DEMANDE DE SOUMISSIONS POUR LE CONTRAT CONCLU DANS LE CADRE DE L'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (AMA) POUR DES SERVICES PROFESSIONNELS EN INFORMATIQUE CENTRÉS SUR LES TÂCHES (SPICT) PLUSIEURS CATÉGORIES DE RESSOURCES – NIVEAU 2 & 3 POUR VOLET 6 : SERVICES DE CYBER PROTECTION POUR L'AGENCE DES SERVICES FRONTALIERS DU CANADA

Table des matières

Liste des annexes du contrat subséquent :

Annexe A Énoncé des travaux
Appendice A de l'annexe A- Procédures d'attribution de tâches,
Appendice B de l'annexe A– Formulaire d'autorisation de tâches,
Appendice C de l'annexe A– Critères d'évaluation des ressources et tableau de réponses,
Appendice D de l'annexe A Attestations à l'étape de l'autorisation de tâches;

Annexe A1 : Glossaire

Annexe B Base de paiement

Annexe C Liste de vérification des exigences relatives à la sécurité
Annex C1 Guide de classification de Sécurité

Liste des pièces jointes à la Partie 1
Piece jointe 1.1: Sommaire des changements de 47419-214911/A

Liste des pièces jointes à la Partie 3 (Instructions pour la préparation des soumissions)
- Pièce jointe 3.1 : Formulaire de présentation de la soumission
- Pièce jointe 3.2 : Instruments de paiement électronique

Liste des pièces jointes à la Partie 4 (Procédures d'évaluation et méthode de sélection)
- Pièce jointe 4.1 : Critères techniques obligatoires
- Pièce jointe 4.2 : Critères techniques cotés
- Pièce jointe 4.3 : Formulaires de réponse des soumissionnaires aux critères corporatifs obligatoires
- Pièce jointe 4.4 : Barème de prix

Liste des pièces jointes à la Partie 5 (Attestations)
Pièce jointe 5.1 Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation

DEMANDE DE SOUMISSIONS POUR LE CONTRAT CONCLU DANS LE CADRE DE L'ARRANGEMENT EN MATIÈRE D'APPROVISIONNEMENT (AMA) POUR DES SERVICES PROFESSIONNELS EN INFORMATIQUE CENTRÉS SUR LES TÂCHES (SPICT) PLUSIEURS CATÉGORIES DE RESSOURCES – NIVEAU 2 & 3 POUR VOLET 6 : SERVICES DE CYBER PROTECTION) POUR L'AGENCE DES SERVICES FRONTALIERS DU CANADA

PARTIE 1 – RENSEIGNEMENTS GÉNÉRAUX

1.1 Introduction

Dans le présent document, on énumère les modalités qui s'appliquent à la demande de soumissions. Le document contient sept parties, ainsi que des annexes et des pièces jointes, comme suit :

Partie 1 Renseignements généraux : Renferme une description générale du besoin.

Partie 2 Instructions à l'intention des soumissionnaires : renferme les instructions, les clauses et les 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 il faut satisfaire dans la soumission, s'il y a lieu, ainsi que la méthode de sélection.

Partie 5 Attestations et renseignements supplémentaires : renferme les attestations et les renseignements supplémentaires à fournir.

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

Partie 7 Clauses du contrat subséquent : contient les clauses et les conditions qui s'appliqueront à tout contrat subséquent.

Les annexes comprennent l'énoncé des travaux, la Base de Paiement, les Exigences relatives à la sécurité et toute autre annexe.

1.2 Sommaire

a. Cette demande de soumission annule et remplace la demande de soumissions numéro 47419-214911/A daté du 7 mai 2021 ayant comme date de clôture le 27 mai 2021; ce document remplace entièrement la version antérieure. Un sommaire des changement est fourni dans la piece jointe 1.1

b. La présente demande de soumissions vise à répondre au besoin de L`Agence des Services Frontaliers du Canada (le « client ») en matière de SPICT dans le cadre de l'AMA pour des SPICT.

c. Elle vise l'attribution de un (1) contrat de une (1) année comprenant 2 options irrévocables d'une année chacune, qui permettent au Canada de prolonger la durée du contrat.

d. Ce besoin comporte des exigences relatives à la sécurité. Pour de plus amples renseignements, consulter la Partie 6, Exigences relatives à la sécurité, exigences financières et autres exigences, et la Partie 7, Clauses du contrat subséquent. Pour en savoir plus sur le filtrage de sécurité du personnel et de l'organisation ainsi que sur les clauses de sécurité, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de TPSGC (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

e. Ce besoin est assujetti aux dispositions de l'Accord sur les marchés publics de l'Organisation mondiale du commerce, de l'Accord de libre-échange Canada-Chili, de l'Accord de libre-échange entre le Canada et le Pérou, de l'Accord de libre-échange Canada-Colombie, de l'Accord de libre-échange Canada-Panama, de l'Accord économique et commercial global entre le Canada et l'Union européenne (AECG), de l'Accord de partenariat transpacifique global et progressiste (APTGP), de l'Accord de libre-échange canadien (ALEC), de l'Accord de libre-échange Canada-Ukraine, de l'Accord de continuité commerciale Canada-Royaume-Uni (ACC Canada-Royaume-Uni). et de l'Accord de libre-échange Canada-Corée.

f. Le Programme de contrats fédéraux pour l'équité en matière d'emploi s'applique au présent besoin; voir la Partie 5 – Attestations et renseignements supplémentaires, la Partie 7 – Clauses du contrat subséquent, et la pièce jointe intitulée « Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation ».

g. La présente demande de soumissions concerne l'attribution d'un contrat comportant des autorisations de tâches pour la livraison du besoin décrit dans les présentes, et ce, partout au Canada, 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 qui sont. Les produits à livrer dans les zones visées par des ERTG au Yukon, dans les Territoires du Nord-Ouest, au Nunavut, au Québec ou au Labrador devront faire l'objet de marchés distincts, attribués en dehors des contrats subséquents.

h. Les soumissionnaires doivent 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 la partie 3, « Instructions pour la préparation des soumissions », de la demande de soumissions, pour obtenir de plus amples renseignements.

i. Seuls les titulaires d'AMA pour des SPICT qui détiennent un AMA pour des SPICT au palier 2, au moment de la clôture des soumissions, dans toutes les catégories de ressources requises dans cet appel d'offres et dans la région de la Capitale Nationale avec un autorisation de sécurité du fournisseur au niveau secret dans le cadre de la série d'AMA nº EN578-170432 peuvent soumissionner. L'AMA pour des SPICT nº EN578-170432 est incorporé par renvoi et fait partie de la présente demande de soumissions, comme s'il y était formellement reproduit, et est assujetti aux conditions contenues dans la présente demande de soumissions. Les conditions en lettres majuscules qui ne sont pas définies dans la présente demande de soumissions ont le sens qui leur a été donné dans l'AMA pour les SPICT.

j. Les titulaires d'AMA invités à soumissionner à titre de coentreprise doivent présenter une soumission à ce titre et ne doivent pas former une autre coentreprise pour soumissionner. Toute coentreprise doit déjà avoir été sélectionnée dans le cadre de l'AMA nº EN578-055605 au moment de la clôture des soumissions pour pouvoir présenter une soumission.

k. Pour chaque volet de travail, les catégories de ressources énumérées ci-dessous doivent être fournies sur demande, conformément à l'annexe A de l'AMA pour des SPICT.

Categorie de Resources	Niveau d'expertise	Nombre estimatif de ressoucres requises
Volet 6 : Services de Cyber Protection de SPICT		
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	2	1
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	3	1
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	2	1
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	3	1
C.7 Spécialiste en conception de sécurité des technologies de l'information	2	2
C.7 Spécialiste en conception de sécurité des technologies de l'information	3	2
C.8 Analyste de la sécurité des réseaux	2	1
C.8 Analyste de la sécurité des réseaux	3	1
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	2	2
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	3	1
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2	1
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	3	1
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2	1
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	3	3
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2	1
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	3	1

1.3 Compte rendu

Les soumissionnaires peuvent demander un compte rendu des résultats du processus de demande de soumissions. Ils doivent 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.

PARTIE 2 – INSTRUCTIONS À L'INTENTION DES SOUMISSIONNAIRES

2.1 Instructions, clauses et conditions uniformisées

(a) Toutes les instructions, clauses et conditions indiquées 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 Travaux publics et Services gouvernementaux Canada (TPSGC).

(b) 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 ou des contrats subséquents.

(c) Le document 2003 (2020-05-28), Instructions uniformisées – biens ou services – besoins concurrentiels, est intégré par renvoi dans la demande de soumissions et en fait partie intégrante. En cas de contradiction entre les dispositions du document 2003 et celles du présent document, ce sont les dispositions de ce dernier qui prévalent.

(d) Le paragraphe 3.a. de l'article 01 « Dispositions relatives à l'intégrité – soumission » des instructions uniformisées 2003, incorporées par renvoi ci-dessus, 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,

(e) Le paragraphe 4 de l'article 05 « Présentation des soumissions » des instructions uniformisées 2003, incorporées par renvoi ci-dessus, est modifié comme suit :

Supprimer : 60 jours

Insérer : 180 jours

(f) Le paragraphe 1 de l'article 08 « Transmission par télécopieur ou par le service Connexion postel » des instructions uniformisées 2003, incorporées par renvoi ci-dessus, est entièrement supprimé et remplacé par ce qui suit :

1. Télécopieur

En raison de la nature de la présente demande de soumissions, TPSGC n'acceptera pas les soumissions qui lui sont transmises par télécopieur ou par courrier électronique.

2.2 Présentation des soumissions

(a) Les soumissions doivent être présentées uniquement à l'Unité de réception des soumissions de Travaux publics et Services gouvernementaux Canada (TPSGC) **par l'entremise du service Connexion postel** au plus tard à la date et à l'heure indiquées sur la page 1 de la demande de soumissions.

Remarque : Pour les soumissionnaires qui doivent s'inscrire au service Connexion postel, l'adresse courriel à utiliser est :

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

Les soumissionnaires intéressés doivent s'inscrire quelques jours avant la date de clôture de la demande de soumissions.

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

(b) En raison de la nature de la présente demande de soumissions, TPSGC n'acceptera pas les soumissions qui lui sont transmises par télécopieur ou par courrier électronique.

2.3 Demandes de renseignements en période de soumission

(a) Toutes les demandes de renseignements doivent être présentées par écrit à l'autorité contractante au plus tard 10 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.

(b) Les soumissionnaires doivent indiquer aussi fidèlement que 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 de 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 Ancien fonctionnaire

(a) Les contrats attribués à d'anciens fonctionnaires qui touchent une pension ou qui ont reçu un paiement forfaitaire doivent résister à l'examen scrupuleux du public et constituer une dépense équitable des fonds publics. Afin de respecter les politiques et les directives du Conseil du Trésor sur les contrats attribués à d'anciens fonctionnaires, les soumissionnaires doivent fournir l'information exigée ci-dessous avant l'attribution du contrat. Si les réponses aux questions et, s'il y a lieu, les renseignements requis, n'ont pas été fournis à la date de fin de l'évaluation des soumissions, le Canada informera le soumissionnaire du délai à l'intérieur duquel l'information doit être fournie. Le défaut de se conformer à la demande du Canada et de satisfaire à l'exigence dans le délai prescrit rendra la soumission non recevable.

(b) Définitions

Aux fins de cette clause, « *ancien fonctionnaire* » signifie tout ancien employé d'un ministère au sens de la *Loi sur la gestion des finances publiques*, L.R., 1985, ch. F-11, un ancien membre des Forces canadiennes ou un ancien membre de la Gendarmerie royale du Canada. Un ancien fonctionnaire peut être :

(i) un individu;

(ii) un particulier qui s'est incorporé;

(iii) une société de personnes constituée d'anciens fonctionnaires;

(iv) une entreprise à propriétaire unique ou une entité dans laquelle la personne visée détient un intérêt important ou majoritaire.

Le terme « *période du paiement forfaitaire* » signifie la période mesurée en semaines de salaire à l'égard de laquelle un paiement a été fait pour faciliter la transition vers la retraite ou vers un autre emploi par suite de la mise en place de divers programmes visant à réduire la taille de la fonction publique. La période du paiement forfaitaire ne comprend pas la période visée par l'indemnité de cessation d'emploi, qui se mesure de façon similaire.

Le terme « *pension* » signifie une pension ou une allocation annuelle versée en vertu de la *Loi sur la pension de la fonction publique* (LPFP), L.R.C., 1985, ch. P-36, et toute augmentation versée en vertu de la *Loi sur les prestations de retraite supplémentaires*, L.R., 1985, ch. S-24, dans la mesure où elle touche la LPFP. La pension ne comprend pas les pensions payables conformément à la *Loi sur la pension de retraite des Forces canadiennes*, L.R., 1985, ch. C-17; à la *Loi sur la continuation de la pension des services de défense*, 1970, ch. D-3; à la *Loi sur la continuation des pensions de la Gendarmerie royale du Canada*, 1970, ch. R-10; à la *Loi sur la pension de retraite de la Gendarmerie royale du Canada*, L.R., 1985, ch. R-11; à la *Loi sur les allocations de retraite des parlementaires*, L.R., 1985, ch. M-5; et à la partie de la pension versée conformément à la *Loi sur le Régime de pensions du Canada*, L.R., 1985, ch. C-8.

(c) Ancien fonctionnaire touchant une pension

Selon les définitions ci-dessus, le soumissionnaire est-il un ancien fonctionnaire touchant une pension? **Oui** ( ) **Non** ( )

Si oui, le soumissionnaire doit fournir les renseignements suivants pour tous les anciens fonctionnaires touchant une pension, le cas échéant :

(i) le nom de l'ancien fonctionnaire;

(ii) la date de cessation d'emploi ou de retraite de la fonction publique.

En fournissant cette information, les soumissionnaires acceptent que le statut du soumissionnaire retenu, en tant qu'ancien fonctionnaire touchant une pension, soit publié dans les rapports de divulgation proactive des contrats, sur les sites Web des ministères, et ce, conformément à l'Avis sur la Politique des marchés : 2012-2 et aux Lignes directrices sur la divulgation proactive des marchés.

(d) Directive sur le réaménagement des effectifs

Le soumissionnaire est-il un ancien fonctionnaire qui a reçu un paiement forfaitaire conformément aux modalités de la Directive sur le réaménagement des effectifs? **Oui** ( ) **Non** ( )

Si oui, le soumissionnaire doit fournir l'information suivante :

(i) le nom de l'ancien fonctionnaire;

(ii) les conditions de l'incitatif versé sous forme de paiement forfaitaire;

(iii) la date de cessation d'emploi;

(iv) le montant du paiement forfaitaire;

(v) le taux de rémunération qui a servi au calcul du paiement forfaitaire;

(vi) la période correspondant au paiement forfaitaire, incluant la date de début, la date de fin et le nombre de semaines;

(vii) le nombre et le montant (honoraires professionnels) des autres contrats assujettis aux conditions d'un programme de réaménagement des effectifs.

Pour tous les contrats attribués pendant la période du paiement forfaitaire, le montant total des honoraires qui peuvent être payés à un ancien fonctionnaire ayant reçu un paiement forfaitaire est limité à 5 000 $, incluant les taxes applicables.

2.5 Lois applicables

Tout contrat subséquent doit être interprété et régi selon les lois en vigueur en Ontario et les relations entre les parties doivent être déterminées par ces lois *(insérer autre province a l`attribution du contrat si sélectionné par le soumissionaire)*

***Remarque à l'intention des soumissionnaires** : 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 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 effectué, cela signifie que les soumissionnaires acceptent les lois applicables indiquées. Les soumissionnaires doivent indiquer, dans le formulaire de présentation de la soumission, la province ou le territoire canadien de leur choix pour tout contrat subséquent.*

2.6 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 conformément à l'article intitulé « Demandes de renseignements en période de soumission ». Le Canada aura le droit d'accepter ou de rejeter n'importe laquelle ou la totalité des suggestions proposées.

2.7 Fondement du titre du Canada sur les droits de propriété intellectuelle

L`Agence des Services Frontaliers du Canada déterminé que tout droit de propriété intellectuelle découlant de l'exécution des travaux prévus par le contrat subséquent appartiendra au Canada, pour les motifs suivants, tel que défini dans la *Politique sur les droits de propriété intellectuelle issus de marchés conclus avec l'État*

I. les droits de propriété intellectuelle sur les renseignements originaux ne peuvent appartenir à l'entrepreneur en vertu d'une loi, d'un règlement, ou d'une obligation antérieure contractée par Canada envers un ou des tiers;

2.8 Données volumétriques

Les données sur le nombre de resources par catégories ont été fournies aux soumissionnaires afin de les aider à préparer leurs soumissions. L'inclusion de ces données dans la présente demande de soumissions ne représente pas un engagement de la part du Canada que son utilisation future des services précisés dans la présente demande de soumissions correspondra à ces données. Elles sont fournies à titre d'information seulement.

2.9 Processus de contestation des offres et mécanismes de recours

(a) Les fournisseurs potentiels ont accès à plusieurs mécanismes pour contester des aspects du processus d'approvisionnement jusqu'à l'attribution du marché, inclusivement.

(b) Le Canada invite les fournisseurs à porter d'abord leurs préoccupations à l'attention de l'autorité contractante. Le site Web du Canada Achats et ventes, sous le titre « Processus de contestation

des soumissions et mécanismes de recours », fournit de l'information sur les organismes de traitement des plaintes possibles, notamment :

(i) Bureau de l'ombudsman de l'approvisionnement (BOA)

(ii) Tribunal canadien du commerce extérieur (TCCE)

(c) Les fournisseurs devraient savoir que des délais stricts sont fixés pour le dépôt des plaintes et qu'ils varient en fonction de l'organisation concernée. Les fournisseurs devraient donc agir rapidement s'ils souhaitent contester un aspect du processus d'approvisionnement.

PARTIE 3 – INSTRUCTIONS POUR LA PRÉPARATION DES SOUMISSIONS

3.1 Instructions pour la préparation des soumissions

(a) **Transmission d'une soumission à l'aide du service Connexion postel**

a. Le Canada demande au soumissionnaire de présenter sa soumission électronique conformément à la section 08 des Instructions uniformisées 2003. Le système Connexion postel a une limite de 1 Go par message individuel affiché et une limite de 20 Go par conversation.

b. La soumission doit être présentée en sections distinctes, comme suit :

i. Section I : Soumission technique

ii. Section II : Soumission financière

iii. Section III : Attestations

iv. Section IV : Renseignements supplémentaires

c. Pour obtenir de plus amples renseignements, veuillez consulter la section 08 « Transmission par télécopieur ou par le service Connexion postel » à https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat/1/2003/23#transmission-par-telecopieurs une autre section de la soumission.

(b) Les prix doivent figurer dans la soumission financière seulement. Aucun prix ne doit être indiqué dans la soumission.

(c) **Présentation de la soumission** : Le Canada demande que les soumissionnaires suivent les instructions de présentation décrites ci-après pour préparer leur soumission :

(i) utiliser un format de page de 8,5 po sur 11 po (216 mm sur 279 mm);

(ii) utiliser un système de numérotation correspondant à celui de la demande de soumissions;

(iii) inclure une page titre comprenant le titre, la date, le numéro de l'invitation à soumissionner, le nom et l'adresse du soumissionnaire et les coordonnées de la personne-ressource;

(iv) inclure une table des matières.

(d) **Politique d'achats écologiques du Canada** : En avril 2006, le Canada a publié une politique exigeant des ministères et des organismes fédéraux qu'ils prennent les mesures nécessaires pour tenir compte des facteurs environnementaux dans le processus d'approvisionnement. Voir la Politique d'achats écologiques (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32573). Pour aider le Canada à atteindre ses objectifs, les soumissionnaires devraient :

(e) **Présentation d'une seule soumission** :

(i) Un soumissionnaire et ses entités liées ne peuvent soumettre qu'une seule soumission en réponse à la présente demande de soumissions. Si un soumissionnaire ou ses entités liées participent à plus d'une soumission (participer signifie faire partie du groupe soumissionnaire, et non pas être un sous-traitant), le Canada donnera deux jours ouvrables à ces soumissionnaires pour indiquer laquelle des soumissions devra être prise en compte par le Canada. À défaut de respecter ce délai, toutes les soumissions visées seront rejetées.

(ii) Aux fins du présent article, peu importe la province ou le territoire où les entités ont été constituées en société ou formées juridiquement (qu'il s'agisse d'une personne physique, d'une personne qui s'est incorporée, d'une société de personnes, d'une société de

personnes à responsabilité limitée, etc.), une entité est considérée comme étant « **liée** » à un soumissionnaire :

(A) s'il s'agit de la même personne morale (c.-à-d. la même personne physique, personne qui s'est incorporée, société de personnes, société de personnes à responsabilité limitée, etc.);

(B) s'il s'agit de « personnes liées » ou de « personnes affiliées » au sens de la *Loi de l'impôt sur le revenu du Canada*;

(C) 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 précédant la date de clôture des soumissions;

(D) si les entités ne sont pas dépendantes l'une de l'autre ou d'un même tiers.

(iii) Les membres individuels d'une coentreprise ne peuvent pas participer à une autre soumission en présentant eux-mêmes une soumission ou en participant à une autre coentreprise.

(i) **Expérience de la coentreprise :**

(i) Lorsque le soumissionnaire est une coentreprise qui possède de l'expérience à ce titre, il peut soumettre l'expérience qu'il a acquise dans le cadre de cette coentreprise.

Exemple : Un soumissionnaire est une coentreprise formée des membres L et O. La demande de soumissions exige que le soumissionnaire possède de l'expérience en prestation de services de maintenance et de dépannage à un client comptant au moins 10 000 utilisateurs pendant 24 mois. En tant que coentreprise (composée de L et O), le soumissionnaire a déjà réalisé ce travail. Il peut donc utiliser cette expérience pour satisfaire à l'exigence. Si le membre L a acquis cette expérience alors qu'il faisait partie d'une coentreprise avec le tiers N, cette expérience ne peut pas être utilisée, car le tiers N ne fait pas partie de la coentreprise soumissionnaire.

(ii) Une coentreprise qui présente une soumission peut évoquer l'expérience de l'un de ses membres pour démontrer qu'elle satisfait à tout critère technique de la présente demande de soumissions.

Exemple : Un soumissionnaire est membre d'une coentreprise composée de X, Y et Z. Si une demande de soumissions exige : (a) que le soumissionnaire ait trois ans d'expérience de la prestation de services de maintenance, et (b) que le soumissionnaire ait deux ans d'expérience de l'intégration de matériel à des réseaux complexes, chacune de ces deux exigences peut être satisfaite par un membre différent de la coentreprise. Cependant, pour un critère donné, par exemple celui qui concerne l'expérience de trois ans de la prestation de services de maintenance, le soumissionnaire ne peut pas indiquer que chaque membre, soit X, Y et Z, a un an d'expérience pour un total de trois ans. Une telle réponse serait déclarée non conforme.

(iii) Les membres de la coentreprise ne peuvent cependant pas mettre en commun leurs capacités pour répondre à un critère technique donné de la présente demande de soumissions. Un membre de la coentreprise peut néanmoins mettre sa propre expérience en commun avec celle de la coentreprise. Chaque fois qu'il doit faire la preuve qu'il répond à un critère, le soumissionnaire doit indiquer quel membre de la coentreprise y répond. Si le soumissionnaire n'a pas indiqué quel membre de la coentreprise répond à l'exigence, l'autorité contractante lui donnera l'occasion de fournir ce renseignement pendant la période d'évaluation. Si le soumissionnaire ne fournit pas ce renseignement pendant la période fixée par l'autorité contractante, sa soumission sera déclarée non recevable.

Exemple : Un soumissionnaire est membre d'une coentreprise composée de A et B. Si, dans une demande de soumissions, on exige que le soumissionnaire ait de l'expérience dans la prestation de ressources pour un minimum de 100 jours facturables, le soumissionnaire peut démontrer son expérience en présentant ce qui suit :

- les contrats signés par le membre A;
- les contrats signés par le membre B;
- les contrats signés par les membres A et B en tant que coentreprise;
- les contrats signés par le membre A et les contrats signés par les membres A et B en coentreprise;
- les contrats signés par le membre B et les contrats signés par les membres A et B en coentreprise.

Le tout doit totaliser 100 jours facturables.

(iv) Les soumissionnaires qui ont des questions concernant l'évaluation des soumissions présentées par une coentreprise devraient poser leurs questions dans le cadre du processus de demande de renseignements dès que possible durant la période de demande de soumissions.

3.2 Section I : Soumission technique

(a) La soumission technique comprend ce qui suit :

(i) **Formulaire de présentation de la soumission** : Les soumissionnaires devraient joindre le formulaire de présentation de la soumission – pièce jointe 4.1 à leur soumission. Il s'agit d'un formulaire commun dans lequel les soumissionnaires peuvent fournir les renseignements exigés dans le cadre de l'évaluation et de l'attribution du contrat, comme le nom d'une personne-ressource ou le numéro d'entreprise – approvisionnement du soumissionnaire. L'utilisation de ce formulaire pour présenter des renseignements n'est pas obligatoire, mais recommandée. Si le Canada considère que les renseignements requis par le formulaire de présentation de la soumission sont incomplets ou doivent être corrigés, le Canada accordera au soumissionnaire la chance de compléter ou de corriger ces renseignements.

