SERVICES PARTAGÉS CANADA

Invitation à se qualifier pour
Véhicule d'approvisionnement des services infonuagiques du gouvernement du Canada (Infonuagiques GC)

ANNEXE A, APPENDICE 2 – VOLET 2 EXIGENCES DE QUALIFICATION POUR ~~LE VOLET 2~~LES FSI ET AFS

Rappel pour les répondants:

- Les réponses à l'**Annexe A, Appendice 2 – Partie A** doivent être soumises à Services partagés Canada (SSC) à l'adresse électronique suivante avant la date limite de la demande de soumissions – ssc.cloudsolicitationsollicitationinfonuagiques.spc@canada.ca

- Les réponses à l'**Annexe A, Appendice 2 – Partie B** doivent être soumises au Centre canadien pour la cybersécurité à l'adresse électronique suivante avant la date limite de soumission – contact@cyber.gc.ca

Les douze (12) exigences suivantes doivent être satisfaites afin de démontrer la conformité à l'assurance du palier 1 **(données jusqu'au niveau Protégé A inclusivement).**

ANNEXE A, APPENDICE 2 – PARTIE A

Exigence obligatoire	Sous-catégorie	Exigence	~~Volet 2 – Nécessaires~~Nécessaire pour démontrer la conformité ~~avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)~~au Volet 2
Exigences générales			
O1	Généralités	Le répondant doit ~~indiquer le fournisseur de services d'infonuagique existant dont~~ : a) Confirmer les services d'infonuagique ~~proposés~~ publics disponibles sur le marché qui seront offerts au gouvernement du Canada au cours de l'étape de l'appel d'offres du présent processus d'approvisionnement.	~~Déterminer~~Indiquer les services d'infonuagique ~~offerts~~publics disponibles sur le marché proposés : _____

Exigence obligatoire	Sous-catégorie	Exigence	Volet 2 – NécessairesNécessaire pour démontrer la conformité avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)au Volet 2
		b) S'identifier comme le fournisseur de services d'infonuagique (FSI) ou l'autre fournisseur de services (AFS) des services d'infonuagique publics disponibles sur le marché proposés qui seront offerts au gouvernement du Canada au cours de l'étape de l'appel d'offres du présent processus d'approvisionnement;	Indiquer _____ Confirmer si le répondant s'identifie comme le fournisseur de services d'infonuagique de la proposition(FSI) ou l'autre fournisseur de services (AFS) pour les services d'infonuagique publics disponibles sur le marché proposés, conformément aux définitions qui figurent à l'annexe E de la demande de soumissions relative à l'ISQ : _____ ☐ Fournisseur de services d'infonuagique (FSI) ☐ Autre fournisseur de services (AFS)
O2	Généralités	Le répondant doit confirmer qu'il est : a) le fournisseur de services d'infonuagique pour autorisé à proposer les services d'infonuagique publics disponibles sur le marché proposés indiqués à l'exigence O1; **OU** b) un autre fournisseur de services qui est : (i) autorisé par le fournisseur de services d'infonuagique disponibles sur le marché proposés indiqués à l'exigence O1; (ii) capables de fournir au Canada tous les services d'infonuagique disponibles sur le marché du fournisseur de services d'infonuagique proposé désigné à l'exigence O1. **OU** c) Revendeur de services d'infonuagique qui est: (i) autorisé par le fournisseur de services d'infonuagique disponibles sur le marché proposés indiqués à l'exigence O1; (ii) capables de fournir au Canada accès à tous les services d'infonuagique disponibles sur le marché du fournisseur	Si le répondant est le **fournisseur de services d'infonuagique : (FSI)** • Aucune preuve de conformité n'est nécessaire pour le point O2. a) SiConfirmer que le répondant n'est pasest le fournisseur de services d'infonuagique et(FSI) pour les services d'infonuagique publics disponibles sur le marché proposés dans leur intégralité en fournissant une copie signée de l'annexe H – Formulaire d'attestation du FSI. Si le répondant est **considéré comme soit un autrel'autre fournisseur de services ou un revendeur de services d'infonuagique: (AFS)** • Le répondant doit fournir une déclaration signée de Indiquer la part du fournisseur departie des services d'infonuagique sur du papier à en tête de l'entreprise du fournisseurproposés qui atteste que : a) lerelève du répondant est un fournisseur autorisé de services d'infonuagique sur le marché offerts paret confirmer que le répondant est le fournisseur de services d'infonuagique désigné à l'exigence O1:(FSI) pour la partie indiquée des services en fournissant une copie signée de l'annexe H – Formulaire d'attestation du FSI. et b) Indiquer le répondant peut fournir tousou les services d'infonuagique offerts sur le marché du fournisseurfournisseurs

