat. Dans le cadre de ce processus d'évaluation, le Canada a évalué l'ISCA de l'entrepreneur sans avoir ciblé de préoccupations en matière de sécurité. L'ISCA suivante a été soumise :

- a) une liste des produits de TI;
- b) la liste des sous-traitants;
- c) les diagrammes de réseau.

Cette ISCA est incluse et constitue l'Appendice E – Processus d'intégrité de la chaîne d'approvisionnement. Les parties reconnaissent également que la sécurité représente un facteur essentiel pour le Canada à l'égard du présent marché et qu'une évaluation continue de l'ISCA sera exigée tout au long de la période visée par le marché. Le présent article régit ce processus.

1.2 Évaluation de la nouvelle ISCA : Au cours de la période visée par le contrat, l'entrepreneur pourrait être appelé à modifier l'ISCA contenue dans l'Appendice G, Processus d'intégrité de la chaîne d'approvisionnement. À cet égard :

- a) L'entrepreneur doit revoir son ISCA au moins une fois par mois pour montrer les changements apportés ainsi que les suppressions et les ajouts qui concernent les services prévus au marché (y compris les produits déployés par ses sous-traitants) durant cette période. Il doit indiquer sur la liste où les changements ont été apportés lors de la période en question. Si aucune modification n'a été apportée au cours du mois, l'entrepreneur doit aviser l'autorité de sécurité de la chaîne d'approvisionnement par écrit que la liste existante est inchangée. Les modifications apportées à la liste des produits de TI doivent être accompagnées par le ou les schémas du réseau, s'il y a lieu.
- b) L'entrepreneur accepte de fournir des mises à jour périodiques (au moins une fois l'an) à l'autorité de sécurité de la chaîne d'approvisionnement pendant la période visée par le contrat au sujet des nouveaux produits qu'il compte déployer dans le cadre des travaux (p. ex. tandis qu'il élabore sa « feuille de route technologique » ou des plans similaires). Cela permettra au Canada d'évaluer ces produits à l'avance afin de cerner toute préoccupation liée à la sécurité avant le déploiement des produits dans le cadre de la prestation des services visés par le contrat. Le Canada s'efforcera d'évaluer de nouveaux produits proposés dans les 30 jours civils, même si les listes de produits plus longues peuvent prendre plus de temps.
- c) Le Canada se réserve le droit de réaliser une évaluation de la sécurité exhaustive et indépendante de tous les nouveaux éléments d'ISCA. À la demande de l'autorité de sécurité de la chaîne d'approvisionnement, l'entrepreneur doit lui fournir tout renseignement dont il a besoin pour réaliser son évaluation.

- d) Le Canada peut confier l'évaluation à ses propres ressources ou à des consultants et peut au besoin se procurer des renseignements additionnels auprès de tiers. Le Canada peut utiliser tout renseignement, qu'il ait été fourni par l'entrepreneur ou provienne d'une autre source, qu'il juge utile afin d'effectuer une évaluation exhaustive de toute nouvelle ISCA proposée.

1.3 Détermination des nouvelles vulnérabilités en matière de sécurité dans l'ISCA qui a déjà été évaluée par le Canada :

- a) L'entrepreneur doit fournir au Canada, en temps opportun, des renseignements sur toutes les vulnérabilités, y compris toute faiblesse ou lacune de conception, ciblées dans le cadre de l'exécution des travaux pour tout produit utilisé dans la prestation des services qui permettraient à une personne non autorisée de compromettre l'intégrité, la confidentialité, les contrôles d'accès, la disponibilité, la cohérence ou le mécanisme de vérification du système ou des données et des applications qu'il héberge.
- b) L'entrepreneur reconnaît que la nature des technologies de l'information est telle que de nouvelles vulnérabilités, y compris les vulnérabilités relatives à la sécurité, sont constamment relevées et, de ce fait, de nouvelles vulnérabilités relatives à la sécurité peuvent être relevées dans l'ISCA qui a déjà fait l'objet d'une évaluation de l'ISCA et pour laquelle aucune préoccupation en matière de sécurité n'a été relevée par le Canada, soit durant le processus d'approvisionnement, soit plus tard au cours de la période visée par le contrat.