(ii) **Justification de la conformité technique** :

(A) **Critères techniques obligatoires** : Dans sa soumission technique, le soumissionnaire doit prouver qu'il s'est conformé aux articles de la pièce jointe 4.1, qui constitue le format demandé pour fournir la justification. La justification ne doit pas être une simple répétition du besoin, mais doit expliquer et démontrer la façon dont le soumissionnaire satisfera aux exigences et exécutera les travaux exigés. Il ne suffit pas de déclarer simplement que la solution ou les ressources proposées sont conformes. Lorsque le Canada détermine que la justification n'est pas complète, la soumission sera jugée non conforme et sera rejetée. La justification peut mentionner des documents supplémentaires joints à la soumission. Cette information peut être mentionnée dans la colonne « Réponse du soumissionnaire » de la pièce jointe 4.1, où les soumissionnaires doivent indiquer l'endroit précis où se trouvent les documents de référence, y compris le titre du document et les numéros de page et d'alinéa. Lorsque la référence n'est pas suffisamment précise, le Canada peut demander que le soumissionnaire dirige le Canada vers l'endroit approprié dans le document.

(B) **Critères techniques cotés :** Dans sa soumission technique, le soumissionnaire doit prouver qu'il s'est conformé aux articles de la pièce jointe 4.2, qui constitue le format demandé pour fournir la justification. La justification ne doit pas être une simple répétition du besoin, mais doit expliquer et démontrer la façon dont le soumissionnaire satisfera aux exigences et exécutera les travaux exigés. Il ne suffit pas de déclarer simplement que la solution ou les ressources proposées

sont conformes. Lorsque le Canada détermine que la justification n'est pas complète, la soumission sera cotée en conséquence. La justification peut mentionner des documents supplémentaires joints à la soumission. Cette information peut être mentionnée dans la colonne « Réponse du soumissionnaire » de la pièce jointe 4.2, où les soumissionnaires doivent indiquer l'endroit précis où se trouvent les documents de référence, y compris le titre du document et les numéros de page et d'alinéa. Lorsque la référence n'est pas suffisamment précise, le Canada peut demander que le soumissionnaire dirige le Canada vers l'endroit approprié dans le document.

(C) Evaluation de l'expérience de l'entreprise (EO1 et EC5) :
Dans l'évaluation de l'expérience de l'entreprise (EO1 et EC5), le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire qui est :

a. la propre expérience d'entreprise du soumissionnaire (y compris l'expérience d'un ou plusieurs membres d'une entreprise commune soumissionnaire);
b. l'expérience d'une société mère ou de personnes qui détient le contrôle du soumissionnaire;
c. l'expérience d'une filiale contrôlée par le soumissionnaire;
d. l'expérience d'une société contrôlée par la même société mère ou la même société de personnes qui contrôle le soumissionnaire, lorsque le contrôle signifie que l'entité détenant le contrôle possède une participation suffisante dans l'entité contrôlée pour avoir le droit de nommer ou d'élire la majorité des membres du conseil d'administration.

Si le soumissionnaire s'est appuyé sur l'expérience de l'une des entités énumérées en (b), (c) ou (d), il doit, sur demande, fournir au gouvernement du Canada des documents démontrant sa relation avec l'entité. TPSGC ne considérera pas qu'une entité possède une expérience d'entreprise si l'expérience revendiquée résulte de l'acquisition des actifs d'une autre entité.

Si le soumissionnaire s'est appuyé sur l'expérience de l'une des entités énumérées aux points (b), (c) ou (d), il devra, au moment de l'attribution du contrat, fournir, à la demande du gouvernement du Canada, la garantie de cette entité pour l'exécution du contrat qui en résultera. Si le soumissionnaire ne peut fournir cette garantie dans les deux semaines suivant l'annonce de sa recommandation pour l'attribution du contrat, le gouvernement du Canada sera en droit de rejeter sa soumission.

(iii) **Coordonnées de clients cités en référence** :

A. Lorsque le Canada évalue les soumissions, il peut, sans toutefois y être obligé, demander qu'un soumissionnaire fournisse des références de clients. Si le Canada envoie une demande écrite à cet égard, le soumissionnaire aura deux jours ouvrables pour fournir les renseignements requis au Canada. Si le soumissionnaire ne respecte pas ce délai, sa soumission sera déclarée non recevable. Ces références de clients doivent toutes confirmer, lorsque TPSGC le demande, les faits énoncés dans la soumission du soumissionnaire, comme il est requis à la pièce jointe 4.1 et 4.2.

B. La question visant à obtenir la confirmation des clients cités en référence devrait être construite de la façon suivante :

Pour les criteres EO1, EO2, EC1, EC2, EC3, EC5

[Nom du soumissionnaire] a-t-il fourni des services de [décrire les services et, le cas échéant, les délais dans lesquels ces services ont dû être fournis] à votre organisation? »

___ Oui, le soumissionnaire a fourni à mon organisation les services décrits ci-dessus.

___ Non, le soumissionnaire n'a pas fourni à mon organisation les services décrits ci-dessus.

___ Je ne veux pas ou ne peux pas fournir de renseignements au sujet des services décrits ci-dessus.

C. Pour chaque client cité en référence, le soumissionnaire doit, au minimum, fournir le nom ainsi que le numéro de téléphone ou l'adresse courriel d'une personne-ressource. Si seul le numéro de téléphone est fourni, il sera utilisé pour demander l'adresse de courriel, et la vérification des références se fera par courriel.

Le soumissionnaire doit en outre indiquer le titre de la personne-ressource. Il incombe au soumissionnaire de s'assurer que la personne-ressource qu'il propose est au fait des services qu'il a offerts et qu'elle accepte d'être citée en référence. Des références de l'État seront acceptées.

3.3 Section II : Soumission financière

(a) **Prix** : Les soumissionnaires doivent présenter leur soumission financière conformément au barème de prix fourni à la pièce jointe 4.4. Le montant total des taxes applicables doit être indiqué séparément, s'il y a lieu. À moins d'indication contraire, les soumissionnaires doivent inscrire un seul taux quotidien ferme, tout compris, en dollars canadiens, dans chacune des cellules nécessitant une inscription dans les tableaux des prix.

(b) **Variation des taux pour les ressources par période** : Pour une catégorie de ressources donnée, lorsque les tableaux financiers fournis par le Canada permettent d'établir des taux fermes différents associés à une catégorie de ressources pour des périodes différentes :

(i) le taux présenté dans la soumission ne doit pas augmenter de plus de 5 % d'une période à une autre;

(ii) le taux présenté dans la soumission pour une même catégorie de ressources pour toute période subséquente ne doit pas être inférieur au taux présenté dans la soumission pour la période comprenant le premier mois de la période initiale du contrat.

(c) **Variation des taux pour les ressources par niveau :** Lorsque les tableaux financiers fournis par le Canada permettent d'établir des taux fermes différents associés à différents niveaux d'expérience dans une même catégorie de ressource et pour la même période, pour cette catégorie de ressource et cette période :

(i) le taux soumis pour le niveau trois doit être égale à celui soumis pour le niveau deux ou supérieur à celui-ci;

(ii) le taux soumis pour le niveau deux doit être égale à celui soumis pour le niveau un ou supérieur à celui-ci.

(d) **Tous les coûts doivent être compris** : La soumission financière doit indiquer tous les coûts relatifs au besoin décrit dans la présente demande de soumissions pour toute la durée du contrat, y compris toute année d'option. Il incombe entièrement au soumissionnaire d'indiquer tout le matériel, les logiciels, les périphériques, le câblage et les composants nécessaires pour satisfaire aux exigences de la présente demande de soumissions, ainsi que les prix de ces articles.

(e) **Prix nuls** : On demande aux soumissionnaires d'entrer « 0,00 $ » pour tout article qu'il ne compte pas facturer ou qui a déjà été ajouté à d'autres prix dans le tableau. Si le soumissionnaire

laisse le champ vide, le Canada considérera que le prix se chiffre à « 0,00 $ » aux fins d'évaluation et pourrait demander au soumissionnaire de confirmer que le prix est bel et bien de « 0,00 $ ». Aucun soumissionnaire ne sera autorisé à ajouter ou à modifier un prix lors de cette confirmation. Si le soumissionnaire refuse de confirmer que le prix d'un article dont le champ est vide est de 0,00 $, sa soumission sera déclarée non recevable.

Remarque à l'intention des soumissionnaires : *Si le Canada reçoit 4 soumissions ou moins* [*le même nombre de soumissions indiqué à l'intitulé « Processus de conformité des soumissions en phases »*] *à la date de clôture de la demande de soumissions, le sous-article précédent « Prix nuls » ne s'appliquera pas.*

(f) **Paiement électronique de factures – soumission** : Si vous êtes disposés à accepter le paiement de factures au moyen d'instruments de paiement électronique, compléter la pièce jointe 3.2 : Instruments de paiement électronique, afin d'identifier lesquels sont acceptés. Si la pièce jointe 3.2 : 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.

3.4 Section III : Attestations

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

PARTIE 4 – PROCÉDURES D'ÉVALUATION ET MÉTHODE DE SÉLECTION

4.1 Procédures d'évaluation

(a) Les soumissions reçues seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, y compris les critères d'évaluation techniques et financiers. Le processus d'évaluation comporte plusieurs étapes, lesquelles sont décrites ci-dessous. Même si l'évaluation et la sélection seront effectuées par étape, le fait que le Canada soit passé à une étape ultérieure ne signifie pas que ce dernier a irréfutablement déterminé que le soumissionnaire a réussi toutes les étapes précédentes. Le Canada se réserve le droit d'exécuter parallèlement certaines étapes de l'évaluation.

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

(c) En plus de tout autre délai établi dans la demande de soumissions :

(i) **Demandes de précisions** : Si le Canada demande des précisions au soumissionnaire au sujet de sa soumission ou s'il veut vérifier celle-ci, le soumissionnaire disposera d'un délai de deux jours ouvrables (ou d'un délai plus long précisé par écrit par l'autorité contractante) pour fournir les renseignements nécessaires au Canada. Si le soumissionnaire ne respecte pas ce délai, sa soumission sera déclarée non recevable.

(ii) **Demandes de renseignements supplémentaires** : Si le Canada demande d'autres renseignements pour l'une des raisons qui suivent (selon la section intitulée « Déroulement de l'évaluation » du document 2003 Instructions uniformisées – biens ou services – besoins concurrentiels).

(A) vérifier tout renseignement fourni par le soumissionnaire dans sa soumission;

(B) communiquer avec une ou plusieurs des références citées par le soumissionnaire (références citées dans les curriculum vitæ des ressources individuelles) dans le but de valider les renseignements fournis par le soumissionnaire,

le soumissionnaire doit fournir les renseignements demandés par le Canada dans les 2 jours ouvrables suivant la demande de l'autorité contractante.

(iii) **Prolongation du délai** : Si le soumissionnaire a besoin de davantage de temps, l'autorité contractante, à sa seule discrétion, peut accorder une prolongation du délai.

4.1.1 Processus de conformité des soumissions en phases

4.1.1.1 Généralités

(a) Le Canada appliquera le processus de conformité des soumissions en phases (PCSP) décrit ci-dessous pour ce besoin SEULEMENT si le Canada reçoit quatre soumissions ou moins pour répondre au besoin à la date de clôture de la demande de soumissions.

(b) Nonobstant tout examen par le Canada aux phases I ou II du Processus, les soumissionnaires sont et demeureront les seuls et uniques responsables de l'exactitude, de l'uniformité et de l'exhaustivité de leurs soumissions, et le Canada n'assume, en vertu de cet examen, aucune obligation ni de responsabilité envers les soumissionnaires de relever, en tout ou en partie, toute erreur ou toute omission, dans les soumissions ou en réponse à toute communication provenant d'un soumissionnaire.

LE SOUMISSIONNAIRE RECONNAÎT QUE LES EXAMENS LORS DES PHASES I ET II DU PRÉSENT PROCESSUS NE SONT QUE PRÉLIMINAIRES ET N'EMPÊCHENT PAS QU'UNE SOUMISSION SOIT NÉANMOINS JUGÉE NON RECEVABLE À LA PHASE III, ET CE, MÊME POUR LES EXIGENCES OBLIGATOIRES QUI ONT FAIT L'OBJET D'UN EXAMEN AUX PHASES I OU II, ET MÊME SI LA SOUMISSION AVAIT ÉTÉ JUGÉE RECEVABLE À UNE PHASE ANTÉRIEURE. LE CANADA PEUT DÉTERMINER À SA DISCRÉTION QU'UNE SOUMISSION

NE RÉPOND PAS À UNE EXIGENCE OBLIGATOIRE À N'IMPORTE QUELLE DE CES PHASES. LE SOUMISSIONNAIRE RECONNAÎT ÉGALEMENT QUE MALGRÉ LE FAIT QU'IL AIT FOURNI UNE RÉPONSE À UN AVIS OU À UN RAPPORT D'ÉVALUATION DE LA CONFORMITÉ (REC) (TEL QUE CES TERMES SONT DÉFINIS PLUS BAS) QU'IL EST POSSIBLE QUE CETTE RÉPONSE NE SUFFISE PAS POUR QUE SA SOUMISSION SOIT JUGÉE CONFORME AUX AUTRES EXIGENCES OBLIGATOIRES.

(c) Le Canada peut, à sa propre discrétion et à tout moment, demander et recevoir de l'information de la part du soumissionnaire afin de corriger des erreurs ou des lacunes administratives dans sa soumission, et cette nouvelle information fera partie intégrante de sa soumission. Ces erreurs pourraient être, entre autres : une signature absente; une case non cochée dans un formulaire; une erreur de forme; l'omission d'un accusé de réception, du numéro d'entreprise d'approvisionnement ou même les coordonnées des personnes-ressources, c'est-à-dire leurs noms, leurs adresses et les numéros de téléphone; ou encore des erreurs d'inattention dans les calculs ou dans les nombres, et des erreurs qui n'affectent en rien les montants que le soumissionnaire a indiqué pour le prix ou pour tout composant du prix. Ainsi, le Canada a le droit de demander ou de recevoir toute information après la date de clôture de l'invitation à soumissionner uniquement lorsque l'invitation à soumissionner permet ce droit expressément. Le soumissionnaire disposera alors d'un délai indiqué pour fournir l'information requise. Toute information fournie hors délais sera refusée.

(d) Le PCSP ne limite pas les droits du Canada en vertu du Guide des clauses et conditions uniformisées d'achat (CCUA) 2003 (2020-05-28) Instructions uniformisées – biens ou services – besoins concurrentiels, ni le droit du Canada de demander ou d'accepter toute information pendant la période de soumission ou après la clôture de cette dernière, lorsque la demande de soumissions confère expressément ce droit au Canada, ou dans les circonstances décrites au paragraphe (c).

(e) Le Canada enverra un Avis ou un REC selon la méthode de son choix et à sa discrétion absolue. Le soumissionnaire doit soumettre sa réponse par la méthode stipulée dans l'Avis ou le REC. Les réponses sont réputées avoir été reçues par le Canada à la date et à l'heure qu'elles ont été livrées au Canada par la méthode indiquée dans l'Avis ou le REC et à l'adresse qui y figure. Un courriel de réponse autorisé dans l'Avis ou le REC est réputé reçu par le Canada à la date et à l'heure auxquelles il a été reçu dans la boîte de réception de l'adresse électronique indiquée dans l'Avis ou le REC. Un Avis, ou un REC, envoyé par le Canada au soumissionnaire à l'adresse fournie par celui-ci dans la soumission ou après l'envoi de celle-ci est réputé avoir été reçu par le soumissionnaire à la date à laquelle il a été envoyé par le Canada. Le Canada n'assume aucune responsabilité envers les soumissionnaires pour les soumissions retardataires, peu importe la cause.

4.1.1.2 Phase I: Soumission financière

(a) Après la date et l'heure de clôture de cette demande de soumissions, le Canada examinera la soumission pour déterminer si elle comporte une soumission financière et si celle-ci contient toute l'information demandée par la demande de soumissions. L'examen par le Canada à la phase I se limitera à déterminer s'il y manque des informations exigées par la demande de soumissions à la soumission financière. Cet examen n'évaluera pas si la soumission financière répond à toute norme ou si elle est conforme à toutes les exigences de la demande.

(b) L'examen par le Canada durant la phase I sera effectué par des fonctionnaires du ministère des Travaux publics et des Services gouvernementaux Canada.

(c) Si le Canada détermine, selon sa discrétion absolue, qu'il n'y a pas de soumission financière ou qu'il manque toutes les informations demandées dans la soumission financière, la soumission sera alors jugée non recevable et sera rejetée.

(d) Pour les soumissions autres que celles décrites au paragraphe (c), Canada enverra un avis écrit au soumissionnaire (« Avis ») identifiant où la soumission financière manque d'informations. Un soumissionnaire dont la soumission financière a été jugée recevable selon les exigences examinées lors de la phase I ne recevra pas d'Avis. De tels soumissionnaires n'auront pas le droit

de soumettre de l'information supplémentaire relativement à leur soumission financière.

(e) Les soumissionnaires qui ont reçu un Avis bénéficieront d'un délai indiqué dans l'Avis (la « période de grâce ») pour redresser les points indiqués dans l'Avis en fournissant au Canada, par écrit, l'information supplémentaire ou une clarification en réponse à l'Avis. Les réponses reçues après la fin de la période de grâce ne seront pas prises en considération par le Canada sauf dans les circonstances et conditions stipulées expressément dans l'avis.

(f) Dans sa réponse à l'Avis, le soumissionnaire n'aura le droit de redresser que la partie de sa soumission financière indiquée dans l'Avis. Par exemple, lorsque l'Avis indique qu'un élément a été laissé en blanc, seule l'information manquante pourra ainsi être ajoutée à la soumission financière, excepté dans les cas où l'ajout de cette information entraînera nécessairement la modification des calculs qui ont déjà été présentés dans la soumission financière (p. ex. le calcul visant à déterminer le prix total). Les rajustements nécessaires devront alors être mis en évidence par le soumissionnaire et seuls ces rajustements pourront être effectués. Toutes les informations fournies doivent satisfaire aux exigences de la demande de soumissions.

(g) Toute autre modification apportée à la soumission financière soumise par le soumissionnaire sera considérée comme une nouvelle information et sera rejetée. Aucun changement ne sera autorisé à une quelconque autre section de la soumission du soumissionnaire. L'intégralité de l'information soumise conformément aux exigences de cette demande de soumissions en réponse à l'Avis remplacera **uniquement** la partie de la soumission financière originale telle qu'autorisée ci-dessus et sera utilisée pour le reste du processus d'évaluation des soumissions.

(h) Le Canada déterminera si la soumission financière est recevable pour les exigences examinées à la phase I, en tenant compte de l'information supplémentaire ou de la clarification fournie par le soumissionnaire conformément à la présente section. Si la soumission financière n'est pas jugée recevable au regard des exigences examinées à la phase I à la satisfaction du Canada, la soumission financière sera jugée non recevable et rejetée.

(i) Seules les soumissions jugées recevables conformément aux exigences examinées à la phase I à la satisfaction du Canada seront examinées à la phase II.

4.1.1.3 Phase II : Soumission technique

(a) L'examen par le Canada au cours de la phase II se limitera à une évaluation de la soumission technique afin de vérifier si le soumissionnaire a respecté toutes les exigences obligatoires d'admissibilité. Cet examen n'évalue pas si la soumission technique répond à une norme ou répond à toutes les exigences de la soumission. Les exigences obligatoires d'admissibilité sont les critères techniques obligatoires tels qu'ainsi décrits dans la présente demande de soumissions comme faisant partie du Processus de conformité des soumissions en phases. Les critères techniques obligatoires qui ne sont pas identifiés dans la demande de soumissions comme faisant partie du PCSP ne seront pas évalués avant la phase III.

(b) Le Canada enverra un avis écrit au soumissionnaire REC précisant les exigences obligatoires d'admissibilité que la soumission n'a pas respectées. Un soumissionnaire dont la soumission a été jugée recevable au regard des exigences examinées au cours de la phase II recevra un REC qui précisera que sa soumission a été jugée recevable au regard des exigences examinées au cours de la phase II. Le soumissionnaire en question ne sera pas autorisé à soumettre des informations supplémentaires en réponse au REC.

(c) Le soumissionnaire disposera de la période de temps précisée dans le REC (« période de grâce ») pour remédier à l'omission de répondre à l'une ou l'autre des exigences obligatoires d'admissibilité inscrites dans le REC en fournissant au Canada, par écrit, des informations supplémentaires ou des clarifications en réponse au REC. Les réponses reçues après la fin de la période de grâce ne seront pas prises en considération par le canada sauf, dans les circonstances et conditions expressément prévues par le REC.

(d) La réponse du soumissionnaire doit adresser uniquement les exigences obligatoires d'admissibilité énumérées dans le rapport d'évaluation de conformité (REC) et considérées comme non accomplies, et doit inclure uniquement les renseignements nécessaires pour ainsi se conformer aux exigences. Toutefois, dans le cas où une réponse aux exigences obligatoires d'admissibilité énumérées dans le REC entraînera nécessairement la modification d'autres renseignements qui sont déjà présents dans la soumission, les rajustements nécessaires devront être mis en évidence par le soumissionnaire. La réponse au REC ne doit pas inclure de changement à la soumission financière. Toute autre information supplémentaire qui n'est pas requise pour se conformer aux exigences ne sera pas prise en considération par le Canada.

(e) La réponse du soumissionnaire au REC devra spécifier, pour chaque cas, l'exigence obligatoire d'admissibilité du REC à laquelle elle répond, notamment en identifiant le changement effectué dans la section correspondante de la soumission initiale, et en identifiant dans la soumission initiale les modifications nécessaires qui en découlent. Pour chaque modification découlant de la réponse aux exigences obligatoires d'admissibilité énumérées dans le REC, le soumissionnaire doit expliquer pourquoi une telle modification est nécessaire. Il n'incombe pas au Canada de réviser la soumission du soumissionnaire; il incombe plutôt au soumissionnaire d'assumer les conséquences si sa réponse au REC n'est pas effectuée conformément au présent paragraphe. Toutes les informations fournies doivent satisfaire aux exigences de la demande de soumissions.

(f) Tout changement apporté à la soumission par le soumissionnaire en dehors de ce qui est demandé, sera considéré comme étant de l'information nouvelle et ne sera pas prise en considération. L'information soumise selon les exigences de cette demande de soumissions en réponse au REC remplacera, intégralement et **uniquement** la partie de la soumission originale telle qu'elle est autorisée dans cette section.

(g) Les informations supplémentaires soumises pendant la phase II et permises par la présente section seront considérées comme faisant partie de la soumission et seront prises en compte par le Canada dans l'évaluation de la soumission lors de la phase II que pour déterminer si la soumission respecte les exigences obligatoires admissibles. Celles-ci ne seront utilisées à aucune autre phase de l'évaluation pour augmenter ou diminuer les notes que la soumission originale pourrait obtenir sans les avantages de telles informations additionnelles. Par exemple, un critère obligatoire admissible qui exige l'obtention d'un nombre minimum de points pour être considéré conforme sera évalué à la phase II afin de déterminer si cette note minimum obligatoire aurait été obtenue si le soumissionnaire n'avait pas soumis les renseignements supplémentaires en réponse au REC. Dans ce cas, la soumission sera considérée comme étant conforme par rapport à ce critère obligatoire admissible et les renseignements supplémentaires soumis par le soumissionnaire lieront le soumissionnaire dans le cadre de sa soumission, mais la note originale du soumissionnaire, qui était inférieure à la note minimum obligatoire pour ce critère obligatoire admissible, ne changera pas, et c'est cette note originale qui sera utilisée pour calculer les notes pour la soumission.

(h) Le Canada déterminera si la soumission est recevable pour les exigences examinées à la phase II, en tenant compte de l'information supplémentaire ou de la clarification fournie par le soumissionnaire conformément à la présente section. Si la soumission n'est pas jugée recevable selon des exigences examinées à la phase II à la satisfaction du Canada, la soumission financière sera jugée non recevable et rejetée.

(i) Uniquement les soumissions jugées recevables selon les exigences examinées à la phase II et à la satisfaction du Canada seront ensuite évaluées à la phase III.

4.1.1.4 Phase III : Évaluation finale de la soumission

(a) À la phase III, le Canada complétera l'évaluation de toutes les soumissions jugées recevables selon les exigences examinées à la phase II. Les soumissions seront évaluées par rapport à l'ensemble des exigences de la demande de soumissions, y compris les exigences d'évaluation technique et financière.

(b) Une soumission sera jugée non recevable et sera rejetée si elle ne respecte pas toutes les exigences d'évaluation obligatoires de la demande de soumissions.

4.2 Évaluation technique

(a) **Critères techniques obligatoires :**

(i) Chaque soumission fera l'objet d'un examen pour en déterminer la conformité avec les exigences obligatoires de la demande de soumissions. Tous les éléments de la demande de soumissions qui constituent des exigences obligatoires sont désignés précisément par les termes « doit », « doivent » ou « obligatoire ». Les soumissions qui ne sont pas conformes à chacune des exigences obligatoires seront déclarées irrecevables et rejetées.

(ii) Les critères techniques obligatoires sont décrits dans la pièce jointe 4.1

(iii) S'il y a lieu, le Processus de conformité des soumissions en phases s'appliquera uniquement aux exigences techniques obligatoires indiquées par l'exposant (^{PC}). Les exigences techniques obligatoires non affectées de l'exposant (^{PC}) ne seront pas assujetties au Processus de conformité des soumissions en phases.

EO1 (^{PC})	**Services facturables ($) par la soumissionnaire (*) pour la prestation de services professionnels de *cybersécurité* en GI-TI dans une infrastructure en nuage public.** **(*) Dans l'évaluation de l'expérience de l'entreprise pour ce critere, le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire tel que défini dans :** **Partie 3, Section 3.2** **Section i ; Soumission Technique** **Justification de la conformité technique** **Paragraphe C (page 17)**

(b) **Critères techniques cotés**

(i) Chaque soumission sera cotée en attribuant une note aux exigences cotées, qui sont précisées dans la demande de soumissions par le terme « cotées » ou par voie de référence à une note. Les soumissions qui ne sont pas complètes et qui ne contiennent pas tous les renseignements exigés dans la demande de soumissions seront cotées en conséquence.

