RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A 0S5
Bid Fax: (819) 997-9776

Revision to a Request for Supply Arrangement - Révision à une demande pour un arrangement en matière d'approvisionnement

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Mainframe & Business Software Procurement Division / Div des achats des ordi principaux et des logiciels de gestion
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Quebec
K1A 0S5

Title - Sujet DAMA - Logiciels-services (GC)	
Solicitation No. - N° de l'invitation EN578-191593/F	**Date** 2019-07-05
Client Reference No. - N° de référence du client 20191593	**Amendment No. - N° modif.** 006
File No. - N° de dossier 003eem.EN578-191593	**CCC No./N° CCC - FMS No./N° VME**
GETS Reference No. - N° de référence de SEAG PW-$EEM-003-35660	
Date of Original Request for Supply Arrangement **Date de demande pour un arrangement en matière d'app. originale**	2019-05-10
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2022-05-10**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
Address Enquiries to: - Adresser toutes questions à: Boyer, Tania	**Buyer Id - Id de l'acheteur** 003eem
Telephone No. - N° de téléphone (613) 858-9232 ( )	**FAX No. - N° de FAX** ( ) -
Delivery Required - Livraison exigée	
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	
Security - Sécurité This revision does not change the security requirements of the solicitation. Cette révision ne change pas les besoins en matière de sécurité de l'invitation.	

Instructions: See Herein

Instructions: Voir aux présentes

Acknowledgement copy required **Accusé de réception requis**	**Yes - Oui** ☐	**No - Non** ☐

The Offeror hereby acknowledges this revision to its Offer.
Le proposant constate, par la présente, cette révision à son offre.

Signature **Date**

Name and title of person authorized to sign on behalf of offeror. (type or print)
Nom et titre de la personne autorisée à signer au nom du proposant.
(taper ou écrire en caractères d'imprimerie)

For the Minister - Pour le Ministre

Canada

DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA)
MÉTHODE D'APPROVISIONNEMENT DE LOGICIELS-SERVICES (INFONUAGIQUE GC)
DEMANDE DE SOUMISSIONS N^{O} : EN578-191593/F
SERVICES PUBLICS ET APPROVISIONNEMENT CANADA (SPAC)

MODIFICATION 006

La modification 006 vise à :

1.0 Répondre aux questions reçues au sujet de la DAMA, comme il est précisé à la section 1.0 ci-dessous;
2.0 Apporter les modifications à la DAMA, comme il est précisé à la section 2.0 ci-après.

1.0 Répondre aux questions sur la DAMA :

Remarque : les questions peuvent avoir été modifiées ou condensées.

QUESTIONS	RÉPONSES
Q.31 Annexe A – Exigences de qualification – Palier 1 O5 et Palier 2 O8 (Assurance d'une tierce partie) Dans le cadre de demandes antérieures du Canada pour lesquelles il fallait fournir des rapports de certification de sécurité SOC 2 Type II, ceux-ci devaient être transmis directement au Centre canadien pour la cybersécurité (CCC) du Centre de la sécurité des télécommunications (CST) puisqu'il s'agissait de rapports comportant des renseignements délicats relatifs à la sécurité. Par ailleurs, la diffusion de ces rapports SOC est habituellement gérée par les évaluateurs tiers plutôt que par le fournisseur de services d'infonuagique, et les rapports sont protégés par un mot de passe de manière à ce que seul le	**R.31** Le Canada a examiné la demande. Palier 1 O5 et Palier 2 O8 (Assurance d'une tierce partie) de l'annexe A, Exigences de qualification, sont modifiées conformément à la section A (i) et (ii), DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA), ci-après.

demandeur puisse y avoir accès. Le Canada pourrait-il confirmer qu'il serait acceptable de lui fournir un hyperlien vers le site Web des évaluateurs tiers pour qu'il puisse accéder au rapport détaillé en toute sécurité? Sinon, veuillez confirmer qu'il serait acceptable de transmettre les rapports SOC directement au CCC du CST pour se conformer à cette exigence.	
Q.32 Annexe A – Exigence obligatoire – Palier 1 O6 (Gestion de la chaîne d'approvisionnement) Les fournisseurs de services d'infonuagique à grande échelle comptent sur un certain nombre de fournisseurs de sous-processeurs pour assurer les services offerts et offrir un soutien connexe. Ces fournisseurs de services offrent une gamme de services, qu'il s'agisse du développement de logiciels ou de leur acceptation par le client. Plusieurs fournisseurs de services d'infonuagique publient des listes publiques de leurs sous-processeurs pour les fournisseurs à grande échelle, auxquelles le gouvernement du Canada peut accéder. À titre de fournisseur de service à grande échelle, il n'est pas pratique que le CCC évalue la liste de sous-processeurs. Nous proposons que l'État tire parti de la certification de la chaîne d'approvisionnement par rapport à la norme NIS 800-161.	**R.32** Le Canada a examiné la demande et l'exigence demeure inchangée.
Q.33 Annexe A – Exigences de qualification – Palier 1, exigence O11 (Gestion des risques de la chaîne d'approvisionnement) Conformément à la norme internationalement reconnue en matière de développement de logiciels sécurisés, l'État devrait demander spécifiquement aux fournisseurs de services SaaS de se conformer / d'être en conformité avec la norme ISO 27034.	**R.33** Le Canada a examiné la demande et l'exigence demeure inchangée.