1.4 Traitement des préoccupations relatives à la sécurité :

- a) Si le Canada informe l'entrepreneur de préoccupations relatives à la sécurité dans un produit qui n'a pas encore été déployé, l'entrepreneur convient de ne pas le déployer dans le cadre du contrat sans le consentement de l'autorité de sécurité de la chaîne d'approvisionnement.
- b) Le Canada peut, à tout moment pendant la période du contrat, informer l'entrepreneur qu'il estime qu'un produit utilisé dans la solution de ce dernier (y compris l'utilisation par un sous-traitant) pourrait compromettre ou servir à compromettre la sécurité de l'équipement, des micrologiciels, des logiciels, des systèmes ou de l'information du Canada; dans un tel cas, l'entrepreneur doit :
 - (iii) Fournir au Canada toute information demandée par l'autorité de sécurité de la chaîne d'approvisionnement afin que le Canada puisse effectuer une évaluation exhaustive.
 - (iv) À la demande de l'autorité de sécurité de la chaîne d'approvisionnement, proposer un plan d'atténuation (y compris un calendrier) dans les 10 jours ouvrables, comme la migration vers un autre produit. L'autorité de sécurité de la chaîne d'approvisionnement informera l'entrepreneur par écrit si le Canada approuve le plan d'atténuation, ou formulera des commentaires sur les préoccupations ou les lacunes relevées dans le plan d'atténuation.
 - (v) Mettra en oeuvre le plan d'atténuation approuvé par le Canada. Ce processus s'applique tant aux nouveaux produits qu'aux produits qui ont déjà été évalués dans le cadre de l'évaluation du processus d'intégrité de la chaîne d'approvisionnement menée par le Canada, mais qui présentent désormais des vulnérabilités en matière de sécurité.
- c) Nonobstant le paragraphe précédent, si le Canada détermine, à sa discrétion, que la préoccupation relevée en matière de sécurité pose une menace pour la sécurité nationale, à la fois grave et imminente, l'autorité de sécurité de la chaîne d'approvisionnement pourrait exiger

que l'entrepreneur cesse immédiatement le déploiement du ou des produits en question dans le cadre des travaux. En ce qui a trait aux produits déjà déployés, l'entrepreneur doit les cibler et les retirer (à la demande de l'autorité de sécurité de la chaîne d'approvisionnement) des travaux selon l'échéancier établi par le Canada. Cependant, avant de prendre une décision définitive à cet égard, le Canada permettra à l'entrepreneur de faire valoir son point de vue dans les 48 heures suivant la réception de l'avis de l'autorité de sécurité de la chaîne d'approvisionnement. Par exemple, l'entrepreneur peut proposer des mesures d'atténuation que le Canada pourra considérer. Le Canada prendra ensuite une décision définitive.

1.5 Conséquences financières :

- a) Toute conséquence financière subséquente à une demande du Canada pour que cesse le déploiement d'un ou de plusieurs produits donnés, ou pour que ceux-ci soient retirés, sera prise en considération et négociée de bonne foi par les parties au cas par cas, et pourra faire l'objet d'une modification au contrat. Cependant, malgré de telles négociations, l'entrepreneur doit cesser le déploiement du ou des produits, ou les retirer, à la demande du Canada. Les négociations se poursuivront séparément. Les parties conviennent qu'à tout le moins, les facteurs suivants seront pris en considération dans leurs négociations, le cas échéant :
 - (i) en ce qui a trait aux produits que le Canada a déjà évalués lors d'une évaluation de l'ICA sans détecter de préoccupation relative à la sécurité, une preuve fournie par l'entrepreneur démontrant depuis combien de temps il est propriétaire des produits;
 - (ii) en ce qui a trait aux nouveaux produits, le fait que l'entrepreneur ait été ou non capable d'aviser au préalable le Canada de l'utilisation des nouveaux produits dans le cadre des travaux;
 - (iii) la preuve démontrant combien l'entrepreneur a payé pour le produit, ainsi que tout montant que l'entrepreneur a prépayé ou s'est engagé à verser en ce qui a trait à la maintenance et à la prise en charge de ce produit;
 - (iv) la durée normale d'utilisation du produit;
 - (v) toute annonce de « fin de vie » ou autre formulée par le fabricant du produit, indiquant que le produit ne sera plus pris en charge;
 - (vi) la durée normale d'utilisation du produit de remplacement proposé;
 - (vii) le temps qu'il reste à la période du contrat;
 - (viii) si le produit existant ou un produit de remplacement est utilisé ou doit être utilisé exclusivement pour le Canada, ou si le produit est aussi utilisé pour fournir des services à d'autres clients de l'entrepreneur ou de ses sous-traitants;
 - (ix) si le produit remplacé peut être déployé de nouveau pour d'autres clients;
 - (x) toute formation nécessaire des employés de l'entrepreneur quant à l'installation, à la configuration et à la maintenance des produits de remplacement, pourvu que l'entrepreneur puisse prouver que ses employés n'auraient pas besoin de cette formation autrement;