(ii) Les exigences cotées sont décrites dans la pièce jointe 4.2.

(c) **Ressources évaluées lors du processus d'autorisation de tâches**

i. Les ressources par catégorie ne seront pas évaluées dans le cadre de la présente demande de soumissions.

ii. Les ressources ne seront évaluées qu'après l'attribution du contrat quand l'entrepreneur devra accomplir des tâches précises. Après l'attribution du contrat, le processus d'autorisation de tâches sera appliqué conformément à la Partie 7 – Clauses du contrat subséquent, selon l'article intitulé « Autorisation de tâches ». Quand un formulaire d'autorisation de tâches sera émis, l'entrepreneur devra proposer une ressource pour satisfaire le besoin précis d'après l'énoncé des travaux du formulaire d'autorisation de tâches. La ressource proposée sera ensuite évaluée d'après les critères indiqués dans l'énoncé des travaux du contrat, conformément à l'appendice C de l'annexe A.

(d) **Vérification des références**

(i) La vérification des références ne se fait pas de façon systématique. Toutefois, si TPSGC choisit de procéder à une vérification des références pour quelque exigence cotée ou obligatoire que ce soit, il le fera pour les soumissionnaires dont la candidature n'a pas été jugée irrecevable à ce stade de l'évaluation.

(ii) Le Canada effectuera la vérification des références par courriel. Il enverra toutes les demandes de vérification des références par courriel dans un délai de 48 heures aux personnes-ressources citées en référence par les soumissionnaires dans leur soumission. La réponse doit être envoyée dans les cinq jours ouvrables suivant l'envoi du courriel de vérification des références, faute de quoi le Canada n'attribuera aucun point ou considérera que le soumissionnaire ne satisfait pas à l'exigence obligatoire en matière d'expérience (selon le cas).

(iii) Le troisième jour ouvrable après l'envoi du courriel, si le Canada n'a pas reçu de réponse, il en avisera le soumissionnaire par courriel pour que ce dernier puisse rappeler à la personne en question qu'il faut répondre au Canada dans le délai de cinq jours ouvrables. Si la personne donnée en référence n'est pas disponible au moment de l'évaluation, le soumissionnaire pourra fournir le nom et l'adresse électronique d'une autre personne chez le même client. Cette possibilité ne sera offerte aux soumissionnaires qu'une fois par client, et ce, uniquement si la personne citée en référence initialement n'est pas disponible (c'est-à-dire que le soumissionnaire ne pourra soumettre le nom d'une autre personne si la première personne-ressource indique qu'elle ne souhaite pas répondre ou qu'elle n'est pas en mesure de le faire). Le délai de cinq jours ouvrables ne sera pas prolongé pour permettre à la nouvelle personne-ressource de répondre. Si le client cité en référence ne répond pas dans les cinq jours ouvrables, le Canada ne communiquera pas avec le soumissionnaire, et ce dernier ne pourra pas soumettre le nom d'une autre personne.

(iv) En cas de contradiction entre l'information donnée par la personne citée en référence et celle fournie par le soumissionnaire, la première prévaudra.

(v) On n'accordera aucun point ou l'on considérera qu'un critère obligatoire n'est pas respecté (selon le cas) si (1) le client cité en référence indique qu'il n'est pas en mesure de fournir l'information demandée ou qu'il ne veut pas le faire, ou (2) le client cité en référence n'est pas un client du soumissionnaire même (par exemple, le client ne peut pas être le client d'une filiale du soumissionnaire). De même, on n'accordera aucun point au soumissionnaire ou l'on considérera qu'un critère obligatoire n'est pas respecté si le client est lui-même une filiale ou une autre entité qui a des liens de dépendance avec le soumissionnaire.

4.3 Évaluation financière

Proposition recevable dont la cote combinée du mérite technique et du prix est la plus élevée

(a) L'évaluation financière sera effectuée d'après les taux quotidiens fermes indiqués dans les soumissions recevables.

(b) Deux méthodes possibles d'évaluation financière peuvent être utilisées pour le présent besoin. La première méthode sera utilisée si trois soumissions ou plus sont jugées recevables (voir la section c) – Évaluation financière – Méthode A, ci-dessous). La deuxième méthode sera utilisée si moins de trois soumissions sont jugées recevables (voir la section d) – Évaluation financière – Méthode B ci-dessous).

(c) **Évaluation financière – Méthode A** : La méthode d'évaluation financière suivante sera utilisée si trois soumissions ou plus sont jugées recevables.

(i) **ÉTAPE 1 – ÉTABLISSEMENT DES MÉDIANES INFÉRIEURES ET SUPÉRIEURES POUR CHAQUE PÉRIODE ET CHAQUE CATÉGORIE DE RESSOURCES** : L'autorité contractante établira, pour chaque période et chaque catégorie de ressources, la fourchette médiane selon les taux fermes quotidiens fournis par les soumissionnaires dont la soumission est jugée recevable sur le plan technique. Pour chaque catégorie de ressources, on calculera la médiane à l'aide de la fonction connexe dans Microsoft Excel. Cette médiane permettra d'établir une fourchette qui prendra en compte un taux médian inférieur correspondant à une **valeur de moins (-) 10 % de la médiane et un taux médian supérieur correspondant à une valeur de plus (+) 30 % de la médiane**. Lorsqu'un nombre pair de soumissions sont jugées recevables sur le plan technique, la moyenne des deux tarifs médians sera utilisée pour calculer la fourchette médiane, alors que dans le cas d'un nombre impair de soumissions jugées recevables sur le plan technique, le tarif médian sera utilisé.

(ii) **ÉTAPE 2 – ATTRIBUTION DES POINTS** : Pour chaque période et chaque catégorie de ressources, les points seront attribués de la façon suivante.

(A) Le soumissionnaire ne recevra aucun point s'il propose, pour une période et une catégorie de ressources données, un tarif quotidien ferme qui est inférieur à la limite de la médiane inférieure, ou supérieur à la limite médiane supérieure établie pour cette période et cette catégorie de ressources.

(B) Le soumissionnaire dont le tarif quotidien ferme entre dans la fourchette des médianes supérieure et inférieure obtiendra des points d'après la formule suivante, qui seront arrondis à deux décimales :

$$\frac{\text{Taux quotidien ferme proposé le plus bas dans la fourchette des médianes}}{\text{Taux quotidien ferme proposé par le soumissionnaire dans les limites de la fourchette des médianes}} \times \text{Maximum de points attribués au tableau 1 ci-dessous}$$

(C) Le soumissionnaire dont le tarif journalier ferme entre dans la fourchette des médianes établies et qui est le plus bas parmi les tarifs proposés obtiendra le nombre maximum de points applicable indiqué au tableau 1 ci-dessous.

TABLEAU 1 – MAXIMUM DE POINTS ATTRIBUÉS					
Categorie de Resources	**Niveau d`expert**	**Période initiale**	**Option 1**	**Option 2**	**TOTAL**
Volet 6 : Services de Cyber Protection de SPICT					
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	2	20	20	20	**60**
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	3	20	20	20	**60**
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	2	20	20	20	**60**
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	3	20	20	20	**60**
C.7 Spécialiste en conception de sécurité des technologies de l'information	2	20	20	20	**60**
C.7 Spécialiste en conception de sécurité des technologies de l'information	3	20	20	20	**60**
C.8 Analyste de la sécurité des réseaux	2	20	20	20	**60**
C.8 Analyste de la sécurité des réseaux	3	20	20	20	**60**
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	2	20	20	20	**60**
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	3	20	20	20	**60**
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2	20	20	20	**60**
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	3	20	20	20	**60**
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2	20	20	20	**60**
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	3	20	20	20	**60**

C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2	20	20	20	**60**
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	3	20	20	20	**60**
TOTAL		320	320	3200	**960**

(iii) **ÉTAPE 3 – NOTE FINANCIÈRE** : On additionnera les points attribués à l'ÉTAPE 2 pour chaque période et chaque catégorie de ressources, et on arrondira le total à deux décimales pour obtenir la note financière. Un exemple d'évaluation financière à l'aide de la méthode A est fourni ci-après.

(iv) EXEMPLE D'ÉVALUATION FINANCIÈRE À L'AIDE DE LA MÉTHODE A

TABLEAU 2 – EXEMPLE D'ÉVALUATION FINANCIÈRE À L'AIDE DE LA MÉTHODE A

Catégories de ressources	Maximum de points	Soumissionnaire 1		Soumissionnaire 2		Soumissionnaire 3	
		Année 1	Année 2	Année 1	Année 2	Année 1	Année 2
Programmeur	150 (75 points par année)	400,00 $	400,00 $	420,00 $	440,00 $	450,00 $	450,00 $
Analyste des activités	100 (50 points par année)	600,00 $	600,00 $	600,00 $	620,00 $	650,00 $	680,00 $
Gestionnaire de projet	50 (25 points par année)	555,00 $	580,00 $	750,00 $	785,00 $	700,00 $	735,00 $
TOTAL	300						

ÉTAPE 1 – Établissement des médianes inférieures et supérieures pour chaque année et chaque catégorie de ressources

(Médiane 1) Pour la catégorie de ressources des programmeurs, la médiane de l'année 1 serait 420 $. La limite inférieure de la bande médiane serait 378 $ et la limite supérieure de la bande médiane serait 546 $.

(Médiane 2) Pour la catégorie de ressources des programmeurs, la médiane de l'année 2 serait 440 $. La limite inférieure de la bande médiane serait 396 $ et la limite supérieure de la bande médiane serait 572 $.

(Médiane 3) Pour la catégorie de ressources des analystes des activités, la médiane de l'année 1 serait 600 $. La limite inférieure de la bande médiane serait 540 $ et la limite supérieure de la bande médiane serait 780 $.

(Médiane 4) Pour la catégorie de ressources des analystes des activités, la médiane de l'année 2 serait 620 $. La limite inférieure de la bande médiane serait 558 $ et la limite supérieure de la bande médiane serait 806 $.

(Médiane 5) Pour la catégorie de ressources des gestionnaires de projet, la médiane de l'année 1 serait 700 $. La limite inférieure de la bande médiane serait 630 $ et la limite supérieure de la bande médiane serait 910 $.

(Médiane 6) Pour la catégorie de ressources des gestionnaires de projet, la médiane de l'année 2 serait 735 $. La limite inférieure de la bande médiane serait 661.50 $ et la limite supérieure de la bande médiane serait 955.50 $.

ÉTAPE 2 – Attribution des points

Soumissionnaire 1

Programmeur - année 1 =	75 points (tarif le plus bas dans les limites inférieure et supérieure de la bande médiane)
Programmeur - année 2 =	75 points (tarif le plus bas dans les limites inférieure et supérieure de la bande médiane)
Analyste des activités - année 1 =	50 points (tarif le plus bas dans les limites inférieure et supérieure de la bande médiane)
Analyste des activités - année 2 =	50 points (tarif le plus bas dans les limites inférieure et supérieure de la bande médiane)
Gestionnaire de projet - année 1 =	0 point (en dehors des limites inférieure et supérieure de la bande médiane)
Gestionnaire de projet - année 2 =	22,22 points, d'après le calcul suivant : taux le plus bas (800 $) ÷ taux proposé par le soumissionnaire (900 $) × 25 points
Soumissionnaire 2	
Programmeur - année 1 =	71,43 points, d'après le calcul suivant : tarif le plus bas (400 $) ÷ tarif proposé par le soumissionnaire (420 $) × 75 points
Programmeur - année 2 =	68.18 points, d'après le calcul suivant : tarif le plus bas (400 $) ÷ tarif proposé par le soumissionnaire (440 $) × 75 points
Analyste des activités – année 1 =	50 points (prix le plus bas dans les limites inférieure et supérieure de la bande médiane)
Analyste des activités – année 2 =	48,39 points, d'après le calcul suivant : tarif le plus bas (600 $) ÷ tarif proposé par le soumissionnaire (620 $) × 50 points
Gestionnaire de projet – année 1 =	23,33 points, d'après le calcul suivant : tarif le plus bas (700 $) ÷ tarif proposé par le soumissionnaire (750 $) × 25 points
Gestionnaire de projet – année 2 =	23,41 points, d'après le calcul suivant : tarif le plus bas (735 $) ÷ tarif proposé par le soumissionnaire (785 $) × 25 points
Soumissionnaire 3	
Programmeur - année 1 =	66,67 points, d'après le calcul suivant : tarif le plus bas (400 $) ÷ tarif proposé par le soumissionnaire (450 $) × 75 points
Programmeur - année 2 =	66,67 points, d'après le calcul suivant : tarif le plus bas (400 $) ÷ tarif proposé par le soumissionnaire (450 $) × 75 points
Analyste des activités – année 1 =	46,15 points, d'après le calcul suivant : tarif le plus bas (600 $) ÷ tarif proposé par le soumissionnaire (650 $) × 50 points
Analyste des activités – année 2 =	44,12 points, d'après le calcul suivant : tarif le plus bas (600 $) ÷ tarif proposé par le soumissionnaire (680 $) × 50 points
Gestionnaire de projet - année 1 =	25 points (prix le plus bas dans les limites inférieure et supérieure de la bande médiane)
Gestionnaire de projet - année 2 =	25 points (prix le plus bas dans les limites inférieure et supérieure de la bande médiane)
ÉTAPE 3 – Note financière	
Soumissionnaire 1 :	75 + 75 + 50 + 50 + 0 + 0 = note financière totale de 250 points sur un total possible de 300 points
Soumissionnaire 2 :	71,43 + 68.18 + 50 + 48,39 + 23,33 + 23.41 = note financière totale de 284,74 points sur un total possible de 300 points
Soumissionnaire 3 :	66,67 + 66,67 + 46,15 + 44.12 + 25 + 25 = note financière totale de 273.61 points sur un total possible de 300 points

(d) **Évaluation financière – Méthode B** : La méthode d'évaluation financière suivante sera utilisée si moins de trois soumissions sont jugées recevables :

(i) **ÉTAPE 1 – ATTRIBUTION DES POINTS** : Pour chaque période et chaque catégorie de ressources, les points seront attribués de la façon suivante :

(A) Les points seront attribués en fonction des calculs ci-dessous, et le total sera arrondi à deux décimales près.

Taux quotidien ferme proposé le plus bas / Taux quotidien ferme proposé par le soumissionnaire x Maximum de points attribués au tableau 3 ci-dessous

Le soumissionnaire offrant le taux quotidien ferme le plus bas obtiendra le nombre maximum de points applicable indiqué au tableau 3 ci-dessous.

TABLEAU 3 – MAXIMUM DE POINTS ATTRIBUÉS

Categorie de Resources	Niveau d`expert	Période initiale	Option 1	Option 2	TOTAL
Volet 6 : Services de Cyber Protection de SPICT					
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	2	20	20	20	**60**
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	3	20	20	20	**60**
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	2	20	20	20	**60**
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	3	20	20	20	**60**
C.7 Spécialiste en conception de sécurité des technologies de l'information	2	20	20	20	**60**
C.7 Spécialiste en conception de sécurité des technologies de l'information	3	20	20	20	**60**
C.8 Analyste de la sécurité des réseaux	2	20	20	20	**60**
C.8 Analyste de la sécurité des réseaux	3	20	20	20	**60**
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	2	20	20	20	**60**
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	3	20	20	20	**60**
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2	20	20	20	**60**
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	3	20	20	20	**60**

C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2	20	20	20	**60**
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	3	20	20	20	**60**
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2	20	20	20	**60**
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	3	20	20	20	**60**
TOTAL		320	320	3200	**960**

(ii) **ÉTAPE 2 – NOTE FINANCIÈRE** : On additionnera les points attribués à l'ÉTAPE 1 pour chaque période et chaque catégorie de ressources, et on arrondira à deux décimales pour obtenir la note financière.

(e) **Justification des taux pour les services professionnels**

D'après l'expérience du Canada, les soumissionnaires proposeront parfois des taux pour une ou plusieurs catégories de ressources au moment de la soumission qu'ils refuseront plus tard de respecter, en affirmant que ces taux ne leur permettent pas de recouvrer les frais ou de rentabiliser leurs activités. Au moment d'évaluer les taux soumis pour les services professionnels, le Canada peut, sans toutefois y être obligé, demander une justification des prix conformément à cet article. Si le Canada demande une justification des prix, elle sera demandée à tous les soumissionnaires conformes proposant un taux au moins 20 % inférieur à la médiane des taux offerts par tous les soumissionnaires conformes pour la ou les mêmes catégories de ressources. Si le Canada demande une justification des prix, le soumissionnaire doit fournir les renseignements suivants :

(i) une facture (avec le numéro de série du contrat ou un autre identificateur unique du contrat) démontrant que le soumissionnaire a fourni et a facturé des services similaires à ceux qui seraient fournis par cette catégorie de ressources à un client (qui n'a aucun lien de dépendance avec le soumissionnaire) pendant au moins trois (3) mois au cours de la période de dix-huit (18) mois précédant la date de clôture de la demande de soumissions, et que les coûts facturés étaient égaux ou inférieurs au taux proposé au Canada;

(ii) relativement à la facture mentionnée en (i), une preuve du client du soumissionnaire démontrant que les services indiqués sur la facture comprennent au minimum 50 % des tâches énumérées dans l'énoncé des travaux pour la catégorie de ressources évaluée, et ce, à un taux déraisonnablement bas. Il peut s'agir d'une copie du contrat (dans lequel on décrit les services à offrir et où l'on démontre qu'au moins 50 % des tâches sont les mêmes que celles qui doivent être effectuées dans le cadre de l'énoncé des travaux de la présente demande de soumissions), ou d'une attestation du client indiquant que les services notés sur la facture comprenaient au moins 50 % des tâches qui doivent être effectuées en vertu de l'énoncé des travaux de la présente demande de soumissions;

(iii) le nom, le numéro de téléphone et, si possible, l'adresse de courriel d'une personne-ressource du client ayant reçu chacune des factures présentées au point (i), afin que le Canada puisse valider tout renseignement fourni par le soumissionnaire.

Lorsque le Canada demande une justification des taux offerts pour une catégorie de ressources particulière, il incombe entièrement au soumissionnaire de présenter l'information (décrite ci-

dessus ou pouvant être autrement demandée par le Canada, y compris l'information qui permettrait au Canada de vérifier les renseignements fournis concernant la ressource proposée) qui permettrait au Canada de déterminer s'il peut réellement se fier à la capacité du soumissionnaire de fournir les services requis aux taux indiqués dans la soumission. Lorsque le Canada détermine que l'information fournie par le soumissionnaire ne justifie pas des taux déraisonnablement bas, la proposition sera jugée irrecevable.

(f) **Formules des tableaux d'établissement des prix**

Si les tableaux des prix fournis aux soumissionnaires comprennent des formules, le Canada peut entrer de nouveau les prix fournis par les soumissionnaires dans un nouveau tableau, s'il estime que les formules ne fonctionnent plus correctement dans la version fournie par un soumissionnaire.

4.4 Méthode de sélection

(a) Évaluation des soumissions

Processus de sélection : Le processus de sélection suivant sera suivi :

(i) Pour être déclarée recevable, une soumission doit respecter les exigences de la demande de soumissions, satisfaire à tous les critères d'évaluation obligatoires et obtenir la note de passage indiquée pour les critères cotés indiqués dans la demande de soumissions.

(ii) Un contrat sera attribué en réponse a cette demande de proposition

(iii) La soumission recevable obtenant la note totale la plus élevée sera recommandée pour l'attribution du contrat. La note maximale qu'un soumissionnaire peut obtenir pour le mérite technique est de 70; la note maximale en ce qui concerne le prix est établie à 30.

(A) Calcul de la note technique totale : on calculera la note technique totale pour chaque soumission recevable en convertissant la note technique obtenue pour les critères techniques cotés par points à l'aide de la formule suivante (le résultat étant arrondi à deux décimales).

Note technique / Note technique maximale (Soumissionnaires, veuillez consulter la note technique maximale) x 70 = Note technique totale

(B) Calcul de la note financière totale : on calculera la note financière totale pour chaque soumission recevable en convertissant la note financière obtenue pour l'évaluation financière à l'aide de la formule suivante (le résultat étant arrondi à deux décimales).

Note financière / Maximum de points attribués total (Soumissionnaires, veuillez consulter le maximum de points attribués total) x 30 = Note financière totale

(C) Calcul de la note totale du soumissionnaire : la note totale du soumissionnaire sera calculée pour chaque soumission recevable à l'aide de la formule suivante :

Note technique totale + note financière totale = note totale du soumissionnaire

(iv) Dans l'éventualité où des soumissionnaires obtiendraient la même note totale, le soumissionnaire ayant obtenu la note technique totale la plus élevée sera classé au premier rang.

(i) Les soumissionnaires devraient noter que l'attribution des contrats est assujettie au processus d'approbation interne du Canada, qui prévoit l'approbation obligatoire du

financement selon le montant de tout contrat proposé. Même si un soumissionnaire a été recommandé pour l'attribution d'un contrat, un contrat sera attribué uniquement si l'approbation interne est obtenue conformément aux politiques internes du Canada. Si l'approbation n'est pas obtenue, aucun contrat ne sera attribué.

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 ce dernier. À moins d'indication contraire, le Canada déclarera une soumission non recevable ou qu'il y a manquement de la part de l'entrepreneur s'il est établi qu'une attestation fournie avec sa soumission comprend de fausses déclarations, faites 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 préalables à l'attribution du contrat et renseignements supplémentaires

Les attestations et les renseignements supplémentaires énumérés ci-dessous devraient être présentés avec l'offre, mais il est possible de les présenter après. Si l'une ou l'autre de ces attestations ou l'un ou l'autre de ces renseignements supplémentaires demandés n'est pas fourni, l'autorité contractante informera le soumissionnaire du délai qu'elle lui accorde pour fournir les renseignements. Si le soumissionnaire ne remet pas les attestations ou les renseignements supplémentaires énoncés ci-dessous dans le délai imparti, son offre sera jugée non recevable.

(a) Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation de soumission

En présentant une soumission, le soumissionnaire atteste que ni lui ni un membre de la coentreprise, si le soumissionnaire est une coentreprise, ne sont nommés dans la « Liste d'admissibilité à soumissionner restreinte par le Programme de contrats fédéraux » qui figure au bas de la page du site Web du Programme du travail d'Emploi et Développement social Canada (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html).

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, est nommé dans la « Liste d'admissibilité à soumissionner restreinte par le Programme de contrats fédéraux » au moment de l'attribution du contrat.

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, est nommé dans la « Liste d'admissibilité à soumissionner restreinte par le Programme de contrats fédéraux » pendant la durée du contrat.

Le soumissionnaire doit fournir à l'autorité contractante la pièce jointe 5.1, 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 la pièce jointe 5.1, Programme de contrats fédéraux pour l'équité en matière d'emploi – Attestation, remplie pour chaque membre de la coentreprise.

(b) Présentation d'une seule soumission

En déposant une soumission, le soumissionnaire atteste qu'il ne se considère pas comme étant « lié » à aucun autre soumissionnaire.

PARTIE 6 – EXIGENCES RELATIVES À LA SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

6.1 Exigences relatives à la sécurité

(a) Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées :

(i) le soumissionnaire doit détenir une attestation de sécurité d'organisation valable, conformément à la Partie 7 – Clauses du contrat subséquent;

(ii) les personnes proposées par le soumissionnaire qui doivent avoir accès à des renseignements ou à des biens classifiés ou protégés, ou encore à des établissements de travail dont l'accès est réglementé, doivent satisfaire aux exigences relatives à la sécurité précisées dans la Partie 7 – Clauses du contrat subséquent;

(b) Avant de délivrer une autorisation de tache, les conditions suivantes doivent être respectées :

(i) les personnes proposées par le soumissionnaire qui doivent avoir accès à des renseignements ou à des biens classifiés ou protégés, ou encore à des établissements de travail dont l'accès est réglementé, doivent satisfaire aux exigences relatives à la sécurité précisées dans la Partie 7 – Clauses du contrat subséquent;

(ii) le soumissionnaire doit fournir le nom de toutes les personnes qui devront avoir accès à des renseignements ou à des biens classifiés ou protégés, ou encore à des établissements de travail dont l'accès est réglementé

(c) On rappelle aux soumissionnaires d'obtenir rapidement la cote de sécurité requise. La décision de retarder l'attribution du contrat, pour permettre au soumissionnaire retenu d'obtenir la cote de sécurité requise, demeure à l'entière discrétion de l'autorité contractante.

(d) Pour obtenir de plus amples renseignements sur les exigences relatives à la sécurité, les soumissionnaires devraient consulter le site Web du Programme de sécurité des contrats de TPSGC (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-fra.html).

(e) Si le soumissionnaire est une coentreprise, chacun des membres de celle-ci doit respecter les exigences relatives à la sécurité.

6.2 Capacité financière

(a) La clause A9033T du Guide des CCUA (2012-07-16), Capacité financière, s'applique, à la différence que le paragraphe 3 est supprimé et est remplacé par : « Si le soumissionnaire est une filiale d'une autre entreprise, chaque société mère, y compris la société mère ultime, devra fournir l'information financière demandée en 1(a) à (f). L'information financière fournie par une société mère ne dégage pas pour autant le soumissionnaire de l'obligation de présenter ses propres renseignements financiers; toutefois, si le soumissionnaire est une filiale d'une autre entreprise, et dans le cours normal des affaires les renseignements financiers ne sont pas générés distinctement pour la filiale, les renseignements financiers de la société mère doivent être fournis. Si le Canada juge que le soumissionnaire ne possède pas la capacité financière, mais que la société mère possède cette capacité, ou si le Canada ne peut évaluer la capacité financière du soumissionnaire puisque son information financière fait partie intégrante de celle de la société mère, le Canada peut, à sa seule discrétion, attribuer le contrat au soumissionnaire sous réserve que la société mère fournisse une garantie au Canada. »

(b) Si le soumissionnaire est une coentreprise, chacun des membres de celle-ci doit respecter les exigences relatives à la capacité financière.