Q.34 Annexe A – Exigences de qualification – Palier 1 O13 et Palier 2 O19 (Fuite d'information) Il revient à un client de vérifier s'il y a eu des fuites d'information et d'y remédier dans un contexte de SaaS. Par défaut, les fournisseurs de services d'infonuagique n'ont pas accès aux données des clients. Les fournisseurs de services d'infonuagique fournissent des outils libre-service afin de permettre aux administrateurs des clients de vérifier s'il y a eu des fuites d'information et d'y remédier dans un environnement infonuagique. La conformité au RI-9 et aux améliorations de contrôle connexes peut ainsi tout de même être assurée. Nous vous demandons de bien vouloir modifier l'exigence O13 du Palier 1 et l'exigence O19 du Palier 2 de manière à demander aux fournisseurs de SaaS de fournir des outils libre-service aux administrateurs des clients aux fins d'intervention en cas de fuite d'information. Par exemple : (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 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 approuvés par écrit par le Canada. Sans égard à ce qui précède, le processus d'intervention en cas de fuite d'information du fournisseur doit comprendre, à tout le moins : (a) un processus d'identification du renseignement précis impliqué dans la contamination d'un actif ou d'un système; (b) un processus visant à isoler et à éradiquer un renseignement ou un système contaminé;	**R.34** Le Canada a examiné la demande. L'exigence O13 du Palier 1 et l'exigence O19 du Palier 2 (Fuite d'information) de l'annexe A, Exigences de qualification, sont modifiées conformément à la section A (iii), DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA), ci-après.

(c) un processus d'identification des renseignements ou des systèmes pouvant avoir été subséquemment contaminés et de toute autre mesure prise pour empêcher la propagation de la contamination. Exigence O13 du Palier 1 et exigence O19 du Palier 2 – Fuite d'information (exigence 2) Puisqu'il revient au client d'intervenir en cas de fuite d'information, nous vous demandons de supprimer l'exigence (2) selon laquelle « Le fournisseur doit transmettre au Canada un processus d'intervention en cas de fuite d'information à jour, et ce, chaque année… ».	
Q.35 Annexe A – Exigences de qualification – Palier 2 O13 (Confidentialité par conception) Il y a lieu de réviser cette exigence puisque la norme qui y est citée ne se rapporte pas au développement d'applications ou à la protection des renseignements personnels. La norme ISO 27034 – Technologies de l'information – Techniques de sécurité – Sécurité d'information est pertinente dans ce cas-ci. Elle traite des éléments du Cycle de vie de développement en sécurité, que le gouvernement du Canada a demandé dans le cadre du profil de contrôle de la sécurité PBMM. La norme ISO 27032 fait référence à la sécurité du cyberespace, ce qui ne correspond pas à la norme applicable dans ce cas-ci.	**R.35** Le Canada a examiné la demande. L'exigence O13 du Palier 2 (Confidentialité par conception) de l'annexe A, Exigences de qualification, est modifiée conformément à la section A (iv), DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA), ci-après.
Q.36 Annexe B – Obligations en matière de sécurité et protection de la vie privée Section 5 (Vérification de la conformité aux obligations de sécurité) Les fournisseurs de services d'infonuagique ne sommes pas mesure de se conformer à cette exigence, puisque qu'ils ne fournissent pas de plans de mise en œuvre et ne signalent pas aux clients les progrès réalisés par rapport aux mesures d'amélioration. Étant donné que ces facteurs auront également une incidence sur les	**R.36** Le Canada a examiné la demande. La section 5 (Vérification de la conformité aux obligations de sécurité) de l'annexe B, Obligations en matière de sécurité et protection de la vie privée, est modifiée conformément à la section A (v), DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA), ci-après.