- (xi) tous les frais de développement nécessaires pour que l'entrepreneur intègre les produits de remplacement au portail de service ainsi qu'aux systèmes d'exploitation, d'administration et de gestion, si les produits de remplacement ne sont pas des produits déployés à d'autres fins dans le cadre des travaux;
 - (xii) l'incidence du changement pour le Canada, y compris la quantité et le type de ressources nécessaires et le temps alloué à la migration.
- b) En outre, à la demande de l'autorité de sécurité de la chaîne d'approvisionnement, l'entrepreneur doit fournir une ventilation détaillée des coûts, une fois que les travaux liés aux préoccupations en matière de sécurité signalées conformément à cet article seront terminés. La ventilation des coûts doit comprendre une liste de tous les éléments de coût applicables concernant le travail demandé par l'autorité de sécurité de la chaîne d'approvisionnement. Elle doit être signée et certifiée par l'agent financier supérieur de l'entrepreneur, à moins que l'autorité de sécurité de la chaîne d'approvisionnement n'ait indiqué autre chose par écrit. Le Canada doit juger que pour chaque élément de coût, des données justificatives ont été fournies avec suffisamment de détails pour permettre une vérification exhaustive. En aucun cas le remboursement des dépenses de l'entrepreneur (ou de l'un de ses sous-traitants) ne dépassera frais remboursables démontrés directement liés à la demande présentée par le Canada pour que cesse le déploiement d'un ou de plusieurs produits donnés ou pour le retrait de ceux-ci.
- c) Nonobstant les autres dispositions du présent article, si l'entrepreneur ou l'un de ses sous-traitants déploie de nouveaux produits qui soulèvent des questions de sécurité de la part du Canada dans le cadre des travaux, le Canada peut exiger que l'entrepreneur ou l'un de ses sous-traitants cesse immédiatement le déploiement du produit, ou qu'il le retire. Dans de tels cas, tous les frais déboursés pour se conformer à la demande du Canada seront la responsabilité de l'entrepreneur ou de ses sous-traitants, tel qu'il a été négocié entre eux. Le Canada n'est pas responsable de ces coûts.

1.6 Généralités :

- a) Le processus décrit dans le présent article peut s'appliquer à un produit unique, à un ensemble de produits, ou à la totalité des produits fabriqués ou distribués par un fournisseur donné.
- b) Le processus décrit dans le présent article vise également les sous-traitants. En ce qui a trait aux répercussions sur les coûts, le Canada reconnaît que les facteurs de coûts liés aux préoccupations au sujet des sous-traitants (plutôt que des produits) pourraient être différents et comprendre de facteurs comme la disponibilité d'autres sous-traitants pour accomplir le travail.
- c) Aux termes du présent article, le non-respect de tout niveau de service en raison du remplacement par un autre produit ou un autre sous-traitant, à la demande du Canada, n'entraînera pas de crédit de service, ni ne sera pris en considération dans les calculs généraux des valeurs métriques, à condition que l'entrepreneur applique les changements nécessaires conformément au plan de migration approuvé par le Canada ou procède immédiatement à la mise en œuvre des exigences du Canada, si le Canada a déterminé que la menace à la sécurité nationale est sérieuse et imminente.