PARTIE 7 – CLAUSES DU CONTRAT SUBSÉQUENT

Remarque à l'intention des soumissionnaires: *Tout contrat résultant listera seulement les volets pertinents ci-dessus qui seront attribués aux soumissionnaires acceptés conformément à la méthode d'évaluation décrite dans la présente demande de soumissions. Si un soumissionnaire est sélectionné pour l'attribution d'un ou plusieurs volets, le Canada se réserve le droit d'attribuer un contrat pour tous les volets de travail alloués à ce soumissionnaire.*

Supprimer ce titre ainsi que la phrase suivante au moment de l'attribution du contrat.

Les clauses suivantes s'appliquent à tout contrat découlant de la demande de soumissions et en font partie intégrante.

7.1 Besoin

(a) _____ (l'« **entrepreneur** ») consent à fournir au client les services décrits dans le contrat, y compris l'énoncé des travaux, conformément au contrat et aux prix qui y sont énoncés. Cela comprend la prestation de services professionnels, à la demande du Canada, à un ou plusieurs emplacements qui seront précisés par ce dernier, à l'exclusion de tout emplacement se trouvant dans des secteurs assujettis à des ententes sur les revendications territoriales globales (ERTG)

(b) **Client** : En vertu du contrat, le « **client** » est Agence des Services Frontaliers du Canada

(c) **Réorganisation du client** : Le changement de dénomination sociale, la réorganisation, le réaménagement ou la restructuration d'un client n'auront aucune incidence sur les obligations de l'entrepreneur (ni ne donneront lieu au paiement d'honoraires supplémentaires). La réorganisation, le réaménagement ou la restructuration du client s'entendent aussi de sa privatisation, de sa fusion avec une autre entité et de sa dissolution, lorsque cette dissolution est suivie de la création d'une ou de plusieurs autres entités dont la mission est semblable à celle du client d'origine. Peu importe le type de restructuration, le Canada peut désigner un autre ministère ou un autre organisme gouvernemental comme autorité contractante ou responsable technique, conformément aux nouveaux rôles et aux nouvelles responsabilités découlant de la restructuration.

(d) **Définitions** : Les termes et expressions définis dans les conditions générales et dans les conditions générales supplémentaires et employés dans ce contrat ont le sens qui leur est attribué dans les conditions générales ou dans les conditions générales supplémentaires. L'expression « utilisateur désigné » dans l'arrangement en matière d'approvisionnement fait référence au client. De plus, « produit livrable » ou « produits livrables » comprend toute la documentation décrite dans le présent contrat. Une référence à un « bureau local » de l'entrepreneur signifie un bureau ayant au moins un employé à temps plein qui n'est pas une ressource partagée qui y travaille

7.2 Autorisation de tâches

(a) **Autorisations de tâches sur demande** : La totalité ou une partie des travaux du contrat seront réalisés « sur demande », au moyen d'une autorisation de tâches. Les travaux décrits dans l'autorisation de tâches doivent être conformes à la portée du contrat. L'entrepreneur ne doit pas commencer les travaux avant d'avoir reçu une autorisation de tâches approuvée, émise par le Canada. L'entrepreneur convient que toute tâche effectuée avant la réception de cette autorisation de tâches approuvée est effectuée à ses propres risques.

(b) **Evaluation des ressources proposées à l'étape de l'autorisation de tâches** : Les processus relatifs à l'établissement d'une autorisation de tâches, en réponse à une autorisation de tâche et liés à l'évaluation d'une autorisation de tâches sont décrits aux appendices A, B, C et D de l'annexe A.

(c) **Formulaire et contenu du projet d'autorisation de tâches** :

(i) Le responsable technique fournira à l'entrepreneur une description des tâches au moyen d'un projet d'autorisation de tâches à l'aide du formulaire figurant à l'annexe __.

(ii) Le projet d'autorisation de tâches doit expliquer en détail les travaux à effectuer et doit également contenir les renseignements suivants :

(A) Le numéro de contrat;

(B) le numéro de tâche;

(C) la date à laquelle la réponse de l'entrepreneur doit être reçue (cette date figurera dans le projet d'AT, mais pas dans l'AT attribuée);

(D) les catégories de ressources et le nombre de ressources nécessaires;

(E) une description des travaux associés à la tâche, notamment les activités à réaliser et les produits livrables à présenter (comme des rapports);

(F) les dates de début et de fin;

(G) toute option pour prolonger la date de fin initiale (s'il y a lieu);

(H) les dates clés des produits livrables et des paiements (s'il y a lieu);

(I) le nombre de jours-personnes requis;

(J) une note indiquant si les travaux comprennent des activités à réaliser sur place, en précisant l'endroit;

(K) le profil linguistique des ressources requises;

(L) le niveau d'attestation de sécurité que doivent posséder les employés de l'entrepreneur;

(M) le prix payable à l'entrepreneur pour l'exécution de la tâche, en indiquant s'il s'agit d'un prix ferme ou du prix maximum de l'autorisation de tâches (et dans le cas du prix maximum, l'autorisation de tâches doit indiquer la façon dont le montant final payable sera déterminé; lorsque l'autorisation de tâches n'indique pas la façon dont le montant final payable sera déterminé, le montant payable est le montant, jusqu'à concurrence du montant maximum, pour les heures réellement travaillées sur le projet que l'entrepreneur justifie en présentant les feuilles de présence remplies au moment de l'exécution des travaux par les employés pour justifier les frais);

(N) toute autre contrainte pouvant avoir des répercussions sur l'exécution de la tâche.

(d) **Réponse de l'entrepreneur à un projet d'autorisation de tâches** : L'entrepreneur doit fournir au responsable technique, dans les 2 jours ouvrables de la réception du projet d'autorisation de tâches ou tout autre délai plus long précisé dans le projet d'autorisation de tâches), une proposition du prix estimatif total pour l'exécution de la tâche et une ventilation de ce coût, établie conformément à la base de paiement du contrat, ainsi que la ou les ressources proposées connexes, conformément à l'appendice A de l'annexe A du contrat. La proposition de prix de l'entrepreneur doit être établie selon les taux stipulés dans le contrat. 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'autorisation de tâches.

(e) **Limite des autorisations de tâches et responsabilités à l'égard de leur émission officielle** :

Pour être attribuée de façon officielle, une autorisation de tâches doit porter les signatures suivantes :

(i) toute autorisation de tâches Doit être signée par le responsable technique, l'autorité contractante de SPAC et l'entrepreneur;

Toute autorisation de tâches qui ne porte pas les signatures requises n'a pas été émise de façon officielle par le Canada et n'est donc pas valide. Tous les travaux réalisés par

l'entrepreneur sans que celui-ci ait reçu une autorisation de tâches officielle seront effectués à ses propres risques. L'entrepreneur doit aviser l'autorité contractante s'il reçoit une autorisation de tâches qui ne porte pas les signatures requises. Au moyen d'un avis écrit envoyé à l'entrepreneur, l'autorité contractante peut suspendre en tout temps le pouvoir du client d'attribuer des autorisations de tâches, ou réduire la valeur indiquée à l'alinéa (i) ci-dessus. L'avis de suspension ou de réduction prend effet dès la réception.

(f) **Rapports d'utilisation périodique** :

(i) L'entrepreneur doit compiler et tenir à jour des données sur les services fournis au gouvernement fédéral, conformément aux autorisations de tâches valides émises dans le cadre du contrat. L'entrepreneur doit fournir ces données conformément aux exigences d'établissement de rapports précisées ci-dessous. Si certaines données requises ne sont pas disponibles, l'entrepreneur doit en indiquer la raison. Si des services ne sont pas fournis pendant une période donnée, l'entrepreneur doit soumettre un rapport portant la mention « NÉANT ». Les données doivent être présentées chaque trimestre à l'autorité contractante. De temps en temps, l'autorité contractante peut également exiger un rapport intérimaire au cours d'une période de référence.

(ii) Les trimestres sont définis comme suit :

(A) premier trimestre : du 1er avril au 30 juin;

(B) deuxième trimestre : du 1er juillet au 30 septembre;

(C) troisième trimestre : du 1er octobre au 31 décembre;

(D) quatrième trimestre : du 1er janvier au 31 mars.

Les données doivent être présentées à l'autorité contractante dans les 15 jours civils suivant la fin de la période de référence.

(iii) Chaque rapport doit contenir les informations suivantes pour chaque autorisation de tâche qui est approuvée et émise de façon officielle (et tel que modifié) :

(A) le numéro de l'autorisation de tâches et le numéro de la version modifiée, le cas échéant;

(B) le titre ou une courte description de chaque tâche autorisée;

(C) le nom, la catégorie de ressources et le niveau de chaque ressource participant à l'exécution de l'autorisation de tâches, le cas échéant;

(D) le coût estimatif total précisé dans l'autorisation de tâches valide de chaque tâche, taxes applicables en sus;

(E) le montant total dépensé jusqu'à présent, taxes applicables en sus, pour chaque tâche autorisée;

(F) les dates de début et de fin de chaque tâche autorisée;

(G) l'état d'avancement de chaque tâche autorisée, s'il y a lieu (p. ex. indiquer si les travaux sont en cours, ou si le Canada a annulé ou suspendu l'autorisation de tâches).

(iv) Chaque rapport doit aussi contenir les informations cumulatives suivantes pour chaque autorisation de tâches émise de façon officielle (et tel que modifié) :

(A) le montant (taxes applicables en sus) précisé dans le contrat (selon la dernière modification, s'il y a lieu) qui correspond à la responsabilité totale du Canada envers l'entrepreneur pour toutes les autorisations de tâches émises de façon officielle;

(B) le montant total, taxes applicables en sus, dépensé jusqu'à présent pour toutes les autorisations de tâches émises de façon officielle.

(g) **Consolidation des AT pour raisons administratives** Le contrat peut etre modifié lorsque nécessaire pour refléter toutes les Authorisation de taches emises jusqu`à jour, pour documenter les travaux performés sous ses authorisations de taches pour des raisons administratives

(h) **Refus d'une autorisation de tâches ou soumission d'une réponse non valide** : L'entrepreneur n'est pas tenu de répondre à chaque projet d'autorisation de tâches présenté par le Canada. Cependant, en plus des autres droits du Canada relatifs à la résiliation du contrat, le Canada peut immédiatement et sans autre avis résilier le contrat pour manquement, conformément aux conditions générales, si, à au moins trois reprises pendant la durée du contrat, l'entrepreneur n'a pas répondu ou n'a pas présenté une réponse valable à la suite de la réception d'un projet d'autorisation de tâches. Par souci de clarté, chaque projet d'autorisation de tâches, identifiable par son numéro de tâche, ne comptera que pour un seul cas. Une réponse valide s'entend d'une réponse donnée dans le délai requis et qui satisfait à toutes les exigences du projet d'autorisation de tâches, y compris la proposition du nombre requis de ressources possédant chacune l'expérience minimale et satisfaisant aux autres exigences des catégories indiquées dans le projet d'autorisation de tâches, selon un prix ne dépassant pas les taux établis à l'annexe B . Chaque fois que l'entrepreneur ne présente pas une réponse valide, l'entrepreneur convient que le Canada peut, à sa discrétion, réduire de 2 % la valeur minimale du contrat indiquée dans la clause intitulée « Garantie des travaux minimums ». Cette réduction sera confirmée, pour des raisons administratives seulement, par une modification au contrat apportée par l'autorité contractante (l'accord de l'entrepreneur n'est pas nécessaire).

7.3 Garantie des travaux minimums

(a) Dans la présente clause :

(i) La « **valeur maximale du contrat** » désigne le montant indiqué à la clause « **Limitation des dépenses** » du contrat.

(ii) La « **valeur minimale du contrat** » représente $20,000.00 (excluant les taxes applicables).

(b) En vertu du présent contrat, le Canada est tenu de demander des travaux pour un montant correspondant à la valeur minimale du contrat ou, à son choix, de payer l'entrepreneur à la fin du contrat conformément au paragraphe c), sauf pour les cas prévus au paragraphe d). En contrepartie de cette obligation, l'entrepreneur convient de se tenir prêt, pendant toute la période du contrat, à exécuter les travaux décrits dans le contrat. La responsabilité maximale du Canada à l'égard des travaux exécutés dans le cadre du contrat ne doit pas dépasser la valeur maximale du contrat, à moins d'une augmentation autorisée par écrit par l'autorité contractante.

(c) Si, pendant la durée du contrat, le Canada n'exige pas une quantité de travaux correspondant à la valeur minimale du contrat, il devra verser à l'entrepreneur la différence entre cette valeur et le coût total des travaux demandés.

(d) Conformément à cet article, le Canada n'aura aucune obligation à l'égard de l'entrepreneur si le Canada résilie l'ensemble du contrat :

(i) pour manquement;

(ii) pour des raisons pratiques à la suite de la décision ou de la recommandation d'un tribunal ou d'une cour, énonçant que le contrat peut être résilié, faire l'objet d'une autre demande de soumissions ou être attribué à un autre fournisseur;

(iii) pour des raisons de commodité dans les dix jours ouvrables suivant l'attribution du contrat.

7.4 Clauses et conditions uniformisées

Toutes les clauses et les conditions désignées par un numéro, une date et un titre sont énoncées dans le Guide des CCUA (https://achatsetventes.gc.ca/politiques-et-lignes-directrices/guide-des-clauses-et-conditions-uniformisees-d-achat), publié par Travaux publics et Services gouvernementaux Canada.

(a) **Conditions générales** :

(i) Le document 2035 (202-05-28), Conditions générales – besoins plus complexes de services, s'applique au contrat et en fait partie intégrante.

En ce qui concerne l'article 30, Résiliation pour raisons de commodité, des conditions générales 2035, la sous-section 04 est supprimée et remplacée par les sous-sections 04, 05 et 06 :

4. Les sommes auxquelles l'entrepreneur a droit selon le présent article et les sommes versées ou dues à l'entrepreneur ne doivent pas dépasser, au total, le prix contractuel.

5. Si l'autorité contractante résilie le contrat en totalité et que les articles de l'accord comprennent une garantie des travaux minimums, le montant total à verser à l'entrepreneur en vertu du contrat ne doit pas dépasser le plus élevé des deux montants suivants :

   (a) le montant total auquel a droit l'entrepreneur selon le présent article, en plus des montants qui lui ont été versés, des montants qui lui seront dus en plus des montants qui devront lui être payés en vertu de la garantie des travaux minimums, ou les montants qui lui sont dus à la date de la résiliation;

   (b) le montant payable selon la garantie des travaux minimums, moins les montants qui ont été versés, qui sont dus ou qui seront dus à l'entrepreneur à la date de la résiliation.

6. Sauf dans la mesure prévue au présent article, l'entrepreneur n'aura aucun recours, notamment en ce qui concerne les dommages-intérêts, la compensation, la perte de profit et l'indemnité découlant de tout avis de résiliation donné par le Canada en vertu du présent article. L'entrepreneur convient de rembourser immédiatement au Canada toute partie de tout paiement anticipé non liquidé à la date de la résiliation.

(b) **Conditions générales supplémentaires** :

Les conditions générales supplémentaires qui suivent :

(i) 4002 (2010-08-16), Conditions générales supplémentaires – Services d'élaboration ou de modification de logiciels;

(ii) 4007 (2010-08-16), Conditions générales supplémentaires – Le Canada détient les droits de propriété intellectuelle sur les renseignements originaux;

s'appliquent au contrat et en font partie intégrante.

7.5 Exigences relatives à la sécurité

Les exigences relatives à la sécurité suivantes (Liste de vérification des exigences relatives à la sécurité 19 et clauses connexes fournies par le Programme de sécurité des contrats), conformément à l'annexe B de l'arrangement en matière d'approvisionnement) EN578-170432 , s'appliquent au contrat et en font partie intégrante.

1. L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une cote de sécurité d'installation valable au niveau secret, délivrée par le Programme de Sécurité des Contrats (PSC), Travaux publics et Services gouvernementaux Canada (TPSGC)

2. Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens protégés/classifiés, ou à des établissements de travail dont l'accès est réglementé, doivent tous détenir une cote de sécurité du personnel valable au niveau fiabilité ou secret tel que requis, délivrée ou approuvée par le PSC, TPSGC

3. L'entrepreneur ou l'offrant ne doit pas emporter de renseignements protégés/classifiés hors des établissements de travail visés; et l'entrepreneur ou l'offrant doit s'assurer que son personnel est au courant de cette restriction et qu'il l'a respecte

4. Les contrats de sous-traitance comportant des exigences relatives à la sécurité ne doivent pas être attribués sans l'autorisation écrite préalable du PSC, TPSGC

5. L'entrepreneur ou l'offrant doit respecter les dispositions :
   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. du Manuel de la sécurité des contrats (dernière édition)

(a) En outre, les ressources peuvent être évaluées pour la cote de fiabilité ou Secret, ou une combinaison des deux, s'il y a lieu] par le responsable technique avant le début des travaux, et à l'occasion pendant la durée du contrat. L'évaluation peut comporter une vérification de la solvabilité. À la demande du responsable technique concernant toute ressource donnée, l'entrepreneur doit fournir :

(i) le niveau de l'autorisation de sécurité attribuée ou approuvée par la DSIC de TPSGC;

(ii) un formulaire SCT 330-23, Formulaire de vérification de sécurité, de consentement et d'autorisation du personnel, dûment rempli et signé (http://www.tbs-sct.gc.ca/tbsf-fsct/330-23-fra.pdf).

(b) Si une ressource ne répond pas aux critères d'évaluation du responsable technique, le Canada peut immédiatement, et sans autre avis, résilier le contrat pour manquement, conformément aux conditions générales.

7.6 Utilisation des équipements de protection individuelle et lignes directrices en matière de santé et de sécurité au travail (SST)

a) Le fournisseur doit se conformer aux exigences du Gouvernement du Canada en lien avec le port d'équipement(s) de protection individuelle sur les lieux de travail et de suivre à tout moment les directives SST en vigueur sur le lieu de travail.

b) Le fournisseur procurera à ses ressources l'équipement de protection individuelle suivant pour le travail sur site : masques prescrits couvrant le visage, gants, visière de protection, et tout autre équipement requis pour entrer ou travailler sur les lieux de travail du Gouvernement du Canada. Le Canada se réserve le droit de modifier la ligne directrice en matière de SST, au besoin, pour y inclure toute recommandation future proposée par les organismes de santé publique.

c) L'entrepreneur garantit que ses ressources suivront à tout moment les directives SST en vigueur sur le lieu de travail pendant la durée du contrat et que celles-ci porteront tout équipement de protection individuelle. Toute ressource qui ne porte pas l'équipement de protection individuelle et/ou qui ne suit pas les directives SST en vigueur sur le lieu de travail se verra refuser l'accès aux lieux de travail du Gouvernement du Canada.

7.7 Période du contrat

(a) **Période du contrat** : La « **période du contrat** » représente toute la période au cours de laquelle l'entrepreneur est obligé d'exécuter les travaux et comprend :

(i) la « **période initiale du contrat** » qui commence à la date d'attribution du contrat et qui prend fin 1 an plus tard;

(ii) la période de prolongation de ce contrat, si le Canada décide de se prévaloir des options énoncées dans le contrat.

(b) **Option de prolongation du contrat** :

(i) L'entrepreneur accorde au Canada l'option irrévocable de prolonger la durée du contrat pour au plus 2 période(s) supplémentaire(s) de 1 année chacune, selon les mêmes conditions. L'entrepreneur accepte, au cours de la période prolongée du contrat, d'être payé conformément aux dispositions applicables définies dans la base de paiement.

(ii) Le Canada peut exercer cette option à n'importe quel moment, en faisant parvenir un avis écrit à l'entrepreneur la date d'échéance du contrat. Cette option ne peut être exercée que par l'autorité contractante et sera confirmée, pour des raisons administratives seulement, par une modification au contrat.

7.8 Responsables

(a) Autorité contractante

L'autorité contractante dans le cadre du contrat est :

Nom : Sylvain Desbois
Titre : Spécialiste en approvisionnement
Travaux publics et Services gouvernementaux Canada
Direction de l'acquisition des services professionnels
Division des Services Professionnels ZV
Téléphone : 819-962-8660
Adresse électronique : sylvain.desbois@tpsgc-pwgsc.gc.ca

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 la réception de demandes ou d'instructions verbales ou écrites de toute personne autre que l'autorité contractante.

(b) **Responsable technique**
(insérer lors de l'attribution du contrat)

Le responsable technique pour le contrat est :

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____
Téléphone : _____
Télécopieur : _____
Adresse électronique : _____

Le responsable technique [représente le ministère ou l'organisme pour lequel les travaux sont exécutés en vertu du contrat, et il] est responsable de toutes les questions liées au contenu technique des travaux prévus dans le contrat. On peut discuter des questions techniques avec le responsable technique; cependant, celui-ci ne peut pas autoriser les changements touchant la

portée des travaux. De telles modifications ne peuvent être effectuées que par l'entremise d'une modification au contrat émise par l'autorité contractante**Représentant de l'entrepreneur**

En son absence

Le responsable technique pour le contrat est
(insérer lors de l'attribution du contrat)

Nom : _____
Titre : _____
Organisation : _____
Adresse : _____
Téléphone : _____
Télécopieur : _____
Adresse électronique : _____

(c) Représentant de l'entrepreneur
(insérer lors de l'attribution du contrat)

7.9 Divulgation proactive des contrats conclus avec d'anciens fonctionnaires

En fournissant des renseignements sur son statut d'ancien fonctionnaire touchant une pension en vertu de la *Loi sur la gestion de la fonction publique*, l'entrepreneur a convenu que ces renseignements seront affichés sur les sites Web ministériels, dans le cadre des rapports de divulgation proactive, conformément à l'Avis sur la politique des marchés 2012-2 du Secrétariat du Conseil du Trésor.

7.10 Paiement

(a) **Base de paiement**

i. **Services professionnels fournis dans le cadre d'une autorisation de tâches avec un prix maximum**: Pour les services professionnels exigés par le Canada, en conformité avec une autorisation de tâches émise de façon officielle, le Canada paiera à l'entrepreneur, rétroactivement, jusqu'à concurrence du prix maximum pour l'autorisation de tâches, pour les heures réellement travaillées ainsi que pour tout produit issu de ce travail conformément aux tarifs journaliers fermes tout compris établis à l'annexe B, Base de paiement, taxes applicables en sus. Les périodes de travail de moins d'une journée seront calculées proportionnellement aux heures travaillées en fonction d'une journée de travail de 7,5 heures

ii. **Services professionnels fournis dans le cadre d'une autorisation de tâches à un prix ferme** : Pour la prestation de services professionnels, sur demande par le Canada et conformément à une autorisation de tâches émise de façon officielle, le Canada paiera à l'entrepreneur le prix ferme établi dans l'autorisation de tâches (selon les tarifs journaliers fermes tout compris établis à l'annexe B), taxes applicables en plus

iii. **Frais de déplacement et de subsistance – Directive sur les voyages du Conseil national mixte :** L'entrepreneur sera remboursé pour les frais de déplacement et de subsistance autorisés qu'il a raisonnablement et convenablement engagés dans l'exécution des travaux, au prix coûtant, sans aucune indemnité pour les frais administratifs généraux ou le profit, conformément aux indemnités relatives aux repas et à l'utilisation d'un véhicule privé qui sont précisées aux appendices B, C et D de la Directive sur les voyages du Conseil national mixte, et selon les autres dispositions de la Directive qui font référence aux « voyageurs » plutôt qu'aux « employés ». Tout déplacement doit être approuvé au préalable par l`autorité technique

iv. **Attribution concurrentielle :** L'entrepreneur reconnaît que le contrat a été attribué à l'issue d'un processus concurrentiel. Aucun montant supplémentaire ne sera versé à l'entrepreneur en compensation d'erreurs, d'oublis ou de mauvaises interprétations ou estimations dans sa soumission.

v. **Taux quotidiens fermes de l'entrepreneur** : L'entrepreneur accepte que les taux énoncés dans l'annexe B demeurent fermes pendant toute la période du contrat, sauf pour ce qui est prévu dans les conditions expresses du contrat. En vertu de l'article 18(1) des Conditions générales 2035 du Guide des CCUA, l'entrepreneur reconnaît que son obligation de fournir les services conformément aux taux fermes énoncés à l'annexe B n'est pas visée par l'application d'une loi existante ou de toute nouvelle loi qui pourrait entrer en vigueur pendant la période du contrat.

vi. **Taux des services professionnels** : D'après l'expérience du Canada, les soumissionnaires proposeront parfois des taux pour une ou plusieurs catégories de ressources au moment de la soumission qu'ils refuseront plus tard de respecter, en affirmant que ces taux ne leur permettent pas de recouvrer les frais ou de rentabiliser leurs activités. Cela annule les avantages que le Canada aurait pu retirer de ce contrat. Si l'entrepreneur ne répond pas ou refuse de présenter une personne possédant les compétences décrites dans le contrat dans le délai prévu au contrat (ou qu'il propose plutôt de présenter quelqu'un d'une autre catégorie, à un taux différent), même si le Canada résilie le contrat en totalité ou en partie ou choisit de se prévaloir de ses droits en vertu des conditions générales, le Canada peut imposer des sanctions ou prendre des mesures conformément à la Politique sur les mesures correctives du rendement des fournisseurs (ou l'équivalent) de TPSGC en vigueur. Ces mesures peuvent comprendre une évaluation de laquelle peut découler l'imposition à l'entrepreneur de conditions qu'il devra respecter pour continuer à faire affaire avec le Canada ou une radiation complète de l'entrepreneur l'empêchant de soumissionner à l'avenir.