fournisseurs tiers de SaaS qui ont été affectés aux plateformes des fournisseurs mondiaux de services d'infonuagique à grande échelle, nous estimons qu'il y aura des conséquences négatives considérables sur les objectifs de l'État qui consistent à offrir un catalogue complet de services au gouvernement du Canada. Nous vous demandons de bien vouloir supprimer l'annexe B, section 5.2 au complet.	
Q.37 Annexe B – Obligations en matière de sécurité et protection de la vie privée Section 7 (Sécurité des réseaux et des communications) L'article 7 (b) ne comprend pas de définition du point de vue de l'État à l'égard des microservices. Les microservices peuvent désigner une multitude de processus dans un continuum allant de processus adjacents dans le même appareil virtuel aux processus distribués à l'échelle d'un réseau public d'un centre de données distinct. Par ailleurs, les clients peuvent décider de configurer leurs services déployés de manière à ne pas utiliser le chiffrement (par exemple, en ce qui a trait à la rétrocompatibilité, les clients peuvent choisir d'utiliser des protocoles obsolètes, comme http, même s'il n'est pas recommandé de le faire. En règle générale, les fournisseurs de services d'infonuagique à grande échelle chiffrent les données en transit entre les serveurs, lorsqu'ils exercent un contrôle total sur les communications. Nous demandons donc au gouvernement du Canada de supprimer cette exigence.	**R.37** Le Canada a examiné la demande. La section 7 (Sécurité des réseaux et des communications) de l'annexe B, Obligations en matière de sécurité et protection de la vie privée, est modifiée conformément à la section A (vi), DEMANDE D'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (DAMA), ci-après.
Q.38 Annexe F – clause du contrat subséquent de logiciel-service Conformément à l'article 4.1 de la clause c) Indemnisation – du contrat subséquent, le Canada demande à l'entrepreneur d'accepter d'indemniser le Canada de toutes les pertes et dépenses (y compris les frais juridiques) découlant de toute réclamation pour violation de	**R.38** Le Canada a examiné la demande. Le paragraphe c) (Indemnisation) de la section 4.1 Services de solution de l'annexe F, Clauses du contrat subséquent, est modifiée conformément à la section B (i), ANNEXE F – CLAUSES DU CONTRAT SUBSÉQUENT, ci-après.

propriété intellectuelle par un tiers fondée sur l'utilisation de la solution par le Canada. Même si l'entrepreneur accepte en principe la disposition précitée, il souhaite préciser qu'une telle disposition devrait être modifiée de manière à clarifier qu'il convient de protéger le Canada, si un tiers prétend que les services ou les produits de SaaS fournis au Canada par l'entrepreneur portent atteinte aux droits de propriété intellectuelle, et de payer les coûts, dommages-intérêts et frais de justice alloués au bout du compte par un tribunal, pourvu que le Canada : a) informe par écrit, sans tarder, l'entrepreneur de la réclamation; b) autorise l'entrepreneur à prendre part pleinement à la contestation de la réclamation et aux négociations visant à la régler et collabore avec lui à cette contestation et à ces négociations; c) obtienne l'approbation préalable de l'entrepreneur à l'égard de toute entente découlant des négociations menées avec le tiers aux fins de règlement. Compte tenu de ce qui précède et du fait que cette disposition porte sur la clause de limitation de la de responsabilité qu'élaborent actuellement SPAC et SPC de concert avec l'industrie de TI, la disposition en question devrait être supprimée et remplacée par la nouvelle clause sur la limitation de la responsabilité (y compris la disposition connexe sur la violation du droit de propriété intellectuelle), dès qu'elle sera prête (voir la remarque à l'article 12 des clauses du contrat subséquent).	
Q.39 Annexe F – clause du contrat subséquent de logiciel-service Conformément à l'article 5.6 – Pas d'infraction – le Canada demande à l'entrepreneur de garantir que	**R.39** Le Canada exige que les fournisseurs soumettent des formulaires d'autorisation de l'éditeur de logiciels-services afin de certifier que, au moment de la prestation d'un arrangement en