Exigence obligatoire	Sous-catégorie	Exigence	~~Volet 2 – Nécessaires~~Nécessaire pour démontrer la conformité ~~avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)~~au Volet 2
		~~de services d'infonuagique proposé désigné à l'exigence O1.~~ ~~.~~	de services d'infonuagique ~~proposé désigné~~pour les parties des services proposés qui ne relèvent pas du répondant et confirmer que le répondant est autorisé à offrir la partie indiquée dans le cadre des services proposés indiqués à l'exigence O1~~.~~ ~~a)~~b) en fournissant une copie signée de l'annexe I – Formulaire d'autorisation du FSI.
O3	Généralités	Le ~~fournisseur de services~~service d'infonuagique ~~désigné~~public proposé par le répondant à l'exigence O1 doit ~~fournir les services d'infonuagique offerts~~être disponible sur le marché à la date de clôture de l'ISQ.	Le répondant doit~~, pour~~ démontrer sa conformité~~, fournir les~~ en fournissant des documents ~~décrivant les services que comportent~~confirmant les services d'infonuagique ~~offerts sur le marché qu'il propose et qui sont décrits~~publics, indiqués à l'exigence O1~~.~~, sont disponibles sur le marché. Pour l'exigence O3, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique public disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant 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.
O4	Généralités	Le ~~fournisseur de~~ répondant doit confirmer que les services d'infonuagique publics disponibles sur le marché ~~doit présenter le~~proposé permettront aux utilisateurs du Canada d'obtenir les prix ~~de chacun des~~pour les services, ~~le mode de~~la facturation et le soutien ~~offert,~~ en dollars canadiens, ~~et, notamment~~y compris, mais sans s'y limiter, les rapports de consommation ~~des données~~.	Le répondant doit~~, pour~~ démontrer ~~qu'il est en~~sa conformité~~, fournir les documents illustrant la capacité du fournisseur~~ en fournissant **UN** des ~~services d'infonuagique disponibles sur le marché proposés à présenter le prix (en dollars canadiens) des services, le mode de facturation et le soutien, notamment la production de rapports sur la consommation des données.~~ ~~Pour être jugés conformes, les documents doivent comporter les~~ éléments suivants : a) ~~des saisies~~Documents qui comprennent des copies d'écran ou ~~des documents relatifs au~~ de la documentation du système détaillant et décrivant comment les services seront tarifés, facturés et soutenus~~,~~ en dollars canadiens. Pour l'exigence O4, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique public disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents

Exigence obligatoire	Sous-catégorie	Exigence	~~Volet 2 – Nécessaires~~Nécessaire pour démontrer la conformité ~~avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)~~au Volet 2
			techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant 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. ou b) Si les services d'infonuagique publics disponibles sur le marché proposé du répondant ne permettent pas actuellement d'obtenir les prix pour les services, la facturation et le soutien en dollars canadiens, (y compris, mais sans s'y limiter, les rapports de consommation), le répondant doit fournir une attestation figurant à l'annexe J.
O5	Généralités	Les services d'infonuagique publics disponibles sur le marché proposés doivent ~~mettre à la disposition de leurs clients les accords~~publier des ententes sur les niveaux de service ~~(ANS) publiés.~~ à la disposition des clients. 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~~habituellement fournis aux clients des services ~~d'infonuagique disponibles sur~~proposés par le ~~marché du fournisseur de services d'infonuagique~~répondant.	Le répondant doit démontrer sa conformité en fournissant des documents qui décrivent les ~~accords~~ententes sur les niveaux de service ~~publiés du fournisseur de services d'infonuagique~~ et les engagements ~~correspondants pour les services d'infonuagique disponibles sur le marché~~ à l'égard des services proposés~~.~~ publiés par le répondant. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) Captures d'écran ou documentation des accords sur les niveaux de service (ANS) publiés détaillant le soutien offert aux clients commerciaux sur le marché et rendu public (c.-à-d. ~~la~~ garantie et ~~les~~ services de maintenance et de soutien) généralement ~~fourni~~fournis aux clients des services d'infonuagique publics disponibles sur le marché du fournisseur de services d'infonuagique, notamment l'engagement en matière de service, le processus de crédit et le pourcentage de temps de disponibilité. Pour l'exigence O5, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont ~~le service~~les services d'infonuagique ~~disponible~~publics disponibles sur le marché ~~satisfait~~satisfont à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant

Exigence obligatoire	Sous-catégorie	Exigence	~~Volet 2 – Nécessaires~~Nécessaire pour démontrer la conformité ~~avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)~~au Volet 2
			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.
O6	Généralités	~~Le fournisseur de~~Les services d'infonuagique public disponibles sur le marché proposés ~~doit~~doivent permettre au consommateur de choisir la langue officielle de son choix, soit le français ou l'anglais, quand il navigue sur le site, commande des services au fournisseur de services d'infonuagique et communique avec lui.	Le répondant doit démontrer comment le service d'infonuagique public disponible sur le marché proposé permet aux consommateurs de choisir l'une des langues officielles, soit le français ou l'anglais. Pour être jugés conformes, les documents produits doivent démontrer la capacité ~~du service d'infonuagique offert sur le marché~~des services à proposer ~~les~~chacune des situations suivantes en français et en anglais : ~~d)~~a) ~~parcours~~Parcours des services sur ~~ses~~leurs sites. Web; ~~e)~~b) Services de commande ~~des services sur ses sites Web~~; ~~f)~~c) ~~communication~~Communication avec l'entreprise pour obtenir de l'aide par téléphone, par courriel ou par clavardage. Pour l'exigence O6, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant 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.
Exigences liées aux installations des centres de données			
O7	Installations des centres de données	Le fournisseur de services d'infonuagique (et, le cas échéant, l'autre fournisseur de services) des services d'infonuagique publics disponibles sur le marché proposés doit mettre en ~~place~~œuvre des mesures de sécurité qui assurent la protection des installations de ~~technologie de l'information (~~TI~~)~~ et des actifs du système d'information dans lesquels les données du ~~gouvernement du Canada~~GC sont stockées et ~~protégées~~traitées contre toute forme de manipulation, de perte, de dommages et de saisie, en fonction	~~Le répondant doit démonter comment les services d'infonuagique disponibles sur le marché proposés mettent 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 GC sont stockées pour protéger celles-ci 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.~~

Exigence obligatoire	Sous-catégorie	Exigence	~~Volet 2 – Nécessaires~~Nécessaire pour démontrer la conformité ~~avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)~~au Volet 2
		d'une approche de sécurité physique axée sur la prévention, la détection, l'intervention et la reprise. Cela comprend au minimum : a) des capacités suffisantes de redondance et de reprise dans les installations de TI et entre celles-ci, y compris, être 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'accord sur les niveaux de service (ANS) 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 validée par deux formes d'identification; f) l'accompagnement des visiteurs et la surveillance des activités des visiteurs; 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 des mesures de protection des données du GC dans les autres lieux de travail (p. ex., lieux 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, de mécanismes de surveillance vidéo dans toutes les zones sensibles et de détection des intrusions.	Le répondant doit fournir des documents démontrant comment le fournisseur de services d'infonuagique publics (et, le cas échéant, l'autre fournisseur de services) des services proposés se conforme à l'exigence O7. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) des documents relatifs au système ou des documents techniques décrivant les politiques, les procédures et les processus utilisés. Pour l'exigence O7, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le service d'infonuagique disponible sur le marché satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant 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.
Exigences relatives à la sécurité du personnel			
O8	Sécurité du personnel	Le fournisseur de services d'infonuagique publics (et, le cas échéant, l'autre fournisseur de services) disponibles sur le marché proposés 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	Le répondant doit démontrer comment le fournisseur de services d'infonuagique publics disponibles sur le marché proposés met 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