(b) **Limitation des dépenses – Total cumulatif de toutes les autorisations de tâche**

(i) La responsabilité totale du Canada envers l'entrepreneur dans le cadre du contrat pour toutes les autorisations de tâches émises de façon officielle, y compris toute modification, ne doit pas dépasser le montant énoncé à la page 1 du contrat, moins les taxes applicables. En ce qui concerne le montant inscrit à la première page du contrat, les droits de douane sont inclus, et les taxes applicables sont incluses.

(ii) Aucune augmentation de la responsabilité totale du Canada ne sera autorisée ou payée à l'entrepreneur, à moins qu'une augmentation n'ait été approuvée, par écrit, par l'autorité contractante.

(iii) L'entrepreneur doit informer, par écrit, l'autorité contractante concernant la suffisance de cette somme :

(A) lorsque 75 % de la somme est engagée; ou

(B) quatre mois avant la date d'expiration du contrat; ou

(C) dès que l'entrepreneur juge que la somme est insuffisante pour l'achèvement des travaux requis dans le cadre des autorisations de tâches autorisées, y compris toutes révisions,

selon la première éventualité.

(i) Lorsqu'il informe l'autorité contractante que les fonds du contrat sont insuffisants, l'entrepreneur doit lui fournir par écrit une estimation des fonds supplémentaires requis. La présentation de cette information par l'entrepreneur n'augmente pas la responsabilité du Canada à son égard.

(c) **Modalités de paiement pour les autorisations de tâches avec un prix maximum** : Pour chaque autorisation de tâches valide émise conformément au contrat et qui comprend un prix maximum :

(i) Le Canada paiera l'entrepreneur une fois par mois uniquement, conformément à la base de paiement. L'entrepreneur doit présenter des feuilles de présence pour chaque ressource, indiquant le nombre de jours et d'heures de travail effectués, pour justifier les montants réclamés sur la facture.

(ii) Une fois que le Canada aura payé le prix maximum pour l'autorisation de tâches, il n'aura plus à verser d'autres montants, mais l'entrepreneur devra achever les travaux décrits dans l'autorisation de tâches et correspondant au prix maximum de l'autorisation de tâches. Si les travaux décrits dans l'autorisation de tâches sont terminés plus tôt que prévu, et que leur coût (en fonction de la durée des travaux confirmée par les feuilles de présence), selon les tarifs établis dans le contrat, est inférieur au prix maximum de l'autorisation de tâches, le Canada ne sera tenu de payer que le temps consacré à la réalisation des travaux liés à l'autorisation de tâches.

(d) **Modalités de paiement pour les autorisations de tâches à prix ferme – Paiement forfaitaire à la fin des travaux** : Le Canada paiera l'entrepreneur lorsque les travaux liés à l'autorisation de tâches valide seront terminés et livrés conformément aux dispositions de paiement du contrat si :

(i) une facture exacte et complète ainsi que tout autre document exigé au contrat ont été présentés conformément aux instructions relatives à la facturation prévues au contrat;

(ii) tous ces documents ont été vérifiés par le Canada;

(iii) les travaux livrés ont été acceptés par le Canada.

(e) **Paiement électronique de factures – contrat**

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

(i) Carte d'achat Visa ;

(ii) Carte d'achat MasterCard ;

(iii) Dépôt direct (national et international) ;

(iv) Échange de données informatisées (EDI) ;

(v) Virement télégraphique (international seulement) ;

(vi) Système de transfert de paiements de grande valeur (plus de 25 M$)

***Remarque à l'intention des soumissionnaires** : Si applicable, le ou les instrument(s) de paiement électronique de factures indiqué(s) par le soumissionnaire à la pièce jointe 3.2 fera partie de tout contrat subséquent.*

(f) **Vérification du temps**

Le temps facturé et l'exactitude du système d'enregistrement du temps de l'entrepreneur peuvent faire l'objet d'une vérification par le Canada, avant ou après que l'entrepreneur a été payé. Si la vérification est effectuée après le paiement, l'entrepreneur s'engage à rembourser tout montant versé en trop, à la demande du Canada.

(g) **Crédits de paiement**

(i) **Incapacité de fournir une ressource** :

(A) Si l'entrepreneur ne peut fournir, dans le délai prescrit par le contrat, une ressource en services professionnels qui possède toutes les qualifications

demandées, l'entrepreneur doit verser au Canada un montant égal au tarif journalier (pour une journée de travail de 7,5 heures) de la ressource demandée pour chaque journée (ou portion de journée) de retard à fournir la ressource, jusqu'à un maximum de dix (10) jours.

(B) **Mesures correctives** : Si, conformément à cet article, les crédits sont applicables durant deux mois consécutifs ou durant trois mois sur une période de douze mois, l'entrepreneur doit présenter un plan d'action écrit décrivant les mesures qui seront prises pour éviter que le problème ne se produise de nouveau. L'entrepreneur aura cinq jours ouvrables pour présenter le plan d'action au client et à l'autorité contractante, et 20 jours ouvrables pour corriger le problème sous-jacent.

(C) **Résiliation pour non-respect du niveau de disponibilité** : Outre les autres droits qui lui sont conférés dans le cadre du contrat, le Canada peut résilier le contrat pour manquement, conformément aux conditions générales, en donnant à l'entrepreneur un avis écrit de trois (3) mois lui faisant part de son intention, si :

(1) le montant total de crédits pour un cycle de facturation mensuelle donné a atteint 10 % de la facture mensuelle; ou

(2) les mesures correctives présentées par l'entrepreneur, décrites ci-dessus, n'ont pas été prises.

La résiliation du contrat entrera en vigueur à la fin de la période de trois (3) mois, sauf si le Canada détermine que l'entrepreneur a mis en œuvre les mesures correctives de façon satisfaisante pendant cette période.

(ii) **Les crédits s'appliquent pendant toute la durée du contrat** : Les parties conviennent que les crédits s'appliquent pendant toute la durée du contrat.

(iii) **Crédits représentant des dommages-intérêts** : Les parties conviennent que les crédits sont des dommages-intérêts et qu'ils représentent la meilleure estimation préalable de la perte pour le Canada dans l'éventualité du manquement applicable. Les crédits ne sont pas une pénalité et ne doivent pas être considérés comme tels.

(iv) **Droit du Canada d'obtenir le paiement** : Les parties conviennent que ces crédits représentent une dette déterminée. Afin d'obtenir le paiement des crédits, le Canada est autorisé en tout temps à retenir, à recouvrer ou à déduire tout montant dû et impayé de toute somme due à l'entrepreneur par le Canada de temps à autre.

(v) **Droits et recours du Canada non limités** : Les parties conviennent que rien dans le présent article ne limite les droits ou les recours dont le Canada peut se prévaloir conformément au présent contrat (y compris le droit de résilier le contrat pour manquement) ou en vertu de la loi en général.

(vi) **Droits de vérification** : Le calcul de l'entrepreneur relatif aux crédits dans le cadre du contrat peut être vérifié par le service de vérification du gouvernement, à la discrétion de l'autorité contractante, avant ou après le versement du paiement à l'entrepreneur. L'entrepreneur doit coopérer entièrement avec le Canada au cours de la réalisation de toute vérification en permettant au Canada d'accéder à tous les documents et systèmes que le Canada juge nécessaires pour veiller à ce que tous les crédits aient été correctement imputés au Canada dans les factures de l'entrepreneur. Si une vérification démontre que des factures passées contiennent des erreurs de calcul des crédits, l'entrepreneur doit payer au Canada le montant, tel qu'il a été déterminé par la vérification, qui aurait dû être crédité au Canada, en plus des intérêts, à compter de la date à laquelle le Canada a versé le paiement excédentaire jusqu'à la date du remboursement (le taux d'intérêt est le taux officiel d'escompte par année de la Banque du Canada en vigueur à la date à laquelle le crédit était dû au Canada, plus 1,25 % par année). Si, à la suite d'une vérification, le Canada détermine que les documents ou les

systèmes de l'entrepreneur servant à déterminer, à calculer ou à enregistrer les crédits ne sont pas adéquats, l'entrepreneur devra mettre en œuvre toutes les mesures supplémentaires exigées par l'autorité contractante pour remédier au problème.

(h) **Aucune obligation de payer pour des travaux non effectués en raison de la fermeture des bureaux du gouvernement**

(i) Si l'entrepreneur, ses employés, ses sous-traitants ou ses représentants fournissent des services dans les locaux du gouvernement dans le cadre du contrat et que ces locaux ne sont pas accessibles en raison de l'évacuation, la fermeture ou l'implantation de mesures restreignant l'accès aux bureaux du gouvernement, et que le travail n'est pas effectué en raison de cette fermeture, le Canada n'a pas la responsabilité de payer l'entrepreneur pour le travail qu'il aurait exécuté s'il n'y avait pas eu de fermeture ou d'accès restreint aux bureaux.

(ii) Si l'entrepreneur, ses employés, ses sous-traitants ou ses agents ne peuvent accéder aux locaux du gouvernement où ils assurent des services en vertu du contrat en raison d'une grève ou d'un lock-out, et que cette situation les empêche de faire leur travail, le Canada n'est pas tenu de payer l'entrepreneur pour les travaux qui auraient pu être effectués s'il avait eu accès aux locaux.

7.11 Instructions relatives à la facturation

(a) L'entrepreneur doit soumettre ses factures conformément à l'information exigée dans les conditions générales.

(b) La facture de l'entrepreneur doit comporter un poste pour chaque sous-alinéa de la base de paiement, et elle doit porter les numéros d'autorisations de tâches applicables.

(c) En soumettant des factures, l'entrepreneur atteste que les biens et services ont été livrés et que tous les frais sont conformes aux dispositions de la base de paiement du contrat, y compris les frais résultant de l'exécution des travaux par des sous-traitants.

(d) L'entrepreneur doit remettre au responsable technique l'original de chaque facture, et une copie à *(insérer lors de l'attribution du contrat)* ***et*** 'autorité contractante.

7.12 Attestations

(a) Sauf indication contraire, le respect continu des attestations fournies par l'entrepreneur dans sa soumission ou avant l'attribution du contrat, toute proposition de prix relative aux autorisations de tâches et la coopération constante quant à la fourniture de renseignements supplémentaires sont des conditions du contrat, et le fait de ne pas les respecter constitue un manquement de la part de l'entrepreneur. Les attestations pourront faire l'objet de vérifications par le Canada pendant toute la durée du contrat.

7.13 Programme de contrats fédéraux pour l'équité en matière d'emploi – Manquement de la part de l'entrepreneur

L'entrepreneur comprend et convient que, lorsqu'il conclut un Accord pour la mise en œuvre de l'équité en matière d'emploi avec le Programme du travail d'Emploi et Développement social Canada, cet accord doit demeurer valide pendant toute la durée du contrat. Si cet accord devient invalide, le nom de l'entrepreneur sera ajouté à la « Liste d'admissibilité limitée à soumissionner au Programme de contrats fédéraux ». L'imposition d'une telle sanction par EDSC sera considéré non conforme aux modalités du contrat.

7.14 Lois applicables

Le contrat doit être interprété et régi selon les lois en vigueur en Ontario.*(insérer le nom de la province ou du territoire précisé par le soumissionnaire dans sa soumission, s'il y a lieu.)*, et les relations entre les parties doivent être déterminées par ces lois.

7.15 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 la convention, ainsi que les différentes clauses du Guide des CCUA qui sont incorporées par renvoi dans les articles de la convention;

(b) les conditions générales supplémentaires, selon l'ordre suivant :

(i) 4002 (2010-08-16), Conditions générales supplémentaires – Services d'élaboration ou de modification de logiciels,

(ii) 4007 (2010-08-16) Conditions générales supplémentaires – Le Canada détient les droits de propriété intellectuelle sur les renseignements originaux,

(c) les conditions générales 2035 *(insérer la date)* – besoins plus complexes de services;

(d) l'annexe A, Énoncé des travaux, y compris ses appendices, comme suit :

(i) Appendice A de l'annexe A- Procédures d'attribution de tâches,

(ii) Appendice B de l'annexe A– Formulaire d'autorisation de tâches,

(iii) Appendice C de l'annexe A– Critères d'évaluation des ressources et tableau de réponses,

(iv) Appendice D de l'annexe A Attestations à l'étape de l'autorisation de tâches;

(e) l'annexe B– Base de paiement;

(f) l'annexe C Liste de vérification des exigences relatives à la sécurité;

(g) les autorisations de tâches émises de façon officielle et toute attestation requise (y compris toutes les annexes, s'il y a lieu)

(h) la soumission de l'entrepreneur datée du _____ *(inscrire la date de la soumission) [si la soumission a été clarifiée ou modifiée, insérer au moment de l'attribution du contrat]*, « clarifiée le _____ » ou « modifiée le _____ » *(inscrire la ou les dates des clarifications ou modifications, le cas échéant).*

7.16 Ressortissants étrangers (entrepreneur canadien)

(a) Clause du guide des CCUA A2000C (2006-06-16) Ressortissants étrangers (entrepreneur canadien)

***Remarque à l'intention des soumissionnaires** : Cette clause ou la suivante (selon que le soumissionnaire retenu est un entrepreneur canadien ou un entrepreneur étranger) fera partie de tout contrat subséquent.*

7.17 Ressortissants étrangers (entrepreneur étranger)

(a) Clause du guide des CCUA A2001C (2006-06-16) Ressortissants étrangers (entrepreneur étranger)

7.18 Exigences en matière d'assurance

(a) **Conformité aux exigences en matière d'assurance**

(i) L'entrepreneur doit respecter les exigences en matière d'assurance énoncées dans le présent article. Il doit conserver la couverture exigée pendant toute la durée du contrat.

Le respect des exigences en matière d'assurance ne dégage pas l'entrepreneur de sa responsabilité en vertu du contrat ni ne la diminue.

(ii) L'entrepreneur doit décider si une couverture supplémentaire est nécessaire pour remplir ses obligations en vertu du contrat et se conformer aux lois applicables. Toute couverture supplémentaire est à la charge de l'entrepreneur et souscrite pour son bénéfice et sa protection.

(iii) L'entrepreneur devrait faire parvenir à l'autorité contractante, dans les dix (10) jours suivant la date d'attribution du contrat, un certificat d'assurance montrant la couverture d'assurance. L'assurance doit être souscrite auprès d'un assureur autorisé à faire affaire au Canada, et le certificat d'attestation d'assurance doit confirmer que la police d'assurance satisfaisant aux exigences est en vigueur. Si le certificat d'attestation d'assurance n'est pas rempli et fourni comme il est demandé, l'autorité contractante en informera l'entrepreneur et lui donnera un délai afin de se conformer aux exigences. Le défaut de répondre à la demande de l'autorité contractante et de se conformer aux exigences dans les délais prévus sera considéré comme un manquement aux conditions générales. L'entrepreneur doit, à la demande de l'autorité contractante, transmettre au Canada une copie certifiée conforme de toutes les polices d'assurance applicables.

(b) **Assurance responsabilité civile commerciale**

(i) L'entrepreneur doit souscrire et maintenir pendant toute la durée du contrat une police d'assurance responsabilité civile des entreprises d'un montant équivalant à celui habituellement fixé pour un contrat de cette nature; toutefois, la limite de responsabilité ne doit pas être inférieure à 2 000 000 $ par accident ou par incident et suivant le total annuel.

(ii) La police d'assurance responsabilité civile commerciale doit comprendre les éléments suivants :

(A) Assuré additionnel : Le Canada est désigné comme assuré additionnel, mais seulement en ce qui concerne les responsabilités qui peuvent découler de l'exécution du contrat par l'entrepreneur. L'intérêt du Canada devrait se lire comme suit : Le Canada, représenté par Travaux publics et Services gouvernementaux Canada.

(B) Blessures corporelles et dommages matériels causés à des tiers découlant des activités de l'entrepreneur.

(C) Produits et activités réalisées : Couverture pour les blessures corporelles ou les dommages matériels découlant de biens ou de produits fabriqués, vendus, manipulés ou distribués par l'entrepreneur, ou découlant des activités réalisées par l'entrepreneur.

(D) Préjudices personnels : La couverture devrait inclure notamment la violation de la vie privée, la diffamation verbale ou écrite, l'arrestation illégale, la détention ou l'incarcération et la diffamation.

(E) Responsabilité réciproque/séparation des assurés : Sans augmenter la limite de responsabilité, la police doit couvrir toutes les parties assurées dans les limites prévues par la couverture. De plus, la police doit s'appliquer à chaque assuré de la même manière et dans la même mesure que si une police distincte avait été établie pour chacun d'eux.

(F) Responsabilité contractuelle générale : La police doit, sur une base générale ou par renvoi explicite au présent contrat, couvrir les obligations assumées en ce qui concerne les dispositions d'assurance contractuelle.

(G) Les employés et, le cas échéant, les bénévoles doivent être désignés comme assurés additionnels.

(H) Responsabilité de l'employeur (ou confirmation que tous les employés sont protégés par la Commission de la sécurité professionnelle et de l'assurance contre les accidents du travail ou par un programme semblable).

(I) Formule étendue d'assurance contre les dommages, comprenant les activités accomplies : La police doit prévoir la couverture des dommages matériels de manière à inclure certains sinistres qui seraient autrement exclus en vertu de la clause d'exclusion usuelle de garde, de contrôle ou de responsabilité faisant partie d'une police d'assurance standard.

(J) Avis d'annulation : L'assureur s'efforcera de donner à l'autorité contractante un avis écrit de trente (30) jours en cas d'annulation de la police.

(K) S'il s'agit d'une police sur la base des réclamations, la couverture doit être valide pour une période minimale de douze (12) mois suivant la fin ou la résiliation du contrat.

(L) Responsabilité civile indirecte du propriétaire ou de l'entrepreneur : Couvre les dommages découlant des activités d'un sous-traitant que l'entrepreneur est juridiquement responsable de payer.

(M) Préjudices découlant de la publicité : L'avenant doit notamment inclure le piratage ou l'appropriation illicite d'idées, ou la violation de droits d'auteur, de marques de commerce, de titres ou de slogans.

(c) **Assurance responsabilité contre les erreurs et les omissions**

(i) L'entrepreneur doit souscrire et maintenir pendant toute la durée du contrat une assurance responsabilité contre les erreurs et les omissions (également appelée assurance responsabilité civile professionnelle) d'un montant équivalant à celui habituellement fixé pour un contrat de cette nature; toutefois, la limite de responsabilité ne doit pas être inférieure à 1 000 000 $ par perte et suivant le total annuel, y compris les frais de défense.

(ii) S'il s'agit d'une assurance responsabilité professionnelle sur la base des réclamations, la couverture doit être valide pour une période minimale de douze (12) mois suivant la fin ou la résiliation du contrat.

(iii) L'avenant suivant doit être compris :

Avis d'annulation : L'assureur s'efforcera de donner à l'autorité contractante un avis écrit de trente (30) jours en cas d'annulation de la police.

7.19 Limitation de la responsabilité – Gestion de l'information/technologie de l'information

(a) Le présent article s'applique malgré toute autre disposition du contrat et remplace l'article des conditions générales intitulé « Responsabilité ». Toute mention dans le présent article de dommages causés par l'entrepreneur comprend les dommages causés par ses employés, ainsi que ses sous-traitants, ses mandataires et ses représentants, ainsi que leurs employés. Le présent article s'applique, que la réclamation soit fondée contractuellement sur un délit civil ou un autre motif de poursuite. L'entrepreneur n'est pas responsable envers le Canada de l'exécution ou de la non-exécution du contrat, sauf dans les cas précisés dans le présent article et dans tout autre article du contrat préétablissant des dommages-intérêts. L'entrepreneur est uniquement responsable des dommages indirects, particuliers ou consécutifs, dans la mesure décrite dans le présent article, même si l'entrepreneur a été avisé de la possibilité de ces dommages.

(b) **Responsabilité de première partie** :

(i) L'entrepreneur est entièrement responsable envers le Canada de tous les dommages, y compris les dommages indirects, particuliers ou consécutifs, causés par l'exécution ou la non-exécution du contrat par l'entrepreneur et qui se rapportent à :

(A) toute violation des droits de propriété intellectuelle, dans la mesure où l'entrepreneur viole l'article des conditions générales intitulé « Atteinte aux droits de propriété intellectuelle et redevances »;

(B) toute blessure physique, y compris la mort.

(ii) L'entrepreneur est responsable de tous les dommages directs causés par l'exécution ou la non-exécution du contrat et touchant des biens personnels ou des biens immobiliers qui appartiennent au Canada ou qui sont occupés par celui-ci.

(iii) Chaque partie est responsable de tous les dommages directs causés par son manquement à l'obligation de confidentialité dans le cadre du contrat. Chaque partie est également responsable de tous les dommages indirects, particuliers ou consécutifs relatifs à sa divulgation non autorisée de secrets de fabrication de l'autre partie (ou des secrets de fabrication d'un tiers fournis par une partie à une autre aux termes du contrat) ayant trait à la technologie de l'information.

(iv) L'entrepreneur est responsable de tous les dommages directs qui se rapportent à une charge ou à une réclamation liée à toute portion des travaux pour lesquels le Canada a effectué un paiement. Cette disposition ne s'applique pas aux charges ou réclamations relatives aux droits de propriété intellectuelle, lesquelles sont traitées au sous-alinéa (i)(A) susmentionné.

(v) L'entrepreneur est également responsable de tout autre dommage direct causé au Canada par l'exécution ou la non-exécution du contrat par l'entrepreneur et qui se rapporte à :

(A) tout manquement aux obligations en matière de garantie en vertu du contrat, jusqu'à concurrence du coût total payé par le Canada (y compris toute taxe applicable) pour les biens et les services touchés par le manquement;

(B) tout autre dommage direct, y compris tous les frais directs identifiables afférents au Canada pour faire appel à une autre partie dans le cadre des travaux si le contrat est résilié en totalité ou en partie pour non-exécution, jusqu'à concurrence d'un maximum global correspondant à la plus élevée des deux valeurs suivantes pour l'application de ce sous-alinéa (B) : 75 % du coût total estimatif (le montant indiqué à la première page du contrat dans la case intitulée « Coût total estimatif » ou le montant indiqué sur chaque commande subséquente, bon de commande ou tout autre document utilisé pour commander des biens ou des services dans le cadre du présent instrument), ou 1 000 000 $.

En aucun cas, la responsabilité totale de l'entrepreneur aux termes de l'alinéa (v) ne dépassera le montant le plus élevé entre le coût total estimatif (comme défini plus haut) du contrat ou 1 000 000 $.

(vi) 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. Ce dernier doit s'assurer de sauvegarder adéquatement ses documents et ses données.

(c) **Réclamations de tiers** :

(i) Que la réclamation soit faite au Canada ou à l'entrepreneur, chaque partie convient qu'elle est responsable des dommages qu'elle cause à tout tiers relativement au contrat, tel que stipulé dans un accord de règlement ou ultimement déterminé par une cour compétente, si la cour détermine que les parties sont conjointement et solidairement responsables ou qu'une seule partie est uniquement et directement responsable envers le tiers. Le montant de la responsabilité sera celui précisé dans l'accord de règlement ou déterminé par le tribunal comme ayant été la portion des dommages que la partie a

causés au tiers. Aucun accord de règlement ne lie une partie, sauf si ses représentants autorisés l'ont approuvé par écrit.

(ii) Si le Canada doit, en raison d'une responsabilité conjointe et individuelle ou d'une responsabilité conjointe et solidaire, payer un tiers pour des dommages causés par l'entrepreneur, l'entrepreneur doit rembourser au Canada le montant ultimement déterminé par un tribunal compétent comme étant la portion de l'entrepreneur des dommages qu'il a lui-même causés au tiers. Toutefois, malgré l'alinéa (i), lequel concerne les dommages-intérêts spéciaux, indirects ou consécutifs subis par des tiers et couverts par le présent article, l'entrepreneur est uniquement responsable de rembourser au Canada la portion des dommages qu'il a causés sur le montant total que doit verser le Canada à un tiers sur ordre d'un tribunal, en raison d'une responsabilité conjointe et individuelle relativement à la violation des droits de propriétés intellectuelles; de blessures physiques, y compris la mort; des dommages touchant les biens personnels matériels ou immobiliers d'un tiers; toute charge ou tout privilège sur toute portion des travaux; ou du non-respect de la confidentialité.

(iii) Les parties sont uniquement responsables l'une envers l'autre des dommages causés à des tiers dans la mesure décrite dans le paragraphe (c).

7.20 Entrepreneur en coentreprise *(supprimer si non-applicable)*

(a) L'entrepreneur confirme que le nom de la coentreprise est _____ et qu'elle est formée des membres suivants : *[énumérer les membres de la coentreprise nommés dans la soumission originale de l'entrepreneur]*.

(b) Pour ce qui est des rapports entre les membres de cette coentreprise, chacun d'eux adopte les conventions, fait les déclarations et offre les garanties suivantes (le cas échéant) :

(i) _____ a été nommé en tant que « membre représentant » de la coentreprise et est pleinement habilité à intervenir à titre de mandataire de chacun des membres de cette coentreprise pour ce qui est de toutes les questions se rapportant au présent contrat;

(ii) en informant le membre représentant, le Canada sera réputé avoir informé tous les membres de cette coentreprise;

(iii) toutes les sommes versées par le Canada au membre représentant seront réputées avoir été versées à tous les membres.

(c) Tous les membres conviennent que le Canada peut, à sa discrétion, résilier le contrat en cas de conflit entre les membres lorsque, de l'avis du Canada, ce conflit nuit d'une manière ou d'une autre à l'exécution des travaux.