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. L'entrepreneur ne peut pas offrir une telle garantie; il peut toutefois accepter de protéger le Canada découlant de toute réclamation pour violation de propriété intellectuelle par un tiers. L'article 5.6 devrait donc être supprimé. De plus, puisque cette disposition porte sur la clause de limitation de la responsabilité qu'élaborent actuellement SPAC et SPC de concert avec l'industrie de TI, la disposition en question devrait être supprimée et remplacée par la nouvelle clause sur la limitation de la responsabilité (y compris la disposition connexe sur la violation du droit de propriété intellectuelle, dès qu'elle sera prête (voir la remarque à l'article 12 des clauses du contrat subséquent).	matière d'approvisionnement, le fournisseur possédait le formulaire d'autorisation prérequis rempli par un tiers qui est propriétaire des droits de propriété intellectuelle (PI). Cependant, les fournisseurs seront autorisés à mettre à jour leur catalogue de solutions SaaS de manière continue et modifieront leur offre commerciale, et bien que le Canada exige que les fournisseurs maintiennent une telle autorité sur les produits livrables, le Canada exige également que les fournisseurs veillent : 1. À avoir et à maintenir l'autorité nécessaire pour exécuter le contrat; 2. À ce que la solution SaaS ne soit pas reconnue comme portant atteinte aux droits qu'un tiers pourrait avoir; et, 3. À ce que l'octroi au Canada par le fournisseur d'un accès à une solution SaaS à des fins d'utilisation ne porte pas atteinte aux droits qu'un tiers pourrait avoir. Finalement, le Canada continuera d'exiger que les fournisseurs indemnisent le Canada pour toute réclamation pour violation contre le Canada, en fonction de l'accès et l'utilisation autorisés par les fournisseurs, conformément au contrat. Le Canada reconnaît que les fournisseurs ne peuvent pas contrôler la présentation de réclamations par un tiers, mais il exige que les fournisseurs protègent le Canada contre de telles réclamations découlant de la prestation d'un fournisseur. Par conséquent, la section 5.6 (Pas d'infraction) est modifiée conformément à la section B (ii), ANNEXE F – CLAUSES DU CONTRAT SUBSÉQUENT, ci-après.

Q.40 Annexe A – Exigences de qualification – Palier 1 O3 (Installations des centres de données) Le fournisseur demande au Canada modifie ou clarifie les éléments suivants : (i) sous-paragraphe e) on y demande deux formes d'identification. Puisque les politiques existantes qui s'appliquent aux services infonuagiques commerciaux disponibles, le fournisseur demande qu'une seule forme d'identification soit exigée; et (ii) sous-paragraphe i), veuillez préciser ce que l'on entend par « sites de télétravail »; qu'est-ce que le Canada entend par « travailler à partir de la maison »? Dans un tel cas, le Canada s'attend-il à pouvoir inspecter le domicile d'un employé?	**R.40** Le Canada a examiné la demande et l'exigence demeure inchangée. (i) En vue de préciser le sous-paragraphe e) de l'exigence O3 du Palier 1 à l'annexe A, Exigences de qualifications, le fournisseur doit fournir au moins deux (un fondamental et un à l'appui) documents d'identité, conformément à la Norme sur le filtrage de sécurité du Secrétariat du Conseil du Trésor du Canada (SCT). (ii) En vue de préciser le sous-paragraphe i) de l'exigence O3 du Palier 1 à l'annexe A, les sites de télétravail s'entendent des sites éloignés où un travail est effectué à l'extérieur du bureau; un employé peut travailler de la maison, d'un café ou de tout autre endroit qui n'est habituellement pas un bureau. « Travailler de la maison » s'entend de la maison de l'employé. Dans ces cas, les employés doivent avoir accès à des renseignements protégés ou confidentiels à partir de leur maison et seront sujets à des inspections à domicile par le Canada. L'inspection est obligatoire pour tous les endroits où des renseignements gouvernementaux confidentiels sont conservés en format papier ou numérique dans la maison de l'employé, le cas échéant. Afin de s'assurer que l'endroit répond aux exigences en matière de sécurité, le fournisseur devra indiquer toutes les adresses où des documents, des renseignements ou des systèmes informatiques confidentiels sont conservés.

Q.41 Nous aimerions attirer votre attention sur les questions qui figurent dans la DP sur le nuage de SPC en lien avec l'intégrité de la chaîne d'approvisionnement. À la lumière des préoccupations ci-après des fournisseurs, l'État pourrait-il réévaluer les exigences de l'ISCA et modifier le processus d'intégrité associé à la présente DAMA de manière à utiliser les certifications reconnues dans l'industrie? Par ailleurs, la cohérence pourrait ainsi être assurée entre SPC et SPAC.	**R.41** Le Canada a examiné la demande et l'exigence demeure inchangée.
Q.42 Les obligations en matière de protection de la vie privée dont il est question à l'appendice D imposent une responsabilité potentielle sur les fournisseurs et ne comprennent pas suffisamment de renseignements pour permettre aux fournisseurs d'en analyse l'incidence : (i) Le Canada peut-il préciser les circonstances dans lesquelles l'autorité contractante exige du fournisseur qu'il procède à une vérification de la protection de la vie privée? (ii) Le Canada peut-il préciser les qualifications (American Institute of Chartered Public Accountants [AICPA], Comptables professionnels agréés du Canada [CPA]) ou Organisation internationale de normalisation (ISO) qu'exige le vérificateur tiers?	**R.42** Le Canada a examiné la demande. (i) La section 1 (Audit de conformité) de l'appendice D, Obligations en matière de protection de la vie privée, est supprimée conformément à la section B (iii), ANNEXE F - CLAUSES DU CONTRAT SUBSÉQUENT, ci-après. (ii) En accordance avec la section 5 de l'annexe B « OBLIGATIONS EN MATIÈRE DE SÉCURITÉ ET PROTECTION DE LA VIE PRIVÉE », Conformément aux certifications ISO obligatoires, un audit de cette norme ou de ce cadre de contrôle sera lancé au moins une fois par an. Chaque audit sera effectué conformément aux normes et règles de l'organisme de réglementation ou de l'accréditation pour chaque norme ou cadre de contrôle applicable; et Chaque audit sera réalisé par des auditeurs tiers indépendants qui (i) sont qualifiés selon le régime de certification AICPA, CPA Canada ou ISO et (ii) sont conformes à la norme ISO / IEC 17020 relative au système de