Exigence obligatoire	Sous-catégorie	Exigence	~~Volet 2 – Nécessaires~~Nécessaire pour démontrer la conformité ~~avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)~~au Volet 2
		systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Les mesures de filtrage doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou utiliser un équivalent acceptable convenu par le Canada. Cela comprend au minimum : a) une description des postes des employés et des sous-traitants qui ont besoin d'un accès aux données du Canada ou qui ont la capacité d'influencer la confidentialité, l'intégrité ou la disponibilité des services; b) le processus visant à s'assurer que les employés et les entrepreneurs connaissent, comprennent et respectent leurs responsabilités en matière de sécurité de l'information et que le rôle que l'on compte leur confier leur convient; c) le processus relatif à la sensibilisation et à la formation en matière de sécurité données à l'arrivée des employés et lorsque les rôles des employés et sous-traitants changent; d) le processus qui est appliqué lorsqu'un employé ou un sous-traitant change de rôle ou au moment d'une cessation d'emploi; e) l'approche de détection des personnes malveillantes potentielles à l'intérieur de l'organisation et les mesures de contrôle mises en œuvre pour atténuer le risque d'accès aux données du GC ou les répercussions sur la fiabilité des services d'infonuagique accueillant les actifs et les données du GC.	aux actifs des systèmes d'information sur lesquels les données du Canada sont stockées et traitées. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) des documents relatifs au système ou des documents techniques décrivant les politiques, les procédures et les processus utilisés. Pour l'exigence O8, il ne suffit pas de reprendre l'exigence obligatoire; on doit expliquer et démontrer la façon dont le fournisseur de services d'infonuagique publics disponibles sur le marché proposés satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse. Si le Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant peut faire référence à des documents supplémentaires soumis avec sa réponse. On lui demande d'indiquer à quel endroit dans la réponse se trouvent les documents mentionnés, leur titre et les numéros de page et de paragraphe.

Exigence obligatoire	Sous-catégorie	Exigence	Volet 2 – NécessairesNécessaire pour démontrer la conformité avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)au Volet 2
Exigences liées à l'assurance d'une tierce partieen matière de protection des données			
O9	Protection des donnéesAssurance d'une tierce partie	Les services d'infonuagique du fournisseur doivent être conçus et élaborés pour garantir la sécurité lieux physiques des services d'infonuagique publics disponibles sur le marché proposés et comprendre la mise en œuvre(où pourraient être hébergées des données du Canada) doivent être situés dans l'un de politiques etces pays : a) Un pays de procédures sur la sécurité l'Organisation du traité de l'information etl'Atlantique Nord (OTAN); b) Un pays de mesuresl'Union européenne (UE); c) Un pays avec lequel le Canada a un accord international bilatéral en matière de sécurité industrielle **Remarque**contrôle **à l'attention des répondants :** Des renseignements supplémentaires sur les pays de lal'OTAN se trouvent au lien suivant : https://www.nato.int/cps/en/natohq/nato_countries.htm Des renseignements supplémentaires sur les pays de l'OTAN se trouvent au lien suivant : https://europa.eu/european-union/about-eu/countries_fr Dans le cadre du Programme de sécurité des contrats, des accords internationaux bilatéraux en matière de sécurité industrielle ont été conclus avec les pays énumérés sur le site Web https://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html de SPAC, tel qu'il est mis à jour de temps à autre.	La conformité doit être démontrée à l'aide d'au moins une des certifications de l'industrie énoncées ci-dessous, puis validée au moyen d'évaluations de tiers indépendants. a) ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences **OU** AICPA Service Organization Control (SOC) 2 Type II **ET** AutoévaluationLe répondant doit fournir les documents démontrant comment le fournisseur des services d'infonuagique publics disponibles sur le marché proposés (décrits à l'exigence O1) répond à l'exigence obligatoire décrite à l'exigence O9. Pour être jugés conformes, les documents doivent comporter les éléments suivants : a) une liste à jour (en date de la clôture de l'invitation à se qualifier) des lieux physiques (y compris le nom de la ville et du pays) de chaque centre de données où pourrait être hébergées les données du Canada, y compris les données de sauvegarde ou les données tenues à des fins de redondance. b) Pour l'exigence O9, il ne suffit pas de ses services conformément à la version 3.01 dereprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la Cloud Controls Matrix (CCM) de la Cloud Security Alliance (CSA) ou à une version subséquente. La certification ISO27001 ou le rapport d'évaluation et l'AICPA SOC 2 Type II doivent : a) indiquer la dénomination sociale dufaçon dont le fournisseur de services d'infonuagique proposé; b)a) satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur finalindiquer la date ou l'état de la certification actuelle;