(d) Tous les membres de la coentreprise sont conjointement et individuellement ou solidairement responsables de l'exécution du contrat en entier.

(e) L'entrepreneur reconnaît que toute modification apportée à la composition de la coentreprise (soit un changement dans le nombre de ses membres ou la substitution d'une autre personne morale à un membre existant) constitue une cession et est soumise aux dispositions des conditions générales du contrat.

(f) L'entrepreneur reconnaît que, le cas échéant, toutes les exigences contractuelles relatives aux biens contrôlés et à la sécurité s'appliquent à chaque membre de la coentreprise.

Remarque à l'intention des soumissionnaires : *Le présent article sera supprimé si le soumissionnaire auquel on attribue le contrat n'est pas une coentreprise. Si l'entrepreneur est une coentreprise, cette clause sera complétée par l'information de sa soumission.*

7.21 Services professionnels – Généralités

(a) L'entrepreneur doit fournir des services professionnels sur demande, tels qu'ils sont précisés dans le présent contrat. Toutes les ressources fournies par l'entrepreneur doivent posséder les compétences décrites dans le contrat (notamment celles relatives à l'expérience, aux titres professionnels, aux études, aux aptitudes linguistiques et à la cote de sécurité) et être capables de fournir les services exigés selon les échéances précisées dans le contrat.

(b) Si l'entrepreneur ne livre pas les produits livrables (à l'exception d'une personne précise) ou n'effectue pas les tâches décrites dans le contrat dans les délais prescrits, en plus de ne pas se conformer à tout autre droit ou recours dont le Canada peut se prévaloir en vertu du contrat ou de la loi, le Canada peut informer l'entrepreneur du manquement et peut exiger que ce dernier fournisse au responsable technique, dans les dix (10) jours ouvrables, un plan écrit décrivant les mesures que l'entrepreneur entend prendre pour remédier au problème. L'entrepreneur doit préparer le plan et le mettre en œuvre à ses frais.

(c) L'article intitulé « Remplacement d'individus spécifiques » des conditions générales 2035 a été supprimé et remplacé par ce qui suit :

Remplacement d'individus spécifiques

(i) Si l'entrepreneur n'est pas en mesure de fournir les services d'une personne en particulier désignée dans le contrat pour exécuter les travaux, il doit, dans les cinq jours ouvrables suivant la réception de l'avis concernant le départ de la personne en question ou son incapacité à entamer les travaux (ou si le Canada en a demandé le remplacement, dans les dix jours ouvrables suivant la remise d'un avis à cet effet), fournir à l'autorité contractante ce qui suit :

(A) le nom, les qualifications et l'expérience d'un remplaçant proposé disponible immédiatement;

(B) les renseignements de sécurité sur le remplaçant proposé exigés par le Canada, s'il y a lieu.

Les qualifications et l'expérience du remplaçant doivent être équivalentes ou supérieures à celles de la ressource initiale.

(ii) Sous réserve d'un retard justifiable, lorsque le Canada constate qu'une personne désignée dans le contrat pour fournir les services n'a pas été mise à disposition ou ne réalise pas les travaux, l'autorité contractante peut choisir :

(A) de revendiquer les droits du Canada ou d'exercer un recours en vertu du contrat ou de la loi, y compris de résilier le contrat en totalité ou en partie, pour manquement, en vertu de l'article intitulé « Manquement de la part de l'entrepreneur »;

(B) d'évaluer les renseignements fournis en vertu du sous-alinéa *c*)(i) ci-dessus ou, s'ils n'ont pas encore été fournis, d'exiger que l'entrepreneur propose un remplaçant que le responsable technique devra évaluer. Les compétences et l'expérience du remplaçant doivent être équivalentes ou supérieures à celles de la ressource initiale et être jugées satisfaisantes par le Canada. Une fois le remplaçant évalué, le Canada pourra l'accepter, exercer les droits décrits à la division (ii)(A) ci-dessus ou encore exiger qu'on lui propose un autre remplaçant en vertu de l'alinéa *c*).

En cas de retard justifiable, le Canada pourra exercer les options décrites à la division c)(ii)(B) ci-dessus au lieu de résilier le contrat en vertu de l'article « Retard justifiable ». La non-disponibilité d'une ressource en raison d'une affectation à un autre contrat ou projet (y compris ceux de l'État) exécuté par l'entrepreneur ou l'une de ses sociétés affiliées ne constitue pas un retard justifiable.

(iii) L´entrepreneur ne doit en aucun cas permettre que les travaux soient exécutés par des remplaçants non autorisés. L'autorité contractante peut ordonner qu'une ressource originale ou qu'un remplaçant cesse d'exécuter les travaux. L'entrepreneur doit alors se conformer sans délai à cet ordre. Le fait que l'autorité contractante n'ordonne pas qu'une ressource cesse d'exécuter les travaux n'a pas pour effet de relever l'entrepreneur de son obligation de satisfaire aux exigences du contrat.

(iv) Les obligations énoncées dans le présent article s'appliquent en dépit des changements que le Canada pourrait avoir apportés au contexte opérationnel du client.

7.22 Services professionnels pour un logiciel existant

(a) **Logiciels existants** : Les « **logiciels existants** » sont des programmes informatiques énumérés à l'annexe A qui appartiennent au Canada ou que le Canada a le droit d'utiliser en vertu d'une licence émise par une tierce partie, et pour lesquels le Canada a besoin de certains services professionnels.

(b) **Services relatifs aux logiciels** : Au cours de la période contractuelle, l'entrepreneur doit fournir au client les « **services relatifs aux logiciels existants** » suivants, selon la demande du Canada, par l'entremise d'une autorisation de tâches :

(i) accès, téléchargement, sauvegarde, installation, chargement, traitement, configuration et mise en œuvre relativement à tout code de logiciel supplémentaire applicable aux logiciels existants (comme les nouvelles éditions, les nouvelles versions, les correctifs et les corrections de bogues), dès qu'ils sont disponibles;

(ii) suivi des versions de logiciels diffusées par l'éditeur de logiciel dans le but de contrôler la configuration;

(c) **Aucune activité de développement de logiciel** : L'entrepreneur n'est pas tenu de développer, de programmer ou de fournir des codes de logiciel supplémentaires liés aux logiciels existants à l'égard des travaux exécutés dans le cadre du contrat.

(d) **Titre** : Sauf indication contraire dans les articles de la présente entente, le titre de propriété des logiciels existants ne sera pas touché par la prestation des services relatifs à ceux-ci. De plus, dans la mesure où un tiers doit avoir une licence pour les utiliser, leur utilisation demeurera assujettie aux modalités de la licence du Canada.

(e) **Accès** : Le Canada fournira à l'entrepreneur les renseignements sur les mots de passe et les codes d'autorisation ou d'autres renseignements semblables qui pourraient se révéler nécessaires pour la prestation des services de logiciels, pourvu que le Canada respecte les obligations sur l'utilisation des logiciels existants. L'entrepreneur convient que la non-divulgation et la non-diffusion du contenu des logiciels existants à une autre personne ou entité constituent des modalités du contrat. Il convient aussi de ne violer d'aucune façon les droits de propriété des logiciels existants.

7.23 Préservation des supports électroniques

(a) Avant de les utiliser sur l'équipement du Canada ou de les envoyer au Canada, l'entrepreneur doit utiliser un produit régulièrement mis à jour pour balayer les supports électroniques utilisés pour exécuter les travaux afin de s'assurer qu'ils ne contiennent aucun virus informatique ou code malveillant. L'entrepreneur doit informer aussitôt le Canada si un support électronique utilisé pour les travaux renferme des virus informatiques ou autres codes malveillants.

(b) Si des renseignements ou des documents électroniques sont endommagés ou perdus pendant que l'entrepreneur en a la garde ou en tout temps avant qu'ils ne soient remis au Canada conformément au contrat, y compris en cas d'effacement accidentel, l'entrepreneur doit les remplacer immédiatement à ses frais.

7.24 Exigences relatives à la production de rapports

L'entrepreneur doit remettre à l'autorité contractante les rapports suivants aux dates précisées ci-après :

- Les rapports trimestriels d'utilisation périodique

De plus, l'entrepreneur doit remttre les rapports suivants au responsable technique :

- Rapports de suivi des anomalies, des demandes de changement et des questions en suspens;
- Rapports mensuels d'avancement du projet ;
- Guides, manuels et rapports à distribuer aux divers intervenants, au besoin;
- Rapport de synthèse des réunions avec animateur;
- Rapports d'activités;
- Notes de conversations, documentation sur la conception et sur la gestion du changement, rapports d'inspection du site et autres travaux demandés dans l'autorisation de tâches.

7.25 Déclarations et garanties

Dans sa soumission, l'entrepreneur a fait des déclarations à propos de sa propre expérience et expertise et de celles des ressources qu'il propose qui ont donné lieu à l'attribution du contrat [et à l'émission d'autorisations de tâches]. L'entrepreneur déclare et certifie que toutes ces déclarations sont véridiques et reconnaît que le Canada s'est fondé sur ces déclarations pour lui attribuer le contrat [et lui assigner des travaux par l'intermédiaire des autorisations de tâches]. De plus, l'entrepreneur déclare et certifie qu'il a et qu'il aura et maintiendra pendant la durée du contrat, ainsi que tout le personnel et les sous-traitants qui effectueront les travaux, les compétences, l'expérience et l'expertise nécessaires pour mener à bien les travaux conformément au contrat et qu'il a (ainsi que le personnel et les sous-traitants) déjà rendu de pareils services à d'autres clients.

7.26 Accès aux biens et aux installations du Canada

Les biens, les installations, le matériel, la documentation et le personnel du Canada ne sont pas forcément mis automatiquement à la disposition de l'entrepreneur. S'il veut y avoir accès, il doit en faire la demande au responsable technique. Sauf indication contraire à cet effet dans le contrat, le Canada n'est pas tenu de fournir à l'entrepreneur l'une ou l'autre des ressources précitées. Si le Canada choisit, à sa discrétion, de mettre ses installations, son matériel, sa documentation et son personnel à la disposition de l'entrepreneur pour effectuer les travaux, il peut exiger une modification de la base de paiement, et des exigences supplémentaires en matière de sécurité peuvent s'appliquer.

7.27 Propriété du gouvernement

Le Canada consent à fournir à l'entrepreneur les articles énumérés ci-dessous (les « **biens du gouvernement** »). La section des conditions générales intitulée « Biens du gouvernement » s'applique aussi à l'utilisation de ces biens par l'entrepreneur.

(a) Voir Annex A

7.28 Règlement des différends

(a) Les parties conviennent de maintenir une communication ouverte et honnête concernant les travaux pendant toute la durée de l'exécution du marché et après.

(b) Les parties conviennent de se consulter et de collaborer dans l'exécution du marché, d'informer rapidement toute autre partie des problèmes ou des différends qui peuvent survenir et de tenter de les résoudre.

(c) Si les parties n'arrivent pas à résoudre un différend au moyen de la consultation et de la collaboration, les parties conviennent de consulter un tiers neutre offrant des services de règlement extrajudiciaire des différends pour tenter de régler le problème.

(d) Vous trouverez des choix de services de règlement extrajudiciaire des différends sur le site Web Achats et ventes du Canada sous le titre « Règlement des différends ».

7.29 Responsabilités relatives au protocole d'identification

L'entrepreneur doit s'assurer que chacun de ses agents, représentants ou sous-traitants (appelés ci-après représentants de l'entrepreneur) respecte les exigences d'auto-identification suivantes :

a) Les représentants de l'entrepreneur qui assistent à une réunion du gouvernement du Canada (à l'intérieur ou à l'extérieur de bureaux du Canada) doivent s'identifier en tant que représentants de l'entrepreneur avant le début de la réunion afin de garantir que chaque participant à la réunion est au courant du fait que ces personnes ne sont pas des employés du gouvernement du Canada.

b) Pendant l'exécution de tout travail sur un site du gouvernement du Canada, chaque représentant de l'entrepreneur doit être clairement identifié comme tel, et ce, en tout temps.

c) Si un représentant de l'entrepreneur doit utiliser le système de courriel du gouvernement du Canada dans le cadre de l'exécution des travaux, il doit clairement s'identifier comme étant un agent ou un sous-traitant de l'entrepreneur dans le bloc de signature de tous les messages électroniques qu'il enverra ainsi que dans la section « Propriété ». De plus, ce protocole d'identification doit être utilisé pour toute autre correspondance, communication et documentation.

d) Si le Canada détermine que l'entrepreneur a contrevenu à n'importe laquelle de ses obligations en vertu du présent article, l'entrepreneur doit, à la suite d'un avis écrit du Canada, présenter un plan d'action écrit décrivant les mesures qui seront prises pour éviter que le problème ne se produise de nouveau. L'entrepreneur aura cinq (5) jours ouvrables pour présenter le plan d'action au client et à l'autorité contractante, et vingt (20 jours ouvrables pour corriger la source du problème.

e) En plus de tous ses autres droits dans le cadre du contrat, le Canada peut résilier le contrat pour manquement si l'entrepreneur ne respecte pas les mesures correctives décrites ci-dessus.

ANNEXE A
ÉNONCÉ DES TRAVAUX

1. Titre

Services professionnels de cybersécurité des technologies de l'information (TI)

2. Objectif

L'Agence des services frontaliers du Canada (ASFC) veut retenir les services d'une organisation pour fournir des ressources professionnelles de cybersécurité en GI-TI possédant une expertise particulière dans le domaine de la conformité et de la sécurité du nuage public et des technologies émergentes, conformément à la description détaillée du présent énoncé des travaux.

Les documents *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*[1]*,* du Centre canadien pour la cybersécurité, et *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage*, du gouvernement du Canada (GC), prévoient les activités suivantes :

- effectuer la catégorisation de la sécurité (sur le plan de la confidentialité, de l'intégrité et de la disponibilité) de chaque service du GC déployé dans un service d'informatique en nuage;
- sélectionner un ensemble approprié de mesures de sécurité en fonction de la catégorie de sécurité du service du GC;
- sélectionner le bon modèle de déploiement et le bon modèle de service d'informatique en nuage pour le service du GC;
- évaluer la mise en œuvre des mesures de sécurité à l'appui du service d'informatique en nuage;
- mettre en œuvre les mesures de sécurité exigées dans le service du GC;
- évaluer la mise en œuvre des mesures de sécurité dans le service du GC;
- autoriser les opérations du service d'informatique en nuage du GC résultant;
- surveiller continuellement la sécurité du service d'informatique en nuage du GC durant l'étape du fonctionnement;
- tenir à jour l'état d'autorisation du service d'informatique en nuage du GC.

Cette approche et les procédures sous-jacentes aident à faire en sorte que les fournisseurs de services d'informatique en nuage (FSI) comprennent les exigences de sécurité du GC, et que les ministères et organismes du GC (ou les organisations consommatrices du GC) et les FSI comprennent leur responsabilité partagée dans la mise en place de mesures de sécurité assez rigoureuses pour permettre l'hébergement des services du GC et de l'information connexe dans divers environnements de nuage.

Ce marché permettra de veiller à ce que les solutions infonuagiques et celles reposant sur des technologies émergentes qui sont utilisées par l'ASFC soient protégées contre les cyberattaques et le vol de données et à ce qu'elles soient toujours pleinement conformes à l'approche de gestion des risques ITSG-33 du gouvernement du Canada, aux lignes directrices du GC relatives à la sécurité infonuagique et aux normes, directives, alertes et avis du Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications (CST).

[1] Élaboré avant la création du Centre canadien pour la cybersécurité par l'une des entités qui en font aujourd'hui partie. Ce contenu demeure pertinent dans le cadre des discussions actuelles touchant la cybersécurité.

3. Contexte

Le mandat de l'Agence des services frontaliers du Canada (ASFC) consiste à fournir des services frontaliers intégrés à l'appui des priorités en matière de sécurité nationale et de sécurité publique et faciliter la libre circulation des personnes et des marchandises à travers la frontière canadienne. Les technologies de l'information (TI) sont cruciales pour s'acquitter de l'obligation de l'Agence d'administrer plus de 90 lois, règlements et accords internationaux.

Vu la nature de ses activités, l'ASFC doit recueillir et utiliser de l'information sur les voyageurs et les biens qui traversent la frontière canadienne, laquelle peut être de nature délicate et confidentielle. Nous sommes responsables de cette information, et sa gestion requiert l'adoption de mesures et de processus rigoureux de protection des renseignements personnels et de sécurité.

L'ASFC a pris des engagements envers la modernisation et le renouvellement, tant à l'interne (grâce à son programme de renouvellement[2]) que dans le cadre d'ententes conclues avec des partenaires, notamment le « Border Five », un forum international sur les enjeux stratégiques touchant la gestion des douanes et des frontières à laquelle participent l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.

Avant que l'Organisation mondiale de la Santé déclare la pandémie de COVID-19 en mars 2020, l'ASFC, conformément à son programme de renouvellement, s'efforçait de tirer parti de technologies novatrices au moyen d'une approche graduelle en vue d'amorcer la migration d'un grand nombre de ses plus de 180 applications traditionnelles gérées par Services partagés Canada (SPC) vers un environnement d'hébergement moderne dans le nuage. Selon la cible établie, 25 % des applications nationales actuelles de l'ASFC vont passer au nuage d'ici la fin de mars 2022. La modernisation des applications de l'ASFC et leur migration vers le nuage apporteront de nombreux avantages à l'Agence, ainsi qu'à la sécurité du pays.

Cependant, la pandémie a poussé l'ASFC à apporter un certain nombre de changements importants à ses projets en accroissant sa présence dans le nuage et en tirant parti d'autres technologies émergentes pour réagir d'urgence et remplir promptement de nouvelles exigences imposées par la situation, comme le suivi des renseignements sur les voyageurs tenus de s'isoler en application des décrets d'urgence en vertu de la *Loi sur la quarantaine*, et pour composer avec une hausse importante des volumes d'importation de marchandises commerciales de faible valeur.

Le travail accompli par l'ASFC dans le cadre de son programme de renouvellement en vue d'accélérer la mise en place des nouvelles technologies et des environnements infonuagiques était essentiel pour favoriser la réaction rapide de l'Agence jusqu'à maintenant, mais ces nouveaux outils et ces nouvelles façons de faire soulèvent des risques complexes et mal connus qui mettent à rude épreuve l'expertise et les capacités actuelles des ressources de sécurité des TI de l'Agence, en raison notamment de lacunes en ce qui concerne la connaissance et la maîtrise de nouvelles technologies.

Ces lacunes pourraient accroître l'exposition de l'Agence à des risques liés à la technologie. Parmi ces risques, mentionnons les suivants : vices de conformité (c.-à-d. ne pas respecter les exigences émanant de la réglementation ou de politiques); vols d'identité; infections par un logiciel malveillant et atteintes à la protection des données; baisse de la confiance du public; et pertes financières. Chaque

[2] Voir *Cahier de transition du premier vice-président 2019 : Direction générale de la politique stratégique (DGPS), Cadre stratégique international pour l'année financière de 2019 à 2022.*

technologie apporte son lot de risques et de vulnérabilités uniques et complexes. Vu les nombreuses menaces potentielles liées à l'hémisphère numérique, la gestion du cyberrisque doit être dynamique et s'adapter continuellement à l'évolution du paysage de menace.

Afin de pouvoir maintenir cette nouvelle cadence et réagir de façon sécuritaire, mais rapide, à de nouvelles situations, à de nouveaux volumes et à d'autres impondérables, l'ASFC a besoin de services professionnels de cybersécurité pour composer avec les vulnérabilités en matière de cybersécurité et assurer la protection des données privées et confidentielles des citoyens et entreprises du Canada et d'ailleurs.

4. Documents de référence

Gouvernement du Canada, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*
https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie.

Gouvernement du Canada, *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage*
https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/approche-procedures-gestion-risques-securite-informatique-nuage.html.

Centre canadien pour la cybersécurité, *Directives*
https://cyber.gc.ca/fr/directives.

Gouvernement du Canada, *Orientation relative à la résidence des données électroniques* (AMPTI 2017-02, archivé)
https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-relative-residence-donnees-electroniques.html.

Cahier de transition du premier vice-président 2019 : Direction générale de la politique stratégique (DGPS), *Cadre stratégique international pour l'année financière de 2019 à 2022*
https://www.cbsa-asfc.gc.ca/pd-dp/tb-ct/evp-pvp/spb-dgps-isf-csi-fra.html#04-1.

Stratégie nationale de cybersécurité
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx.

Loi sur l'accessibilité pour les personnes handicapées de l'Ontario (LAPHO) – Normes d'accessibilité intégrées
https://www.ontario.ca/fr/page/propos-des-lois-sur-laccessibilite.

Municipalité d'East Gwillimbury — Normes d'accessibilité pour le service à la clientèle [Disponible en anglais seulement].
http://www.eastgwillimbury.ca/About_Us/About_the_Town/Accessibility_Standards_for_Customer_Service.htm

En plus de ces documents de référence, l'entrepreneur doit également se référer à l'annexe A1 : Glossaire

5. Portée des travaux

Le fournisseur doit aider et soutenir l'ASFC dans les 4 domaines de travail suivants :

a) Services d'évaluation de la sécurité infonuagique
   i. Examiner la mise en œuvre et l'application de politiques, de normes, de procédures, de lignes directrices, de processus, de mécanismes et de contrôles par l'ASFC et ses fournisseurs de services infonuagiques à la lumière des politiques, des directives et des lignes directrices en matière de sécurité du gouvernement du Canada qui s'appliquent afin d'assurer l'intégrité, la confidentialité et l'accessibilité de l'information, des applications et des charges de travail tout au long de leur cycle de vie.
   ii. Examiner la portée, les responsabilités partagées et les modèles touchant la sécurité infonuagique (y compris la documentation liée au contrat du fournisseur de services infonuagiques) et fournir des conseils à cet égard, examiner la documentation relative à l'architecture et à la conception et préparer ou examiner une matrice des responsabilités en matière de sécurité infonuagique, une matrice des contrôles infonuagiques, etc.
   iii. Évaluer les équipes des opérations de sécurité; fournir des avis sur la capacité des secteurs responsables de gérer et de remplir leurs responsabilités; élaborer et mettre au point des mesures de gestion précises à l'égard des besoins en matière d'outils, de formation, de personnel, de collaboration et de communication.
   iv. Rédiger des rapports, par exemple : pour l'analyse de sécurité des données, les concepts d'opération, les énoncés de sensibilité, les évaluations de la menace, les évaluations des facteurs relatifs à la vie privée, les évaluations des vulnérabilités non techniques, les évaluations des risques et la présentation des menaces, vulnérabilités et risques liés à la sécurité des TI.
   v. Mener les activités de certification et d'accréditation.
   vi. Mener des évaluations techniques de la sécurité par rapport aux biens de l'ASFC, y compris les suivants :
      - charges de travail de niveau Protégé B/Intégrité moyenne/Disponibilité moyenne (PBMM) et non classifiées;
      - données et environnements de développement et d'essai (masquage, brouillage ou chiffrement de données);
      - solutions déployées en tant que modèles IaaS, PaaS ou SaaS — à l'intérieur et à l'extérieur du Canada;
      - adaptation de profils de contrôle de sécurité;
      - examen et intégration de données probantes sur l'évaluation provenant de sources tierces (CCC, SOC, FedRAMP, ISO, etc.).

b) Évaluation de la vulnérabilité
   i. Réalisée dans le cadre des essais de sécurité menés durant le développement d'une solution pour valider l'efficacité de la conception de sécurité et cerner les lacunes éventuelles dans la configuration ou l'inclusion de contrôles, y compris :
      - analyse de code statique;
      - essais statiques et dynamiques;
      - essais de pénétration — réseaux;
      - tests de sécurité visant les applications et les produits;
      - mise à l'essai de tous les ensembles architecturaux : réseau, application, base de

données, infrastructure.

ii. Réalisée périodiquement à l'égard de solutions déployées afin d'assurer la conformité continue et le caractère adéquat des contrôles à la lumière de nouvelles menaces.

c) Opérations touchant la sécurité infonuagique
   i. Aider l'ASFC à sélectionner, à déployer, à intégrer, à configurer et à entretenir les meilleurs outils de surveillance et autres outils liés à la cybersécurité; élaborer et intégrer des processus de sécurité à la gestion des services infonuagiques; établir des mesures stratégiques et opérationnelles de la sécurité.
   ii. S'occuper de la surveillance des systèmes de sécurité et de l'intervention en cas d'incident; mener des enquêtes sur des incidents; préparer des séances d'information, des rapports et des plans d'action sur la sécurité.
   iii. Surveiller la conformité afin d'assurer l'observation et la vigilance continues.
   iv. Assurer la transition et le transfert de connaissances sur les opérations de sécurité vers l'ASFC.

d) Fournir des conseils techniques, un soutien, une ingénierie et une recherche dans la conception, le développement et la sécurisation de solutions fondées sur des technologies émergentes ou en évolution (comme des réseaux infonuagiques publics, des applications mobiles, la biométrie, l'automatisation robotisée de processus, les interfaces API, l'intelligence artificielle/l'apprentissage machine et la technologie IRF) :

   i. effectuer des recherches et cerner des menaces précises impliquées dans le déploiement par le gouvernement du Canada de solutions de TI fondées sur ou incorporant des technologies émergentes;
   ii. fournir une expertise technique afin d'influencer, d'orienter et de soutenir la conception et le développement de solutions au moyen de ces technologies;
   iii. examiner et donner des conseils sur la conception, le développement (y compris l'examen des codes), la configuration et les opérations de solutions;
   iv. fournir à l'ASFC des analyses instructives, des conseils et du soutien en matière d'ingénierie et de conception sur les moyens réalisables de permettre et de faciliter l'adoption et l'utilisation de technologies novatrices tout en renforçant la posture de sécurité de l'Agence ou en l'aidant à atténuer l'exposition aux menaces inhérentes à ces technologies;
   v. tenir l'Agence au courant de l'évolution des risques en matière de sécurité liés à la technologie;
   vi. fournir des conseils sur la façon dont l'ASFC peut évaluer et mettre en œuvre des mesures pour s'adapter constamment aux nouvelles technologies et au développement dans le domaine de la cybersécurité.