	management de la qualité à la sélection et aux frais du fournisseur. Chaque vérification donnera lieu à la production d'un rapport de vérification qui doit être mis à la disposition du Canada. Le rapport d'audit doit clairement divulguer toute constatation importante du tiers auditeur. L'entrepreneur doit, à ses frais, résoudre rapidement les problèmes et corriger les anomalies relevées dans tout rapport de vérification à la satisfaction du vérificateur.
Q.43 Annexe F (anciennement l'annexe E) – EXIGENCES RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEURS ÉTRANGERS Nous demandons que le Canada confirme que cette annexe F ne s'applique pas à un fournisseur canadien même si ce dernier fait appel à des sous-traitants et à des sous-fabricants situés à l'extérieur du Canada.	**R.43** Le Canada confirme que l'annexe F (anciennement l'annexe E), EXIGENCES RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEURS ÉTRANGERS, s'applique effectivement aux sous-fabricants ou aux sous-traitants étrangers situés à l'extérieur du Canada. Le fournisseur canadien qui emploie des sous-traitants ou sous-fabricants étrangers doit se conformer à l'ANNEXE F, EXIGENCES RELATIVES À LA SÉCURITÉ POUR LES FOURNISSEURS ÉTRANGERS.

2.0 Les clauses et les modalités suivantes sont intégrées à la DAMA :

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

(i) **SUPPRIMER l'exigence « O5 du Palier 1 », en entier et la REMPLACER par ce qui suit :**

Exigence
Le logiciel-service doit être conçu et développé pour assurer la sécurité de leur logiciel-service public proposé disponible sur le marché, y compris la mise en œuvre des politiques, des procédures et des contrôles de sécurité de l'information. Pour les fournisseurs qui ont déjà complété l'évaluation en sécurité en fournissant au CCC les rapports de certification de sécurité SOC 2 Type II et qui ont déjà conclu une entente de non-divulgation (END) avec le CCC doivent transmettre leur certification et leurs rapports de certification directement au CCC à contact@cyber.gc.ca afin de se conformer à cette exigence. Pour les fournisseurs qui n'ont pas complété l'évaluation en sécurité, le processus d'intégration commencera une fois que la soumission respectera les exigences de la demande d'arrangement en matière d'approvisionnement et satisfera à tous les critères d'évaluation techniques et financiers obligatoires et fournira tous les éléments obligatoires de certifications pour être déclarée recevable. SPAC référera ensuite le fournisseur aux services clients de CCC pour commencer le processus d'intégration de l'évaluation en TI et pour conclure une END en vue de recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire exigée aux termes de cette exigence.

(ii) **SUPPRIMER l'exigence « O8 du Palier 2 » et la remplacer par ce qui suit :**

Exigence
Le logiciel sous forme de service commercialement disponible doit être conçu et élaboré pour garantir la sécurité du logiciel-service commercialement disponible proposé et comprendre la mise en oeuvre de politiques et de procédures sur la sécurité de l'information et de mesures de contrôle de la sécurité. Le fournisseur du logiciel-service commercialement disponible proposé doit également se conformer aux exigences de sécurité sélectionnées dans le Profil des mesures de sécurité pour les services de la TI du GC fondés sur l'informatique en nuage pour les renseignements classés « Protégés B, intégrité moyenne,