Formatted: Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0.63 cm

Exigence obligatoire	Sous-catégorie	Exigence	~~Volet 2 – Nécessaires~~Nécessaire pour démontrer la conformité ~~avec l'exigence en matière d'assurance du palier 1 (faible incidence) (données jusqu'au niveau Protégé A inclusivement)~~au Volet 2
			~~La portée du rapport doit renvoyer aux lieux et aux services proposés par les services d'infonuagique disponibles sur le marché proposés. 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;~~ étayer sa réponse. ~~d)~~ Si le gouvernement du Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant 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.~~être valide pour toute la durée du contrat;~~ ~~e) 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 (SGQ);~~ ~~avoir été émis au cours des 12 mois précédant la date de clôture de la soumission.~~

ANNEXE A, APPENDICE 2 – PARTIE B

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 2
Exigences en matière de protection des données			
O10	Assurance d'une tierce partie~~Protection des données~~	Les ~~lieux physiques~~ services du fournisseur de services d'infonuagique publics (et, le cas échéant, de l'autre fournisseur de services) doivent être conçus et élaborés pour garantir la sécurité des services d'infonuagique disponibles sur le marché proposés ~~(où pourraient être hébergées des données du Canada) doivent être:~~ ~~a) des pays de l'Organisation du Traité de l'Atlantique Nord (OTAN);~~ ~~b) des pays membres de l'Union européenne (UE);~~ ~~c) des pays avec lesquels le Canada a un accord international ou bilatéral~~ et comprendre la mise en ~~matière~~œuvre de ~~sécurité industrielle.~~ politiques et ~~**Remarque** : Le programme~~ de procédures sur la sécurité ~~des contrats (PSC) a conclu un accord international ou bilatéral en matière~~ de l'information et de mesures de contrôle de la sécurité ~~industrielle avec les pays énumérés dans le site Web suivant : http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html. La liste est mise à jour périodiquement.~~ .	Le répondant doit fournir au Canada les documents démontrant comment le fournisseur ~~des~~de services d'infonuagique publics (et, le cas échéant, l'autre fournisseur de services) disponibles sur le marché proposés ~~(décrits à~~respecte l'exigence ~~O1) répond à l'exigence obligatoire décrite à l'exigence~~ O10. ~~Pour être jugés conformes,~~ Le répondant doit fournir les ~~documents doivent comporter~~certifications suivantes de l'industrie concernant les services proposés pour démontrer sa conformité : 1) Un des éléments suivants : a. ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences; ou b. 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 des services d'infonuagique; 2) Contrôle de l'organisation des services de l'AICPA (SOC) 2 Type II pour les principes de confiance en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité. Chaque certification ou rapport d'évaluation fourni doit : a) Être valide à la date de clôture de la demande de soumissions; b) indiquer la dénomination sociale du fournisseur de services d'infonuagique proposé; c) indiquer la date ou l'état de la certification actuelle; ~~a)~~ La portée du rapport doit renvoyer aux lieux et aux services proposés par les services d'infonuagique disponibles sur le marché proposés. Si la méthode créée est utilisée~~une liste à jour (en date de la clôture de l'invitation à se qualifier) des lieux physiques (y compris le nom de la ville et du pays) de chaque centre de données où pourrait être hébergées les données du Canada, y compris les données de sauvegarde ou les données tenues à des fins de redondance.~~