- d) Si l'entrepreneur est informé qu'un sous-traitant déploie un produit faisant l'objet de préoccupations en matière de sécurité dans le cadre des travaux, il doit immédiatement en aviser l'autorité contractante et le responsable technique, et doit voir à l'application des modalités de son marché avec le sous-traitant. L'entrepreneur reconnaît ses obligations en vertu des Conditions générales 2030, paragraphe 9(3).
- e) Toute décision prise par le Canada à cet égard concerne un produit ou un sous-traitant précis et son emploi proposé dans le cadre du présent contrat; une telle décision ne signifie aucunement que le même produit ou sous-traitant serait nécessairement évalué de la même façon, si son emploi était proposé à une autre fin ou dans un autre contexte.

2. Sous-traitance

2.1 Malgré les conditions générales, aucune partie des travaux ne peut être sous-traitée (même à une société affiliée de l'entrepreneur) sans le consentement écrit préalable de l'autorité de sécurité de la chaîne d'approvisionnement. Pour obtenir le consentement écrit de l'autorité de sécurité de la chaîne d'approvisionnement, l'entrepreneur doit fournir les renseignements suivants :

- a) le nom du sous-traitant;
- b) la partie des travaux à réaliser par le sous-traitant;
- c) le niveau de vérification d'organisation désignée ou d'attestation de sécurité d'installation du sous-traitant;
- d) la date de naissance, le nom complet et la cote de sécurité des employés du sous-traitant qui devront avoir accès aux installations du Canada;
- e) la sous-liste de vérification des exigences relatives à la sécurité remplie et signée par l'agent de sécurité d'entreprise de l'entrepreneur, en vue d'être remplie par la Direction de la sécurité industrielle canadienne;
- f) tout autre renseignement demandé par l'autorité de sécurité de la chaîne d'approvisionnement.

2.2 Pour les besoins de cet article, le terme « sous-traitant » ne comprend pas les fournisseurs sans lien de dépendance avec l'entrepreneur dont le seul rôle est de fournir de l'équipement de télécommunication ou tout autre équipement ou logiciel que l'entrepreneur utilisera pour assurer la prestation de ses services, y compris si l'équipement sera installé dans le réseau de base ou l'infrastructure de l'entrepreneur.

3 Changement de contrôle

3.1 En tout temps pendant la période du contrat, si l'autorité de sécurité de la chaîne d'approvisionnement en fait la demande, l'entrepreneur doit fournir au Canada :

- a) un organigramme sur lequel figurent toutes les personnes morales et sociétés de personnes liées à l'entrepreneur; aux fins d'application de ce paragraphe, une personne morale ou une société de personnes sera considérée comme une autre partie :

- (i) s'il s'agit de « personnes liées » ou de « personnes affiliées » selon la Loi de l'impôt sur le revenu du Canada;
 - (ii) si les entités entretiennent une relation fiduciaire (découlant d'un arrangement entre organismes ou toute autre forme de relation fiduciaire), ou ont entretenu une telle relation au cours des deux années ayant précédé la demande de renseignements;
 - (iii) si les entités ne sont pas dépendantes l'une de l'autre ou d'un même tiers;
- b) une liste de tous les actionnaires de l'entrepreneur; si l'entrepreneur est une filiale, ces renseignements doivent être fournis pour chaque société mère ou société partenaire, et ce, jusqu'au propriétaire ultime. En ce qui concerne les sociétés cotées en Bourse, le Canada prévoit que les circonstances dans lesquelles il exigerait une liste exhaustive des actionnaires seraient inhabituelles et que toute demande de sa part d'une liste des actionnaires d'une société cotée en Bourse se limiterait normalement à une liste des actionnaires détenant au moins 1 % des actions avec droit de vote;
 - c) une liste de tous les cadres et administrateurs de l'entrepreneur, comprenant l'adresse du domicile, leur date et leur lieu de naissance ainsi que leur(s) citoyenneté(s); si l'entrepreneur est une filiale, ces renseignements doivent être fournis pour chaque société mère ou société partenaire, et ce, jusqu'au propriétaire ultime;
 - d) tout autre renseignement sur la propriété et le contrôle, demandé par le Canada.