Exigence
disponibilité moyenne » (PBMM) pour la portée du logiciel-service commercialement disponible proposé fourni. La conformité sera validée et vérifiée au moyen du processus d'évaluation de la sécurité des technologies de l'information (TI) du fournisseur de services infonuagiques (CSP) du Centre canadien pour la cybersécurité (CCCS) (ITSM.50.100) (https://cyber.gc.ca/fr/orientation/processus-devaluation-de-la-securite-des-technologies-de-linformation-sappliquant-aux). Tout fournisseur qui a participé au processus doit fournir de la documentation confirmant qu'il a terminé le processus d'intégration avec (i) une copie du plus récent rapport d'évaluation rempli fourni par le CCCS; et (ii) une copie du rapport sommaire le plus récent fourni par le CCCS. Cela accélérera le processus de qualification et, en même temps, n'oblige pas le fournisseur à démontrer la conformité. Pour les fournisseurs qui ont déjà complété l'évaluation en sécurité en fournissant au CCC les rapports de certification de sécurité SOC 2 Type II et qui ont déjà conclu une entente de non-divulgation (END) avec le CCC doivent transmettre leur certification et leurs rapports de certification directement au CCC à contact@cyber.gc.ca afin de se conformer à cette exigence. Pour les fournisseurs qui n'ont pas complété l'évaluation en sécurité, le processus d'intégration commencera une fois que la soumission respectera les exigences de la demande d'arrangement en matière d'approvisionnement et satisfera à tous les critères d'évaluation techniques et financiers obligatoires et fournira tous les éléments obligatoires de certifications pour être déclarée recevable. SPAC référera ensuite le fournisseur aux services clients de CCC pour commencer le processus d'intégration de l'évaluation en TI et pour conclure une END en vue de recevoir une copie du formulaire de soumission d'intégration, ainsi que toute information supplémentaire exigée aux termes de cette exigence.

(iii) **SUPPRIMER l'exigence «O13 du Palier 1 et l'exigence O19 du Palier 2» en entier, et les REMPLACER par ce qui suit :**

Exigence
Fuite d'information (1) Le fournisseur doit avoir un processus documenté qui énonce son approche en cas d'incident de fuite d'information. Le processus du fournisseur doit être harmonisé i) aux directives de la section IR-9 intitulée « Intervention en cas de fuite d'information » du document ITSG-33, ou ii) à une autre pratique exemplaire du secteur approuvée par écrit par le Canada. Nonobstant ce qui précède, le processus d'intervention en cas de fuite d'information du fournisseur doit comprendre, à tout le moins : a) un processus d'identification des éléments de données précis utilisés dans la contamination d'un système; b) un processus visant à isoler et à éradiquer un système contaminé; c) un processus d'identification des systèmes pouvant avoir été subséquemment contaminés et toute autre mesure prise pour empêcher la propagation de la contamination; d) une confirmation d'une personne-ressource, de procédures appropriées et d'une entente concernant la communication sécurisée afin d'offrir de l'aide, si possible, aux administrateurs du service à la clientèle. (2) À la demande du Canada, le fournisseur doit fournir un document qui décrit le processus d'intervention en cas de fuite d'information du fournisseur.

(iv) **SUPPRIMER l'exigence «O13 du Palier 2», en entier et la REMPLACER par ce qui suit :**

Exigence
Le fournisseur doit démontrer qu'il met en œuvre une confidentialité par conception au cours du cycle de vie du développement de son logiciel, conformément au 'développement sécurisé', tel qu'énoncé ci-dessous : Développement sécurisé (1) Le fournisseur doit mettre en œuvre un cycle de vie de développement de logiciels et de systèmes qui applique les principes d'ingénierie de la sécurité des systèmes d'information tout au long de leur cycle de vie et dans le développement de logiciels, de sites Web et de services. Ce cycle de vie doit être conforme aux normes et aux pratiques exemplaires du secteur, comme : (i) NIST; (ii) ISO 27034; (iii) ITSG-33; (iv) Safecode; (v) Open Web Application Security Project (OWASP) (p. ex. Application Security Verification Standard [ASVS] ou une norme équivalente approuvée par le Canada par écrit). (2) À la demande du Canada, le fournisseur doit fournir un document qui décrit le logiciel documenté de l'entrepreneur, ainsi que l'approche et le processus adoptés relativement au cycle de vie du développement du système.