6. Tâches et produits livrables des ressources

Aux fins de la prise en charge des aspects décrits dans la section 5, le fournisseur doit mettre à la disposition de l'ASFC des ressources professionnels de cybersécurité des TI dans les catégories de SPICT suivantes (mais sans s'y limiter), au besoin, sur présentation d'autorisations de tâche (AT).

Catégories de ressources	Niveaux
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque	2, 3
C.3. Analyste de la certification et accréditation et des évaluations de la menace et des risques en sécurité des technologies de l'information	2, 3
C.7 Spécialiste en conception de sécurité des technologies de l'information	2, 3
C.8 Analyste de la sécurité des réseaux	2, 3
C.9. Opérateur de systèmes de sécurité des technologies de l'information	2, 3
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2, 3
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2, 3
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2, 3

Voici les tâches et les produits livrables associés aux exigences propres aux ressources. Les tâches et les produits livrables seront énoncés dans les autorisations de tâche.

6.1 C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources.

a. Examiner, analyser ou appliquer les politiques, les procédures et les lignes directrices des gouvernements étrangers, du gouvernement fédéral et des gouvernements provinciaux ou territoriaux en matière de sécurité des TI.
b. Examiner, analyser et appliquer les pratiques exemplaires de sécurité des TI, le droit et les principes éthiques nationaux et internationaux en informatique, l'architecture de sécurité des TI et les méthodes de gestion des risques quant à la sécurité des TI.
c. Élaborer des documents d'orientation décrivant les moyens de s'assurer que la sécurité des TI et la cyberprotection constituent des instruments opérationnels.
d. Offrir des services de consultation et de planification stratégique sur les questions relatives à la sécurité des TI.
e. Réaliser des études de faisabilité, des évaluations des technologies ainsi que des analyses de rentabilité, en plus de proposer des plans de mise en œuvre des systèmes liés à la sécurité des TI.
f. Élaborer des politiques et des stratégies de recherche et développement sophistiquées.
g. Recueillir et compiler les besoins du client en matière de protection de l'infrastructure de l'information et de sécurité des TI, puis établir leur ordre de priorité.
h. Examiner et prioriser les programmes en matière de protection de l'infrastructure de l'information et de sécurité des TI.
i. Élaborer une vision, des stratégies et des concepts stratégiques pour l'architecture de sécurité des TI à l'aide du Programme de transformation opérationnelle et du Modèle de référence stratégique du gouvernement du Canada (MRSG).

j. Élaborer des programmes et des concepts de service en matière de sécurité des TI à l'aide des MRSG suivants : le Modèle de la logique du programme, le Modèle d'harmonisation des programmes et services, le Modèle de responsabilisation et d'intégration des services, le Modèle de transition de l'état, le Modèle d'information et le Modèle de rendement.

6.2 C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources.

a. Examiner, analyser ou appliquer les politiques fédérales en matière de sécurité des TI, les processus de certification et d'accréditation de sécurité des systèmes de TI, les produits de sécurité, les mesures de protection et les pratiques exemplaires en matière de sécurité des TI, ainsi que des stratégies d'atténuation des risques liés à la sécurité des TI.
b. Déterminer les menaces pour les systèmes d'exploitation et les architectures sans fil, ainsi que les éléments vulnérables de ces systèmes et architectures.
c. Relever les menaces de nature personnelle, technique, physique et procédurale ainsi que les vulnérabilités à l'égard des systèmes des TI du gouvernement fédéral.
d. Rédiger des rapports, par exemple : pour l'analyse de sécurité des données, les concepts d'opération, les énoncés de sensibilité, les évaluations de la menace, les évaluations des facteurs relatifs à la vie privée, les évaluations des vulnérabilités non techniques, les évaluations des risques et la présentation des menaces, vulnérabilités et risques liés à la sécurité des TI.
e. Mener les activités de certification incluant : élaboration de plans de certification de sécurité, vérification de la conformité des mesures de sécurité aux politiques et aux normes applicables, validation des exigences de sécurité basée sur le mappage de la politique de sécurité des systèmes et des exigences de sécurité fonctionnelles et sur le suivi des exigences de sécurité appliquées aux différents stades de conception, vérification de l'application appropriée des mesures de protection et du respect des exigences d'assurance (inclut la confirmation de la configuration adéquate du système et l'attestation que les mesures de protection répondent aux normes applicables), tests et évaluation de la sécurité pour déterminer si les mesures de protection techniques fonctionnent correctement, et évaluation des risques résiduels mis au jour lors de l'évaluation des risques pour déterminer s'ils sont acceptables.
f. Effectuer des activités liées à l'accréditation, notamment : l'examen, par l'accréditeur, des résultats de l'homologation indiqués dans les documents d'examen conceptuel, pour s'assurer que les risques entourant l'exploitation du système seront acceptables et que celui-ci sera en conformité avec les politiques et normes de sécurité pertinentes du Ministère et celles qui lui sont propres; et la détermination des conditions d'exploitation du système (aux fins d'approbation). Cela peut comprendre les formes d'autorisation suivantes :
    - l'autorisation d'élaboration, donnée de concert par l'exploitant et l'accréditeur, de passer à l'étape d'élaboration suivante dans le cycle de vie du système de TI si celui-ci doit traiter des renseignements de nature délicate pendant son élaboration;
    - l'autorisation d'exploitation écrite permettant l'exploitation du système de TI mis en place, de même que le traitement de renseignements de nature délicate lorsque les risques associés à l'exploitation du système sont jugés acceptables et que celui-ci est conforme aux normes et politiques de sécurité applicables;
    - l'autorisation provisoire, également donnée par écrit, pour autoriser le traitement de renseignements de nature délicate dans des circonstances particulières, lorsqu'on n'a pas encore réussi à ramener les risques à un niveau acceptable, mais

qu'il est nécessaire d'exploiter le système en cours d'élaboration.

6.3 C.7 Spécialiste en conception de sécurité des technologies de l'information, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources :

a. Examiner, analyser ou appliquer : des méthodes, modèles et cadres d'architecture comme The Open Group Architecture Framework (TOGAF), le Federal Enterprise Architecture Program (FEAP) (gouvernement américain), l'Architecture de sécurité intégrée du gouvernement du Canada, le cadre de Zachman et le Unified Mobility Manager (UMM).
b. Examiner, analyser ou appliquer un large éventail de technologies de sécurité, dont de nombreux types de systèmes ou d'architectures d'applications et de nombreuses plateformes matérielles et logicielles, y compris :
    - les normes d'annuaire comme X.400, X.500 et SMTP;
    - les systèmes d'exploitation comme MS, Unix, Linux et Novell;
    - les protocoles réseau comme HTTP, FTP et Telnet;
    - les routeurs, les multiplexeurs et les commutateurs réseau;
    - les protocoles DNS (services de nom de domaine) et NTP (protocole de synchronisation réseau);
c. Examiner, analyser ou appliquer des architectures, des normes ainsi que des protocoles de communication et de sécurité des TI protégés (comme les protocoles IPSec, TLS, SSH, S-MIME et HTTPS).
d. Examiner, analyser ou appliquer des protocoles de sécurité des TI pour toutes les couches de l'OSI (interconnexion des systèmes ouverts) et toutes les piles TCP/IP (protocole de contrôle de transmission/protocole Internet).
e. Examiner, analyser ou appliquer l'importance et les conséquences des tendances du marché et de la technologie afin de les appliquer aux feuilles de route pour les architectures et la conception des solutions (p. ex. sécurité des services Web, sécurité des interfaces API, gestion des incidents, gestion de l'identité).
f. Examiner, analyser ou appliquer les pratiques exemplaires et les normes en matière de zonage réseau et les principes de défense en profondeur.
g. Analyser les statistiques, outils et techniques de sécurité des TI.
h. Analyser les données de sécurité et présenter des avis et des rapports.
i. Assurer la conception d'architectures de sécurité et le soutien technique.
j. Réaliser des études liées à la classification ou à la désignation de sécurité des données.
k. Préparer des alertes et avis de sécurité des TI sur mesure provenant de sources publiques et privées.

et

l. Examiner, analyser ou appliquer les pratiques, technologies et architectures de gestion de l'identité, des justificatifs d'identité et de l'accès.
m. Élaborer et présenter du matériel d'exposés pour soutenir la communication avec les praticiens de la sécurité des TI, les cadres supérieurs, etc.
n. Effectuer des recherches et cerner des menaces précises associées au déploiement par le gouvernement du Canada de solutions de TI qui reposent sur des technologies émergentes ou intègrent de telles technologies (y compris l'infonuagique, les technologies mobiles, la technologie IRF, l'intelligence artificielle, l'automatisation robotisée de processus, la biométrie, les interfaces API, etc.).

o. Fournir à l'ASFC des conseils instructifs et du soutien en matière d'ingénierie et de conception sur les moyens réalisables de permettre et de faciliter l'adoption et l'utilisation de technologies émergentes tout en renforçant la posture de sécurité de l'Agence ou en l'aidant à atténuer l'exposition aux menaces inhérentes à ces technologies.
p. Examiner, analyser et identifier les menaces techniques et les vulnérabilités de l'infrastructure infonuagique, des bases de données et des technologies émergentes.
q. Tenir l'Agence au courant de l'évolution des risques en matière de sécurité liés à la technologie.

6.4 C.8 Analyste de la sécurité des réseaux, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources.

a. Examiner, analyser ou appliquer :
    - les protocoles de sécurité Internet (TLS, HTTPS, S-MIME, IPSec, SSH);
    - les protocoles TCP/IP, UDP, DNS, SMTP;
    - les algorithmes cryptographiques approuvés par le GC;
    - les normes d'annuaire comme X.400, X.500 et SMTP;
    - les protocoles réseau (HTTP, FTP, Telnet);
    - le renforcement de la sécurité réseau (p. ex. procédure d'interpréteur de commandes, détermination des services);
    - les mesures de protection techniques pour la sécurité des TI;
    - les outils et techniques de sécurité des TI;
    - les systèmes d'exploitation comme MS, Unix, Linux et Novell;
    - les systèmes de détection des intrusions et coupe-feu;
    - les routeurs, les multiplexeurs et les commutateurs réseau;
    - les technologies sans fil.
b. Analyser les données de sécurité et présenter des avis et des rapports.
c. Effectuer des analyses d'impact pour la mise en œuvre de nouveaux logiciels, les modifications de configuration importantes et la gestion des correctifs.
d. Élaborer des modèles et essais de validation de principe en sécurité des TI touchant des technologies émergentes.
e. Concevoir ou élaborer des protocoles de sécurité des TI.
f. Déceler et analyser les menaces techniques pesant sur les réseaux et leurs vulnérabilités.
g. Analyser les outils et techniques de sécurité des TI.
h. Effectuer les tâches associées à l'autorisation et à l'authentification dans les environnements physiques et logiques.
i. Préparer des alertes et avis de sécurité des TI sur mesure provenant de sources publiques et privées.
j. Réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.

et

k. Examiner, analyser et identifier les menaces techniques et les vulnérabilités de l'infrastructure infonuagique, des bases de données et des technologies émergentes.

6.5 C.9. Opérateur de systèmes de sécurité des technologies de l'information, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources.

a. Examiner, analyser ou appliquer :
   - les protocoles réseau (HTTP, FTP, Telnet);
   - les protocoles de sécurité Internet (p. ex. TLS, HTTPS, S-MIME, IPSec, SSH);
   - les protocoles TCP/IP, UDP, DNS, SMTP;
   - les normes d'annuaire comme X.400, X.500 et SMTP;
   - les routeurs, les multiplexeurs et les commutateurs réseau;
   - le renforcement de la sécurité réseau (p. ex. procédure d'interpréteur de commandes, détermination des services);
   - les technologies sans fil;
   - les menaces techniques à l'endroit des réseaux et les vulnérabilités de ceux-ci;
   - les mesures de protection techniques pour la sécurité des TI;
   - les produits matériels et logiciels de sécurité des TI.

b. Configurer des systèmes d'exploitation comme MS, Unix, Linux et Novell.
c. Configurer la gestion de la sécurité des TI.
d. Configurer des systèmes de détection des intrusions, des coupe-feu et des vérificateurs de contenu, extraire et analyser des rapports et des journaux, et intervenir en cas d'incidents en matière de sécurité.
e. Configurer et mettre à jour les analyseurs de virus.
f. Réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.

et

g. Utiliser des outils de gestion des informations et des événements de sécurité (GIES) et des outils de surveillance de la sécurité infonuagique, comme AWS Security Hub ou Azure Sentinel.

6.6 C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources.

a. Examiner, analyser ou appliquer :
   - les outils d'analyse des agents de menace et autres nouvelles technologies, notamment les outils de protection des renseignements personnels, l'analyse prédictive, les techniques VoIP, la visualisation et la fusion des données, les dispositifs de sécurité sans fil, les PBX et les coupe-feu pour téléphonie;
   - les détecteurs d'accès entrant, les perceurs de mots de passe;
   - les services consultatifs du domaine public sur les vulnérabilités des TI;
   - les analyseurs réseau et des outils d'analyse des vulnérabilités comme SATAN, ISS, Portscan et NMap;
   - les protocoles réseau (HTTP, FTP, Telnet);
   - les protocoles de sécurité Internet, comme TLS, HTTPS, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP et SNMP;

- la sécurité des systèmes sans fil;
- les systèmes de détection des intrusions, les coupe-feu et les vérificateurs de contenu;
- les systèmes de détection et de prévention des intrusions dans les hôtes et les réseaux (gestion des antivirus).

b. Déceler les menaces pesant sur les réseaux et leurs vulnérabilités techniques.
c. Mener des examens et analyses des journaux de sécurité des systèmes sur site.
d. Recueillir, compiler, analyser et diffuser de l'information publique sur les menaces et les vulnérabilités pesant sur les ordinateurs en réseau, les incidents de sécurité et les interventions en réponse aux incidents.
e. Préparer ou tenir des réunions d'information sur les menaces, les vulnérabilités ou les risques liés à la sécurité des TI.
f. Réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.

et

g. Examiner, analyser et identifier les menaces techniques et les vulnérabilités de l'infrastructure infonuagique, des bases de données et des technologies émergentes.

6.7 C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources.

a. Examiner, analyser ou appliquer :
    - la capacité de recherche et développement sur la sécurité des TI dans l'industrie et les universités canadiennes;
    - les normes d'annuaire comme X.400, X.500 et SMTP;
    - les protocoles réseau comme HTTP, FTP et Telnet;
    - les protocoles de sécurité Internet (TLS, HTTPS, S-MIME, IPSec, SSH);
    - les normes de sécurité des technologies sans fil et Bluetooth;
    - les protocoles et normes TCP/IP, UDP, DNS, SMTP et SNMP;
    - les systèmes de détection des intrusions, de coupe-feu et de vérificateurs de contenu;
    - les algorithmes cryptographiques;
    - les pratiques exemplaires de sécurité.
b. Élaborer et mettre en œuvre des programmes de sécurité tels la biométrie, la gestion des droits d'auteur numériques, les étiquettes RFID, le contrôle d'accès et la gestion des supports amovibles.
c. Conceptualiser et élaborer des prototypes ainsi que des modèles et essais de validation de principe, y compris à l'égard de fonctionnalités et de technologies émergentes liées à la sécurité.
d. Analyser des rapports de recherche et développement sous l'angle de la sécurité des TI.
e. Participer à des forums nationaux et internationaux sur la recherche et le développement.
f. Réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.

et

g. Examiner, analyser et identifier les menaces techniques et les vulnérabilités de l'infrastructure infonuagique, des bases de données et des technologies émergentes.

h. Réaliser une analyse des besoins envisagés sous l'angle de la sécurité des TI afin de cerner les besoins des utilisateurs, les besoins en matière de système et les besoins en matière de capacité concernant les technologies émergentes.
i. Fournir une expertise relative à la sécurité de technologies émergentes comme la biométrie, l'intelligence artificielle, la technologie IRF, les technologies mobiles, les technologies sans fil, le contrôle d'accès, les technologies à capteurs, l'automatisation robotisée de processus, les interfaces API, etc.
j. Fournir à l'ASFC des conseils et du soutien en matière d'ingénierie, de conception et de développement sur les moyens réalisables de permettre et de faciliter l'adoption et l'utilisation de technologies émergentes tout en renforçant la posture de sécurité de l'Agence ou en l'aidant à atténuer l'exposition aux menaces inhérentes à ces technologies.
k. Tenir l'Agence au courant de l'évolution des risques en matière de sécurité liés à la technologie.

6.8 C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveaux 2 et 3

Voici une liste non exhaustive des responsabilités associées à cette catégorie de ressources.

a. Examiner, analyser et/ou appliquer :
    - la politique et les lignes directrices du Conseil du Trésor sur l'évaluation des facteurs relatifs à la vie privée;
    - la *Loi sur la protection des renseignements personnels* et ses règlements d'application;
    - les politiques du Conseil du Trésor sur la protection de la vie privée et des renseignements personnels;
    - la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE);
    - les politiques et les lignes directrices du gouvernement en TI-GI;
    - les initiatives Gouvernement en direct (GED);
    - le réseau de la Voie de communication protégée, y compris ses processus opérationnels et techniques, ainsi que les services offerts;
    - les pratiques et les principes liés à la sécurité des TI;
    - les solutions technologiques en matière de sécurité des TI.
b. Réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) et des évaluations préliminaires des facteurs relatifs à la vie privée (EPFVP) des projets et des concepts, conformément aux exigences énoncées dans :
    - la Politique d'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor;
    - les lignes directrices du Conseil du Trésor sur l'EFVP;
    - d'autres normes, procédures et lignes directrices pertinentes.
c. Analyser les flux d'information à l'aide du modèle d'EFVP fourni par le client.
d. Effectuer une analyse des facteurs relatifs à la vie privée pour démontrer la conformité avec les principes généraux reconnus en matière de respect de la vie privée et pour reconnaître les risques d'entrave à la vie privée.
e. Élaborer des plans de gestion des risques relatifs à la vie privée.
f. Élaborer des recommandations quant aux stratégies possibles d'atténuation des risques d'entrave à la vie privée.
g. Réaliser des tâches soutenant directement le programme ministériel de cyberprotection et de sécurité des TI.

et

h. Effectuer une analyse pour déterminer les risques d'entrave à la vie privée et démontrer la conformité avec les exigences en matière de respect de la confidentialité des données des partenaires internationaux du Canada, le cas échéant.

6.9. Tâches communes

- Effectuer une analyse technique et des évaluations de l'incidence technique.
- Fournir des évaluations stratégiques des tendances technologiques et des nouvelles technologies.
- Évaluer les outils technologiques dans l'ensemble de l'organisation et participer à leur sélection.
- Préparer des documents techniques, comme l'analyse des besoins, l'analyse des possibilités, les documents d'architecture technique et la modélisation mathématique des risques.
- Rechercher du matériel de source ouverte afin d'analyser les tendances et les technologies nouvelles.
- Superviser des projets.
- Préparer des séances d'information à l'intention des cadres supérieurs.
- Élaborer et fournir des documents de formation pour le transfert de connaissances reliées aux catégories de ressources.

7. Produits livrables

L'entrepreneur doit fournir et soumettre les produits livrables au responsable technique et/ou tel qu'identifié/exigé dans l'AT. L'autorisation de tâche (AT) individuelle définira les documents et les produits livrables requis pour le projet/l'exigence spécifique.

Les produits livrables peuvent inclure, mais sans s'y limiter :

a. un plan de travail pour les travaux à entreprendre;
b. un rapport d'étape sur une base bimensuelle ou mensuelle sur les activités entreprises qui comprend les éléments suivants :
    1. activités achevées au cours de la période considérée,
    2. activités prévues pour la prochaine période de rapport,
    3. risques/problèmes qui nécessiteront l'attention du responsable technique,
    4. actions correctives requises;
c. des documents, présentations et autres matériaux, à la demande du responsable technique;
d. un rapport trimestriel d'utilisation des autorisations de tâches.

Les documents peuvent inclure, mais sans s'y limiter :

1. examen de la gestion des risques liés au nuage;
2. évaluation de la sécurité infonuagique;
3. matrice des responsabilités en matière de sécurité infonuagique;
4. conception de la sécurité infonuagique;
5. matrice des contrôles infonuagiques;
6. analyse de la sécurité des données;
7. concepts d'opération;
8. énoncés de sensibilité;
9. évaluations des menaces;

10. évaluations préliminaires des facteurs relatifs à la vie privée (EPFVP);
11. évaluations des facteurs relatifs à la vie privée (EFVP);
12. plans de gestion des risques relatifs à la vie privée;
13. évaluations non techniques de la vulnérabilité;
14. évaluations de la menace et des risques;
15. séances d'information et rapports sur les menaces, la vulnérabilité et les risques liés à la sécurité des TI;
16. plans d'analyse et de mise en œuvre de solutions de sécurité des TI;
17. sondages et études des besoins;
18. recherche, et analyse des options;
19. schéma théorique et logique de l'architecture;
20. documentation technique relative à la conception de la sécurité;
21. documentation sur la gestion du changement;
22. documentation sur la gestion des configurations;
23. exigences en matière de sécurité des TI;
24. algorithmes, modélisation mathématique des risques;
25. contrôles de système;
26. modèles de démonstration de faisabilité;
27. stratégies d'essai de la sécurité des TI;
28. plans, scénarios et rapports relatifs aux essais de la sécurité des TI;
29. rapports de suivi des anomalies, des demandes de changement et des questions en suspens;
30. plans et guides de mise en œuvre;
31. guides des procédures normales d'exploitation;
32. analyses d'impact et stratégies connexes;
33. plans de projet;
34. documents d'analyse;
35. schéma théorique et logique de la sécurité des systèmes;
36. conseils oraux et écrits;
37. matériel de transfert des connaissances et de formation;
38. documents de réflexion et notes d'information;
39. alertes et avis de sécurité des TI;
40. schéma de processus, flux décisionnels et flux de données;
41. dossiers et documents de présentation;
42. facilitation des réunions et rapports (p. ex. rapports d'étape mensuels);
43. indicateurs;
44. rapports d'incidents de sécurité;
45. rapports opérationnels;
46. notes de conversation.

Les produits livrables doivent être présentés sous forme électronique dans les formats indiqués dans l'autorisation de tâche (p. ex. applications Microsoft Project ou Microsoft Office Suite comme indiqué dans l'AT). Tous les produits livrables électroniques doivent être conformes aux normes logicielles du Ministère, qui sont actuellement la dernière version de Microsoft Office Suite. Au besoin, l'ASFC remettra au fournisseur les formulaires et modèles requis pour respecter ces normes.

Il se peut que les ressources du fournisseur doivent avoir accès aux renseignements exclusivement accessibles dans les installations du Canada situées dans la RCN. Tous les documents élaborés ou mis à jour par chacune des ressources du fournisseur doivent être fournis au chargé de projet aux fins d'examen, d'approbation et de signature (au besoin). Le chargé de projet doit avoir accès en tout temps à tous les travaux prévus dans le contrat.

Chaque AT indiquera la langue et le format exigés à l'égard du produit livrable.