À la demande de l'autorité de sécurité de la chaîne d'approvisionnement, l'entrepreneur doit aussi fournir ces renseignements concernant ses sous-traitants. Toutefois, si le sous-traitant considère que cette information est confidentielle, l'entrepreneur peut remplir ses obligations en demandant à ce dernier de fournir l'information directement à l'autorité de sécurité de la chaîne d'approvisionnement. Que cette information soit fournie par l'entrepreneur ou le sous-traitant, le Canada s'engage à la prendre en charge, conformément au paragraphe 23(3) des Conditions générales 2035 (Conditions générales – besoins plus complexes de biens), si elle porte une mention « confidentielle » ou « exclusive ».

3.2 L'entrepreneur doit aviser, par écrit, l'autorité de sécurité de la chaîne d'approvisionnement de:

- a) tout changement de contrôle concernant l'entrepreneur;
- b) tout changement de contrôle concernant une société mère (personne morale ou société de personnes) de l'entrepreneur, et ce, jusqu'au propriétaire ultime;
- c) tout changement de contrôle concernant un sous-traitant exécutant une partie des travaux (y compris tout changement de contrôle concernant une société mère [personne morale ou société de personnes] du sous-traitant, et ce, jusqu'au propriétaire ultime).

L'entrepreneur doit fournir cet avis dans les 10 jours ouvrables du gouvernement fédéral suivant le changement de contrôle (ou dans le cas d'un sous-traitant, au plus tard 15 jours ouvrables du gouvernement fédéral après le changement de contrôle). Lorsque possible, le Canada demande que l'entrepreneur l'avise de toute transaction de changement de contrôle proposée.

3.3 Dans cet article, un « changement de contrôle » comprend, sans toutefois s'y limiter, un changement direct ou indirect de contrôle effectif de la personne morale ou de la société de personnes, que ce changement découle de la vente, du grèvement ou de la disposition des

actions (ou d'un autre type de quote-part dans la société de personnes) par tout autre moyen. Dans le cas où l'entrepreneur ou le sous-traitant est une coentreprise, cette obligation s'applique à un changement de contrôle touchant un membre (une personne morale ou une société de personnes) de la coentreprise. Si l'entrepreneur ou le sous-traitant est une société de personnes ou une société en commandite, cette obligation s'applique aussi à toute personne morale ou société en commandite qui est un associé.

- a) Si le Canada détermine, à sa seule discrétion, qu'un changement de contrôle dans l'entreprise de l'entrepreneur (concernant aussi bien l'entrepreneur lui-même que l'une de ses sociétés mères, jusqu'au premier propriétaire) peut porter atteinte à la sécurité nationale, le Canada peut résilier le contrat sans fautes en fournissant un avis à l'entrepreneur dans les 90 jours suivant l'avis de changement de contrôle de l'entrepreneur. Le Canada ne devra pas justifier la résiliation de contrat en raison d'un changement de contrôle si le Canada détermine, à sa discrétion, que ces justifications elles-mêmes pourraient porter atteinte à la sécurité nationale.
- b) Si le Canada décide, à sa discrétion, qu'un changement de contrôle touchant un sous-traitant (concernant aussi bien le sous-traitant lui-même que l'une de ses sociétés mères, jusqu'au premier propriétaire) pourrait porter atteinte à la sécurité nationale, le Canada informera l'entrepreneur par écrit de sa décision. Le Canada n'aura pas à justifier sa décision si le Canada détermine, à sa discrétion, que ces justifications elles-mêmes pourraient porter atteinte à la sécurité nationale. L'entrepreneur devra, dans les 90 jours suivant la réception de l'avis, prendre des dispositions avec un autre sous-traitant, que le Canada juge acceptable, pour la réalisation de la partie des travaux exécutée par le sous-traitant actuel (ou l'entrepreneur devra exécuter lui-même cette partie des travaux). Si l'entrepreneur ne le fait pas dans le délai prescrit, le Canada pourra résilier le contrat sans fautes en fournissant un avis à l'entrepreneur dans les 180 jours suivant le premier avis de changement de contrôle de l'entrepreneur.
- c) Dans le présent article, une résiliation sans fautes signifie qu'aucune des parties n'est tenue responsable en ce qui a trait au changement de contrôle ou à la subséquente résiliation, et que le Canada ne devra payer que les services ayant été fournis avant la date d'entrée en vigueur de la résiliation.
- d) Malgré ce qui précède, le droit à la résiliation sans fautes du Canada ne s'applique pas dans les circonstances où une réorganisation interne n'a pas d'incidence sur la propriété de la société mère (personne morale ou société de personnes) de l'entrepreneur ou du sous-traitant, selon le cas; cela signifie que le Canada n'a pas le droit de résilier le contrat en vertu du présent article si l'entrepreneur ou le sous-traitant est contrôlé, en tout temps, directement ou indirectement, par le même premier propriétaire. Toutefois, dans un tel cas, les exigences relatives à l'avis du présent article s'appliquent toujours.