Formatted: Indent: Left: 0 cm

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 2
			~~Pour l'exigence O10, il ne suffit pas de reprendre l'exigence obligatoire; le répondant doit expliquer et démontrer la façon dont le fournisseur de services d'infonuagique satisfait à l'exigence. Le répondant peut fournir des copies d'écran, des documents techniques et des documents destinés à l'utilisateur final pour étayer sa réponse.~~ d) ~~Si le~~ 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 e) 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 (SGQ). **Remarque :** • **Des certifications doivent être fournies pour toutes les parties des services proposés indiquées à l'exigence O1.** • **Les certifications doivent être accompagnées de rapports d'évaluation.** ~~Canada détermine que la justification est incomplète, la réponse du répondant sera jugée non conforme. Dans sa justification, le répondant 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.~~
Exigences en matière de gestion des risques liés à la chaîne d'approvisionnement			
O11	Gestion de la chaîne d'approvision-nement	Le répondant doit fournir une liste de tous les fournisseurs tiers, ainsi que les renseignements portant sur la nature de leur statut (p. ex., filiale, sous-traitant, etc.) qui fourniraient au Canada des services d'infonuagique publics disponibles sur le marché proposés. Pour les besoins de cette exigence, une entreprise qui fournit des biens au fournisseur de services d'infonuagique publics disponibles sur le marché proposés, mais qui n'effectue pas une partie de la chaîne d'approvisionnement qui pourrait fournir au Canada des services d'infonuagique publics disponibles sur le marché proposés, n'est pas considérée comme un tiers. Les tiers peuvent comprendre, par exemple, les techniciens qui pourraient être déployés ou qui entretiennent les services	Le répondant 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 des services d'infonuagique publics disponibles sur le marché proposés, qu'il s'agisse : (i) de sous-traitants du répondant ou du fournisseur de services d'infonuagique publics; (ii) de sous-traitants des sous-traitants du répondant ou du fournisseur de services d'infonuagique publics, en aval; (iii) de toute filiale. La liste doit au moins comporter ce qui suit : a) le nom du tiers; b) l'adresse du siège social du tiers;

Exigence obligatoire	Sous-catégorie	Exigence	Nécessaire pour démontrer la conformité au Volet 2
		d'infonuagique publics disponibles sur le marché du fournisseur de services d'infonuagique qui ont été proposés par le répondant à l'exigence O1. **Remarque :** Les répondants sont informés que les étapes d'approvisionnement subséquentes peuvent les obliger à informer régulièrement le Canada de toute mise à jour de la liste de fournisseurs tiers.	c) la portion des travaux qui serait exécutée par le tiers; d) les emplacements où le tiers fournirait au Canada les services d'infonuagique publics disponibles sur le marché proposés; e) tout tiers qui pourrait avoir accès aux données du Canada dans le cadre des services d'infonuagique publics disponibles sur le marché proposés. Si le ~~fournisseur~~FSI ou l'AFS de services d'infonuagique publics disponibles sur le marché proposés ne fait appel à aucun tiers pour effectuer une partie quelconque de la chaîne d'approvisionnement qui pourrait fournir au Canada des services d'infonuagique publics disponibles sur le marché proposés, le répondant doit l'indiquer dans sa réponse à cette exigence.
O12	Gestion des risques liés à la chaîne d'approvisionnement	Le fournisseur des services d'infonuagique publics (et, le cas échéant, l'autre fournisseur de services) disponibles sur le marché proposés (décrits à l'exigence O1) doit mettre en œuvre des mesures de protection visant à atténuer les menaces et les vulnérabilités associées à la chaîne d'approvisionnement des services de TI. Ces mesures comprennent, sans s'y limiter, la conception et la mise en œuvre de mesures de contrôle visant à atténuer et à contenir les risques liés à la sécurité des données au moyen de la répartition convenable des tâches, de l'accès reposant sur le rôle et des droits d'accès minimaux pour tout le personnel au sein de la chaîne d'approvisionnement.	Le répondant doit démontrer comment le fournisseur de services d'infonuagique publics (et, le cas échéant, l'autre fournisseur de services) disponibles sur le marché proposés se conforme ~~aux exigences figurant dans~~ à l'exigence O12~~.~~, selon ce qui est documenté dans le programme d'évaluation de la sécurité des technologies de l'information du fournisseur de services d'infonuagique. Pour être jugés conformes, les documents fournis doivent présenter au moins l'une des trois options suivantes : 1. ISO/IEC 27036 Technologies de l'information – Techniques de sécurité – Sécurité des renseignements pour la relation avec le fournisseur (parties ~~-~~ 1 à 4); ou 2. NIST Special Publication 800-161 – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*; ou 3. Toute autre norme ou pratique exemplaire pouvant démontrer que les services d'infonuagique disponibles sur le marché proposés respectent les exigences. Le plan de gestion des risques liés à la chaîne d'approvisionnement doit décrire l'approche du fournisseur de services d'infonuagique en matière de gestion des risques liés à la chaîne d'approvisionnement et démontrer comment le fournisseur de services d'infonuagique publics disponibles sur le marché proposés réduira et atténuera les risques liés à la chaîne d'approvisionnement.