(v) **SUPPRIMER la «section 5» de l'annexe B, Obligations en matière de sécurité et protection de la vie privée, en entier et la REMPLACER par ce qui suit :**

5. Vérification de la conformité

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

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

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

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

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

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

(vi) **SUPPRIMER la «section 7» de l'annexe B, Obligations en matière de sécurité et protection de la vie privée, en entier et la REMPLACER par ce qui suit :**

7. Sécurité des réseaux et des communications

Le fournisseur doit :

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

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

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

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

(vii) **SUPPRIMER Nécessaire pour démontrer la conformité au palier 2 « O9 » en entier et la REMPLACER par ce qui suit :**

Nécessaire pour démontrer la conformité au palier 2
Le fournisseur doit démontrer la conformité aux exigences de sécurité sélectionnées dans le Profil de contrôle de sécurité du GC pour les services infonuagiques de TI du GC disponibles (https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/services-informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html) pour la portée des Services fournis par le fournisseur dans le cadre du Programme d'évaluation de la sécurité des TI en vertu de la section 4 intitulée « Programme d'évaluation de la sécurité informatique du fournisseur de services en nuage» de l'annexe B - Obligations en matière de sécurité et protection de la vie privée. La conformité doit être démontrée par la mise en correspondance des contrôles de sécurité avec les certifications applicables de l'industrie indiquées ci-dessous, et validée au moyen d'évaluations par des tiers indépendants. La cartographie des contrôles de sécurité doit être incluse; Profil de contrôle de sécurité du GC pour les services de TI du GC en nuage et Certification de l'industrie dans le cadre d'une assurance par un tiers détaillée au palier 2 O8.

B. ANNEXE F – CLAUSES DU CONTRAT SUBSÉQUENT

(i) **SUPPRIMER le «paragraphe c) de la section 4.1, Services de la solution», en entier et le REMPLACER par ce qui suit :**

c) « **Indemnisation :** Si quelqu'un allègue que, en raison de l'accès du Canada à des services de solution SaaS ou de leur utilisation par le Canada, ce dernier porte atteinte aux droits de propriété intellectuelle, le Canada avisera rapidement le fournisseur par écrit de cette réclamation. Dans ces circonstances, ou si quelqu'un allègue que le fournisseur porte atteinte aux droits de propriété intellectuelle associés à la solution SaaS de ce contrat :

1. le fournisseur doit immédiatement prendre l'une des mesures suivantes :

   a) prendre toutes les mesures nécessaires pour acquérir les droits et être en mesure de continuer d'offrir les services de la solution au Canada, conformément au contrat;

   b) modifier ou remplacer la partie qui porte prétendument atteinte ou la totalité de la solution SaaS, et continuer à fournir les services de la solution au Canada, conformément au contrat;

c) si les options ci-dessus ne sont pas viables, fournir un préavis écrit au sujet de la réclamation au Canada et proposer une solution SaaS « de rechange » aux termes de services d'une solution nouvelle ou provisoire, conformément au contrat; fournir les services de la solution nouvelle ou provisoire au même prix que les services de la solution concernée, et ce, pour la durée du contrat, indépendamment du prix commercial du fournisseur pour la solution SaaS de rechange ou de la plus grande fonctionnalité de la solution SaaS de rechange; et, à la demande du Canada, fournir de la formation sans frais supplémentaires sur l'utilisation de la solution SaaS de rechange;

d) fournir un préavis écrit au Canada afin de l'informer de la résiliation du contrat, y compris le nom du requérant, la nature de la réclamation, le rôle présumé du fournisseur dans la violation alléguée relative à la solution SaaS et une confirmation de l'incapacité du fournisseur à continuer à fournir les services de la solution au Canada conformément au contrat. Pour permettre cette résiliation, le fournisseur doit fournir au Canada un accès accru à toute donnée du gouvernement du Canada utilisée ou conservée par l'entremise de la solution SaaS à des fins de récupération ou de migration, et rembourser entièrement toute partie du prix contractuel que le Canada a déjà versée au cours des 12 derniers mois, ou à partir de la date de la violation, selon le moment qui survient en premier.

Si le fournisseur omet de se conformer à la présente section dans un délai raisonnable, le fournisseur convient de rembourser le Canada pour tous les coûts que ce dernier peut avoir déboursés pour régler la réclamation pour violation, y compris l'approvisionnement de services d'une nouvelle solution. »

(ii) **SUPPRIMER la section «5.6, Pas d'infraction», en entier et la REMPLACER par ce qui suit :**

« L'entrepreneur garantit **qu'à sa connaissance,** rien dans la solution, ou dans l'utilisation de la solution par le Canada, ne **constitue ou** ne constituera une appropriation illicite de la propriété intellectuelle ou des autres droits d'un tiers ni ne les enfreindra. »

(iii) **SUPPRIMER la section «1, Audit de conformité», de l'appendice D Obligations en matière de protection de la vie privée en entier.**

(iv) **SUPPRIMER la section 7.5, « Droit de résiliation», en entier et la REMPLACER par ce qui suit :**

7.5 « Droits et recours

7.5.1 Les droits sont cumulatifs

Tous les droits et recours prévus dans le contrat ou par la loi sont cumulatifs et non exclusifs.