Competitive procurement starts with prerequisite National Security Exemption	L'approvisionnement concurrentiel commence par l'exemption relative à la sécurité nationale préalable
Bidder provide Supply Chain Security Information (SCSI) to Contracting Authority	Le soumissionnaire fournit l'information sur la sécurité de la chaîne d'approvisionnement (ISCA) à l'autorité contractante.
Cyber and IT Security (CITS) reviews SCSI in consultation with Security Partners	La Cybersécurité et sécurité de la technologie de l'information (CSTI) examine l'ISCA conjointement avec les partenaires en matière de sécurité.
Bidder has 10 calendar days to resubmit revised SCSI with mitigation applied	Le soumissionnaire a 10 jours civils pour présenter à nouveau l'ISCA révisée comprenant les mesures d'atténuation utilisées.
Decision by CITS	La CSTI rend sa décision.
Yes	Oui
Bidder receives approval letter to continue to next phase of procurement	Le soumissionnaire reçoit l'autre d'approbation lui permettant de passer à l'étape suivante de l'approvisionnement.
Competitive procurement completes with resulting contract	L'approvisionnement concurrentiel se termine par l'attribution du contrat.
Cross check of lists provided for SCI at implementation	Comparaison des listes fournies pour l'ICA lors de la mise en œuvre.
No	Non
1 st Rejection: Debrief session with Bidder to identify mitigations	1 ^{er} refus : séance de compte rendu avec le soumissionnaire pour déterminer les mesures d'atténuation.
2 nd Rejection: Bidder does not qualify	2 ^e refus : le soumissionnaire est exclu du processus.
On-going SCI auditing from the moment the contract has been awarded until it ends.	Vérification continue de l'ICA à partir du moment où le contrat est attribué jusqu'à la fin du contrat.
Contractor provides revised SCSI on regular basis	L'entrepreneur fournit de l'ISCA révisée régulièrement.
CITS reviews SCSI in consultation with Security Partners	La CSTI examine l'ISCA conjointement avec les partenaires en matière de sécurité.

Contractor has to resubmit revised SCSI with mitigation applied	L'entrepreneur doit présenter à nouveau l'ISCA révisée comprenant les mesures d'atténuation utilisées.
Decision by CITS	La CSTI rend sa décision.
Yes	Oui
Contractor receives Approval	L'entrepreneur reçoit l'approbation
Non	Non
Debrief session with Contractor	Séance de compte rendu avec l'entrepreneur
Internal threat evaluation can lead to the review of specific equipment or services	L'évaluation des menaces internes peut mener à l'examen de matériel ou de services précis.
Contractor has to resubmit revised SCSI with mitigation applied	L'entrepreneur doit présenter à nouveau l'ISCA révisée comprenant les mesures d'atténuation utilisées.
CITS in consultation with Security Partners monitors threats or security audits	La CSTI, conjointement avec les partenaires en matière de sécurité, surveille les menaces ou les vérifications de sécurité.
Threat identified?	A-t-on décelé une menace?
Yes	Oui
Debrief session with Contractor	Séance de compte rendu avec l'entrepreneur

Appendice H – FORMULAIRE D’AUTORISATION DE TÂCHES

APPENDICE A DE L’APPENDICEE

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 SPAC	DE DE DE	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.