7.5.2 Résiliation pour manquement

a) **Avis de manquement.** L'autorité contractante peut transmettre à l'entrepreneur un avis écrit de résiliation pour manquement de tout ou partie du contrat. L'avis indiquera la violation, les circonstances pertinentes, le délai proposé, les travaux ou les services touchés (en cas de résiliation partielle), les exigences relatives à un plan d'action, les services de transition ou de migration nécessaires, et la date effective de la résiliation. L'avis indiquera également si le Canada conserve d'autres réclamations de dommages-intérêts.

b) **Conformité du fournisseur.** L'entrepreneur doit respecter les exigences en matière d'assurance prévues dans l'avis.

c) **Violation totale.** Si, de l'avis raisonnable du Canada, le manquement de l'entrepreneur est une violation totale ou substantielle du contrat, le Canada peut immédiatement résilier le contrat au moyen d'un préavis. Par souci de clarté, l'avis du Canada peut être fondé sur les circonstances, y compris, sans toutefois s'y limiter :

i. le non-respect d'une obligation contractuelle substantielle par l'entrepreneur;

ii. le fait que l'entrepreneur semble irréfutablement ne pas être en mesure de respecter une obligation contractuelle substantielle en raison de facteur hors de son contrôle, ce qui inclut une insolvabilité réelle ou apparente, l'omission répétée de produire des produits livrables acceptables en vertu du présent contrat ou de contrats similaires avec le Canada;

iii. des violations non corrigées multiples ou répétées d'une obligation contractuelle intermédiaire par l'entrepreneur;

iv. un manquement de l'entrepreneur qui a des répercussions négatives sur les activités du gouvernement.

d) **Autre manquement**

i. Si les manquements de l'entrepreneur ne sont pas des violations totales, le Canada déterminera le délai dans lequel l'entrepreneur doit corriger le manquement et peut exiger un plan d'action.

ii. Si, en réponse à l'avis, l'entrepreneur indique son incapacité ou son manque de volonté à corriger le manquement, le Canada peut résilier le contrat pour manquement immédiatement.

iii. Si le contrat (y compris les autorisations de tâches individuelles) précise qu'un manquement particulier ne permettra aucun délai, le Canada peut résilier le contrat pour manquement immédiatement sans fournir la possibilité de corriger le manquement.

e) Le Canada n'est pas tenu d'aviser l'entrepreneur des manquements. Les parties conviennent que le Canada peut choisir de ne pas utiliser de processus de préavis officiel ou de prolonger le délai imparti à l'entrepreneur, et que cela pourra considérer comme une renonciation de la part du Canada à certains droits ou une acceptation du manquement de l'entrepreneur par le Canada.

f) Si le Canada résilie le contrat pour manquement, le Canada ne paiera que pour les travaux ou services complétés livrés et acceptés avant la date de la résiliation. Le Canada ne paiera aucun montant qui dépasse la valeur des travaux ou services acceptés.

7.5.3 Résiliation pour raisons de commodité

a) **Avis de résiliation.** L'autorité contractante peut transmettre au fournisseur un avis écrit de résiliation pour raisons de commodité de tout le contrat ou d'une partie du contrat. L'avis indiquera la violation, la date effective de la résiliation, les travaux ou les services touchés (en cas de résiliation partielle), et les services de transition ou de migration nécessaires. L'entrepreneur doit se conformer aux exigences prévues par l'avis, y compris continuer à effectuer ou à livrer des services ou des travaux qui ne sont pas touchés par la résiliation.

b) L'entrepreneur convient de rembourser immédiatement au Canada la portion de toute avance non liquidée à la date de la résiliation.

c) Si, en vertu du paragraphe a), le Canada résilie :

a. **les travaux,** le Canada paiera à l'entrepreneur les coûts raisonnables liés à la résiliation des travaux engagés par l'entrepreneur, excluant particulièrement les coûts liés à la cessation d'emploi d'employés, à moins que l'entrepreneur établissent que ces coûts découlent d'obligations légales;

b. **les services,**

i. pour les services d'abonnement payés par avance chaque mois, le Canada renoncera à son droit de réclamer la partie non liquidée d'une avance à la date de la résiliation; et

ii. pour les services d'abonnement annuel, ou comportant des périodes contractuelles définies, et incluant des paiements annuels faits par avance, le Canada renoncera à son droit de réclamer la partie d'une avance qui n'est pas liquidée le dernier jour du mois suivant la date de la résiliation,

d) Les parties conviennent que ces montants représentent une estimation authentique des dommages liquidés qu'encourrait l'entrepreneur en raison d'une résiliation précoce du contrat, et qu'il ne s'agit pas d'une pénalité.

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