8. Environnement technique

L'environnement technique de l'ASFC comprend plusieurs technologies, notamment :

Langage de balisage extensible (XML)

- XAML
- Langage de définition de schéma XML (XSD)
- Définition de type de document (DTD)
- XPATH
- XSLT
- Xquery, jQuery
- Notation des objets du langage Java (JSON)
- Cadres JavaScript — REACT, Node.js
- HTML, HTML5
- Java
- Python
- VB.NET
- TypeScript (Angular)
- Hibernate

Langages de programmation propres aux applications mobiles

- SWIFT et IU de SWIFT
- Kotlin
- Coca et Coca Touch
- Ionic
- React Native
- JQuery Mobile
- Objective-C
- Java
- Xamarin

Langages de programmation propres à l'infonuagique

- Scriptage Ancible
- Scriptage AWS CloudFormation
- Scriptage Azure Resource Manager (ARM)
- Scriptage Terraform
- Outils et cadres de développement
- EDI Eclipse
  Visual Studio Code, EDI Visual Studio Enterprise
- EDI AWS Cloud9
- GitHub Desktop

- Microsoft Teams
- Éditeur OpenAPI (Swagger)
- Xcode
- JEE (Websphere)
- JMS (Websphere MQ)
- WebSphere Application Server (WAS), serveur d'applications Tomcat, application JBoss
- Cadre Spring et Spring Integration, cadre Spring Boot
- Jersey REST, Apache REST
- ANT, Apache Maven, SVN, git
- Azure DevOps
- AWS DevOps — CodeCommit, CodePipeline, etc.
- Interface de ligne de commande AWS
- Windows PowerShell
- AWS Cloud Development Kit (CDK)
- UiPath Orchestrator

Protocoles de communication

- TCP/IP
- Protocole de transfert de fichiers (FTP)
- Transfert sécurisé de fichiers (SFTP)
- Protocole de transfert hypertexte (HTTP)
- Protocole de transfert de courrier simple (SMTP)
- Transfert géré de fichiers, y compris le logiciel de MSFT de TPSGC
- Protocole de sécurité (SSL)/protocole de sécurité de la couche transport (TLS)

Échange de données informatisées (EDI)

- ANSI X.12
- EDIFACT
- Normes de l'IATA
- Modèle de données de l'Organisation mondiale des douanes (OMD)
- Modèles de données financières, sur le transport

Interopérabilité et intégration

- Normes de services Web : SOAP et REST
- Langage de description de services Web (WSDL)
- Notation des objets du langage Java (JSON)
- Logiciel de gestion des règles d'affaires
- Bus de service d'entreprise
- Chiffrement/déchiffrement dans une ICP
- CA IDM et CA SM
- IBM DataPower
- GatewayScript
- IBM Sterling Transformation
- Cartes IBM Transformation Extender

Données et analytique

- IBM DB2 sous UNIX, z/OS
- Bases de données Sybase et Oracle
- SAP HANA
- SAP Business Suite
- IBM PureData
- IBM DataStage
- IBM Infosphere Suite
- IBM SPSS
- IBM Cognos Suite
- Erwin Data Modeler
- Bases de données infonuagiques — AWS DynamoDB, AWS RDS Postgress SQL, AWS RDS MySQL
- AWS RedShift, AWS DataLake, AWS Glue (outil ETL), AWS Athena
- Azure Analytics

Systèmes d'exploitation et autres plateformes

- Android
- iOS
- Unix Solaris
- Red Hat Linux
- Amazon Linux
- Windows Server 2016, Server 2019
- VMware
- Z-OS
- Microsoft Windows 10 (Desktop)
- Infrastructure de nuage publique AWS
- Infrastructure de nuage publique Azure

AWS

- AWS Security Hub
- AWS Guard Duty
- AWS CloudTrail
- AWS Web Application Firewall
- AWS Identity and Access Management
- Amazon Detective
- Amazon Macie
- AWS Systems Manager Ops Center

Azure

- Azure Sentinel
- Azure Monitor
- Azure Network Monitor
- Azure Security Center

- Azure Log Analytics Workspace

Autre

- UiPath, UiPath Studio, UiPath Robot/Assistant
- IBM Data Studio
- Spring Tool Suite
- Netezza
- SSAName3
- COBOL
- OS/360
- ACO
- SQL
- R
- Python
- Scala
- ArcGIS
- MS Dynamics
- OpenText GCDocs
- SAP SuccessFactors
- Citrix
- IBM Rational Software Architect
- Archimate, Qualiware
- Adobe
- Microsoft Office/Office 365
- Microsoft Active Directory
- CA APM Introscope
- Vue.js
- Apache Jmeter
- SmartBear SoapUI

Autres technologies nouvelles et émergentes et logiciels connexes

Autres bases de données, langages ou applications logicielles de GI-TI utilisés au sein de l'ASFC

9. Lieu des travaux

Le personnel du fournisseur peut être appelé à travailler sur place dans les locaux de l'ASFC dans la RCN, ou dans les locaux du fournisseur à l'extérieur. Le lieu où les services seront fournis sera indiqué dans chaque autorisation de tâche (AT).

Certains services, en particulier le (5) b), pourraient être dispensés en partie à l'extérieur des environnements de l'ASFC grâce à l'équipement du fournisseur et/ou de l'ASFC. Toutefois, à aucun moment des données protégées ne devront être stockées à l'extérieur de l'infrastructure de l'ASFC. Les autres services et tâches se dérouleront dans les environnements de l'ASFC et seront intégrés à ceux-ci grâce à l'équipement de l'ASFC.

10. Exigences linguistiques

Bien que les ressources proposées doivent être à l'aise en anglais, il peut être nécessaire que des ressources spécifiques s'expriment couramment dans les deux langues officielles, ce qui sera précisé dans l'AT.

11. Heures de travail

Les heures de travail sont de 7 h à 18 h du lundi au vendredi, et les ressources du fournisseur doivent, sauf indication contraire dans l'AT, travailler 7,5 heures par jour pendant cette période. Toutes les ressources du fournisseur doivent être en mesure de travailler en dehors des heures normales pendant la durée du contrat. Le fournisseur peut devoir fournir les ressources en soirée, la fin de semaine ou durant des jours fériés. Le responsable technique doit préalablement approuver les heures travaillées au-delà du nombre d'heures/de jours facturables dans un mois.

12. Réunions

À moins d'indication contraire dans l'énoncé des travaux ou dans une autorisation de tâche émise par le chargé de projet, ou à moins d'une autre entente conclue avec le chargé de projet, les réunions entre le Canada et le fournisseur auront lieu dans la région de la capitale nationale à un moment choisi par les deux parties. Le Canada déterminera le lieu des réunions. Les réunions seront présidées par le Canada. Le Canada fournira les installations, le matériel et les services raisonnablement nécessaires au bon déroulement des réunions.

Le fournisseur devra faire en sorte que la personne responsable du volet des travaux devant faire l'objet de discussions ou une personne apte à la représenter et autorisée à effectuer les travaux selon le contrat soit présente à la réunion. Afin de limiter les déplacements et les interruptions dans le déroulement du travail, le Canada et le fournisseur peuvent, d'un commun accord, tenir des vidéoconférences ou des conférences téléphoniques plutôt que des réunions en personne.

13. Exigences en matière de déplacements

Il n'existe aucune exigence relative aux déplacements.

14. Contraintes, normes et spécifications

Le fournisseur devra composer avec les contraintes et l'espace de travail imposés par le Ministère. Il peut s'agir de politiques et de procédures obligatoires gouvernementales, d'activités connexes actuelles ou proposées, d'exigences en matière de sécurité, de sensibilité requise par rapport à d'autres intérêts, de soucis de protection de l'environnement, de conservation des ressources et de toute autre restriction pertinente.

Les lignes directrices, normes, directives et politiques de sécurité internes de l'ASFC et du gouvernement du Canada qui s'appliquent comprennent, sans s'y limiter, les suivantes (voir la section 4, Documents de référence) :

I. Gouvernement du Canada, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*
II. Gouvernement du Canada, *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage*
III. Centre canadien pour la cybersécurité, *Directives*
IV. Gouvernement du Canada, *Orientation relative à la résidence des données électroniques* (AMPTI 2017-02, archivé)

Tous les travaux doivent être réalisés au Canada et toutes les technologies et l'information de l'ASFC doivent demeurer au Canada.

Le gouvernement du Canada s'efforce de s'assurer que les biens et services qu'il achète sont inclusifs de par leur conception et accessibles par défaut, conformément à la Loi canadienne sur l'accessibilité, aux règlements et aux normes connexes, ainsi qu'à la Politique sur les marchés du Conseil du Trésor. Les normes d'accessibilité suivantes s'appliquent au présent besoin :

I. *Loi sur l'accessibilité pour les personnes handicapées de l'Ontario* (LAPHO) – Normes d'accessibilité intégrées
II. Municipalité d'East Gwillimbury — Normes d'accessibilité pour le service à la clientèle

15. <u>Renseignements et équipement fournis par le gouvernement</u>

L'ASFC fournira, sous réserve des exigences prédéfinies relatives à la sécurité, et seulement aux membres du personnel désignés du fournisseur, l'accès à certaines bases de données ou applications installées dans les ordinateurs ou les réseaux de l'ASFC, à seule fin de l'exécution des tâches liées au contrat. Le responsable technique, à sa seule discrétion, déterminera le type et les paramètres d'accès.

L'ASFC procurera également ce qui suit au personnel du fournisseur :

- documents internes pertinents;
- locaux à bureaux et laissez-passer (indiqués au besoin dans l'autorisation de tâche);
- matériel informatique, par exemple un ordinateur portable (indiqués au besoin dans l'autorisation de tâche).

ANNEX A1 : GLOSSAIRE

Terme	Contexte
Analyse des vulnérabilités	Une **analyse des vulnérabilités** consiste en une analyse de sécurité automatisée qui est conçue pour détecter les faiblesses connues par une évaluation des ordinateurs, des réseaux ou des applications. Ils sont utilisés pour cibler et détecter les vulnérabilités découlant d'une mauvaise configuration ou programmation dans une ressource réseau, telle qu'un pare-feu, un routeur, un serveur Web ou un serveur d'applications. Les scanneurs modernes utilisés pour les analyses des vulnérabilités effectuent des analyses authentifiées et non authentifiées. … Bien souvent, le scanneur de vulnérabilités moderne peut personnaliser les rapports de vulnérabilité ainsi que les logiciels installés, les ports ouverts, les certificats et autres informations sur l'hôte qui peuvent être demandées dans le cadre du flux de travaux. • Les analyses authentifiées permettent au scanneur d'accéder directement aux ressources du réseau au moyen de protocoles d'administration à distance tels que SSH (Secure Shell) ou RDP (Remote Desktop Protocol) et de s'authentifier en utilisant les justificatifs d'identité fournis. Ainsi, le scanneur de vulnérabilités peut accéder à des données de niveau inférieur, comme des services précis et le détail de configuration du système d'exploitation hôte. Il est ensuite en mesure de fournir des renseignements détaillés et précis sur le système d'exploitation et les logiciels installés, y compris les problèmes de configuration et les correctifs de sécurité manquants. • Les analyses non authentifiées peuvent entraîner de nombreux faux positifs et ne génèrent pas de renseignements détaillés sur le système d'exploitation des ressources et les logiciels installés. Cette méthode est utilisée en général par les auteurs des menaces ou les analystes de sécurité qui tentent de déterminer la position de sécurité des ressources accessibles à partir de l'extérieur. Source : Wikipédia
Application essentielle aux activités	Une **application essentielle aux activités** est une application indispensable ou importante pour le fonctionnement d'une organisation. Autrement dit, il s'agit d'une application fondamentale à un secteur d'activité qui, en cas d'interruption, pourrait provoquer de graves pertes financières, des poursuites judiciaires, le mécontentement des clients et une baisse de productivité. Ces applications peuvent aller des petits outils aux outils spécialisés, en passant par les principaux systèmes des secteurs d'activité. Elles peuvent être exécutées sur le système ou les serveurs du client, peuvent comprendre des produits commerciaux, être une application ou un système tiers, ou être tout système développé à l'interne.

Terme	Contexte
Apprentissage automatique (ML)	**L'apprentissage automatique** est un sous-ensemble de l'IA (intelligence artificielle) qui est axé sur la capacité des machines à recevoir un ensemble de données et à apprendre par elles-mêmes, par la modification des algorithmes à mesure qu'elles traitent les renseignements qu'elles reçoivent. Le simple fait d'utiliser un algorithme afin de prédire le résultat d'un événement n'est pas un apprentissage automatique, contrairement à l'utilisation des résultats de la prédiction afin d'améliorer les prévisions futures. L'objectif est d'apprendre à partir des données relatives à une certaine tâche afin de maximiser le rendement de la machine pour cette tâche donnée. L'apprentissage automatique vise principalement la précision, et non le succès. Sources : DataScienceCentral.com, Hackernoon.com
« Border Five »	Le groupe **« Border Five »** est un groupe de discussion informel qui traite des questions politiques sur la gestion des douanes et des frontières. L'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis y participent. Source : Wikipédia
Centre des opérations de sécurité (COS)	Un **centre des opérations de sécurité** (SOC) comprend une équipe responsable de la sécurité de l'information ainsi que l'infrastructure, les outils et les processus nécessaires pour surveiller et analyser la posture de sécurité d'une organisation sur une base continue. L'objectif de l'équipe du COS est de détecter, d'analyser et de réagir aux incidents de cybersécurité en utilisant une combinaison de solutions technologiques et un ensemble solide de processus. Ces centres sont généralement dotés d'analystes et d'ingénieurs en sécurité et de gestionnaires qui supervisent les opérations de sécurité. Le personnel du COS travaille en étroite collaboration avec les équipes d'intervention en cas d'incidents dans l'organisation pour s'assurer que les problèmes de sécurité sont traités promptement, dès qu'ils sont constatés. L'infrastructure type du COS comprend des pare-feu, des SPI/SDI (systèmes de prévention d'intrusion/système de détection d'intrusion), des solutions de détection des violations, des envois-tests et un système « SIEM » qui sert à la gestion de l'information et des événements de sécurité. La technologie devrait être mise en place pour collecter les données grâce aux flux de données, à la télémétrie, à la capture de paquets, au journal du système et à d'autres méthodes pour que les données puissent être corrélées et l'activité des données, analysée par le personnel du COS. Le centre de cybersécurité surveille également les réseaux et les points d'extrémité afin de

Terme	Contexte
	détecter les vulnérabilités et protéger les données sensibles, tout en se conformant aux règlements industriels ou gouvernementaux. Source : Digital Guardian
Configuration[1]	Par **configuration**, on entend la disposition, les relations et la personnalisation de composants matériels ou logiciels qui constituent un système informatique, de sorte que ce dernier soit en mesure d'exécuter les tâches pour lesquelles il est conçu selon des exigences données.
Configuration[2]/Configurer[2]	La **configuration** peut également faire référence à l'action de structurer ou de personnaliser des composants matériels ou logiciels d'un système informatique, de sorte qu'il puisse exécuter les tâches pour lesquelles il est conçu selon des exigences données.
Cybersécurité	On entend par **cybersécurité** l'ensemble des technologies, des processus et des pratiques conçus pour protéger les réseaux, les appareils, les programmes et les données contre les attaques, les dommages ou les accès non autorisés. On peut aussi l'appeler « sécurité des technologies de l'information » ou « sécurité informatique ». Source : DigitalGuardian.com
Données protégées	Aux fins du marché, les **données protégées** sont les données d'une application dont la nature est réputée sensible et qui nécessitent des dispositifs de sécurité répondant à un des profils de contrôle suivants : i. Protégé B, intégrité moyenne, disponibilité moyenne (PBMM) ou SECRET, intégrité moyenne, disponibilité moyenne ii. FEDRAMP – Modéré ou élevé; iii. NIST SP 800-53 – Modéré ou élevé
Essais de pénétration	**L'essai de pénétration** est une cyberattaque simulée autorisée sur un système informatique et effectué pour évaluer la sécurité du système. Le test sert à cibler les faiblesses (ou « vulnérabilités »), y compris la possibilité pour des parties non autorisées d'accéder aux caractéristiques et aux données du système, et les forces du système, ce qui permet de réaliser une évaluation complète des risques. […] Voici une description que fait le « National Cyber Security Center » des tests de pénétration : Méthode permettant d'assurer la sécurité d'un système informatique en tentant une violation totale ou partielle de la sécurité du système en question, au moyen des mêmes outils et techniques qu'utiliserait un adversaire. Source : Wikipédia

Terme	Contexte
Évaluation des attestations d'études canadiennes	Une **évaluation des attestations d'études canadiennes** est une affirmation de la comparabilité générale d'une attestation d'études internationale avec une attestation d'études canadienne. Le Centre d'information canadien sur les diplômes internationaux (CICDI) aide les personnes qui souhaitent faire évaluer leurs attestations d'études et leurs compétences professionnelles en les dirigeant vers les organisations compétentes.
Évaluation des menaces et des risques	**L'évaluation des menaces et des risques** (EMR) désigne un processus qui consiste à définir les ressources du système et la façon dont elles peuvent être compromises, par l'évaluation du niveau de risque que posent les menaces pour les actifs et la recommandation de mesures de sécurité pour les atténuer. Le terme désigne également le résultat (le produit) généré par ce processus. Source : https://cyber.gc.ca/fr/glossaire/ERM
Évaluation de sécurité	Mise à l'essai ou évaluation des contrôles de sécurité de gestion, opérationnels et techniques dans un système d'information afin de déterminer la mesure dans laquelle ces derniers ont été mis en œuvre correctement, fonctionnent comme prévu, et produisent les résultats attendus en ce qui a trait au respect des exigences de sécurité. Source : NIST Computer Security Resource Center
Évaluation des risques pour la sécurité des entreprises informatiques	Les **évaluations des risques pour la sécurité des entreprises informatiques** sont effectuées pour permettre aux organisations d'évaluer, de cibler et de modifier leur position globale relativement à la sécurité et pour permettre au personnel de sécurité, des opérations et de la gestion organisationnelle, entre autres, de considérer l'ensemble de l'organisation du point de vue d'un agresseur et de travailler ensemble. Ce processus est nécessaire à la participation de la direction de l'organisation en vue d'assigner des ressources et de mettre en œuvre les solutions de sécurité appropriées. Une évaluation complète des risques relatifs à la sécurité de l'entreprise permet également de déterminer la valeur des différents types de données générées et stockées dans l'organisation. Sans évaluer la valeur des différents types de données dans l'organisation, il est presque impossible de classer par priorité les ressources technologiques et de les affecter là où elles sont le plus utiles. Afin d'évaluer correctement les risques, la direction doit déterminer les données qui s'avèrent les plus précieuses pour l'organisation, les

Terme	Contexte
	mécanismes de stockage utilisés pour ces données et les vulnérabilités y afférentes. Source : ISACA
Examen d'évaluation et d'autorisation de sécurité (EAS)	Processus par lequel les ministères s'assurent que seuls les logiciels et matériels autorisés sont installés dans leur environnement de technologie de l'information (TI). L'évaluation de la sécurité est un processus continu qui évalue les pratiques et les contrôles de sécurité afin de déterminer s'ils sont mis en œuvre correctement, s'ils fonctionnent comme prévu et s'ils permettent d'atteindre les résultats souhaités. L'autorisation de sécurité consiste à obtenir et à maintenir une décision de gestion sur le risque en matière de sécurité qui accepte explicitement le risque résiduel connexe en s'appuyant sur les résultats d'une évaluation de sécurité. Cette autorisation est appelée « autorisation d'exploitation » (AE). Cette procédure est décrite de façon détaillée dans le guide ITSG-33. Source : Services partagés Canada, Audit d'évaluation et d'autorisation de sécurité
Gestion du risque de sécurité	**La gestion du risque de sécurité** est la pratique qui consiste à donner priorité aux mesures de défense de la cybersécurité en fonction des effets négatifs possibles des menaces que visent ces mesures. L'établissement d'une approche de gestion des risques pour les investissements en matière de cybersécurité reconnaît qu'aucune organisation ne peut éliminer complètement toutes les vulnérabilités des systèmes ou bloquer toutes les cyberattaques. Grâce à la gestion du risque en matière de cybersécurité, une organisation s'occupe généralement en premier lieu des lacunes, des tendances des menaces et des attaques qui importent le plus pour le bon déroulement de ses activités. Source : https://cybersecurity.att.com
Infonuagique	On entend par **infonuagique** un modèle permettant l'accès réseau sur demande à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) pouvant être réservées et libérées par un minimum d'effort et d'interaction avec le fournisseur.
Intelligence artificielle (IA)	**L'intelligence artificielle** (IA) concerne l'utilisation d'ordinateurs pour imiter les fonctions cognitives des humains, donc la façon dont les systèmes peuvent réagir et se comporter dans certaines circonstances. Lorsque les machines effectuent des tâches qui

Terme	Contexte
	reposent sur des algorithmes de manière « intelligente », il s'agit alors d'IA. L'objectif est de simuler l'intelligence naturelle pour résoudre des problèmes complexes. Elle est utilisée principalement pour la prise de décisions. L'IA vise principalement à augmenter les chances de réussite, sans forcément améliorer la précision. Sources : DataScienceCentral.com, Hackernoon.com
Nuage public	**Le nuage public** s'entend d'un style de traitement informatique qui offre à des clients externes des capacités informatiques évolutives et souples en tant que service au moyen des technologies d'Internet, c'est-à-dire que le nuage public utilise les technologies de traitement informatique en nuage pour soutenir des clients qui sont à l'extérieur de l'organisation du fournisseur. L'utilisation du nuage public génère les types d'économies évolutifs et le partage des ressources, ce qui peut réduire les coûts et accroître le choix des technologies offertes. Du point de vue d'un organisme gouvernemental, l'utilisation du nuage public fait en sorte que toute organisation (peu importe le secteur d'activité ou le territoire) peut utiliser les mêmes services (p. ex. l'infrastructure, la plateforme ou les logiciels), sans toutefois garantir l'emplacement où seraient stockées et situées les données. Source : Gartner Aux fins du présent marché, le nuage public comprend les services et l'infrastructure virtuelle fournis par un fournisseur de services infonuagiques (comme AWS, Microsoft Azure et Google Cloud) qui sont accessibles sur le réseau Internet public.
Organisation du secteur public	Aux fins du présent marché, une **organisation du secteur public** est définie comme suit : tout ministère, toute agence ou toute société d'État fédéral; tout gouvernement provincial ou d'État; toute administration municipale (représentant une population de plus de 500 000 personnes).
Palmarès OWASP Top 10	Le **palmarès OWASP Top 10** est un important document de sensibilisation à la sécurité des applications. Il représente un large consensus sur les plus importants risques de sécurité envers les applications. Parmi les membres du projet, mentionnons les experts en sécurité de divers pays, qui ont mis en commun leur expertise afin de créer cette liste. Source : OWASP
Pare-feu de prochaine génération/	Les **pare-feu de prochaine génération** représentent une catégorie de pare-feu mis en œuvre dans des logiciels ou sur du matériel

Terme	Contexte
Pare-feu NG	informatique. Ils peuvent détecter et bloquer des attaques complexes en appliquant des mesures de sécurité au niveau du protocole, du port et de l'application. Contrairement aux pare-feu normaux, ils réalisent une inspection plus approfondie et plus intelligente. En outre, ils offrent d'autres fonctionnalités, telles que le soutien à l'intégration d'Active Directory l'inspection SSH et SSL et le filtrage de maliciels selon la réputation. Source : Techopedia
Sécurisé	Aux fins du présent marché, le terme « **sécurisé** » désigne les environnements ou les infrastructures qui sont nécessaires pour assurer la conformité à un des profils de sécurité suivants : • Protégé B, intégrité moyenne, disponibilité moyenne (PBMM) du gouvernement du Canada ou un niveau supérieur; • SECRET, intégrité moyenne, disponibilité moyenne du gouvernement du Canada ou un niveau supérieur; • FEDRAMP – Modéré ou élevé; • NIST SP 800-53 – Modéré ou élevé; • ISO 27001 et ISO 27017.
Solution d'entreprise	Les **solutions d'entreprise** sont conçues pour intégrer les multiples aspects des activités d'une entreprise par l'échange bilatéral d'information provenant de divers secteurs de processus opérationnels et des bases de données connexes. Elles permettent aux entreprises de récupérer et de distribuer des données essentielles à la mission dans l'organisation, offrant ainsi aux gestionnaires des renseignements sur l'exploitation en temps réel.
Technologies émergentes	Pour les besoins de ce marché, **les technologies émergentes** constituent des technologies de l'information qui sont caractérisées par une nouveauté radicale (dans les ***organisations du secteur public***), une croissance relativement rapide, une cohérence, une incidence importante, une incertitude et une ambiguïté. Elles comprennent notamment : ***l'intelligence artificielle (IA),*** l'intelligence augmentée, ***l'apprentissage automatique « (ML) »***, l'apprentissage profond « (DL) », les réseaux neuronaux « (NN) », l'automatisation robotisée des processus « (RPA) », la biométrie, l'analytique des données massives/l'analytique prédictive, l'identification par radiofréquence « (RFID) », le traitement automatique du langage naturel, les applications mobiles, la reconnaissance vocale et les robots conversationnels. Aux fins du présent marché, elles excluent toute forme de l'informatique en nuage sans les technologies susmentionnées.

Terme	Contexte
Vérification de sécurité	Une **vérification de sécurité** est un examen approfondi du programme de sécurité informatique et de cybersécurité d'une organisation dont le but est de garantir la mise en place de contrôles internes dans l'organisation pour prévenir ou atténuer convenablement les risques de cyberattaques : • en mesurant l'étendue de la conformité des politiques, des normes, des procédures et des processus concernant la documentation, la communication et le règlement des incidents de sécurité; • en évaluant les mécanismes actuels de surveillance et de production de rapports concernant les principales activités liées à la cybersécurité.

APPENDICE A DE L'ANNEXE A

PROCÉDURE D'ATTRIBUTION DE TÂCHES

1. Lorsqu'un besoin relatif à une tâche précise sera identifié, une version préliminaire du formulaire d'autorisation de tâches joint à l'appendice B de l'annexe A sera remise à l'entrepreneur. Lorsqu'il reçoit un formulaire d'autorisation de tâches, l'entrepreneur doit soumettre au responsable technique son offre de prix pour les catégories de ressources demandées d'après les renseignements contenus dans le formulaire d'autorisation de tâches, ainsi que la ou les ressources proposées connexes. L'offre de prix doit être signée et envoyée au Canada dans le délai de réponse précisé dans le formulaire d'autorisation de tâches. L'entrepreneur disposera d'un délai d'au moins deux jours ouvrables (ou tout autre délai plus long précisé dans le projet d'autorisation de tâches) pour présenter son offre de prix.

2. Avec chaque proposition de prix, l'entrepreneur doit proposer le nombre requis de ressources, et pour chaque ressource proposée, l'entrepreneur doit fournir un curriculum vitæ ainsi que les renseignements relatifs à l'attestation de sécurité demandée, et doit remplir les tableaux de réponse à l'appendice C de l'annexe A qui portent sur les catégories de ressources indiquées dans le projet d'autorisation de tâches. La même personne ne peut être proposée pour plus d'une catégorie de ressources. Les curriculum vitæ devraient montrer que chaque personne proposée répond aux exigences décrites en matière de qualification (y compris les exigences en matière d'études, d'expérience de travail et d'accréditation professionnelle). En ce qui a trait aux ressources proposées :

   (i) Les ressources proposées peuvent être des employés de l'entrepreneur ou des employés d'un sous-traitant, ou des entrepreneurs indépendants auxquels l'entrepreneur confierait une partie du travail en sous-traitance. (Se reporter à l'appendice D de l'annexe A, Attestations.)

   (ii) En ce qui concerne les exigences en matière d'études touchant un grade, un titre ou un certificat en particulier, le Canada ne tiendra compte que des programmes d'études ayant été réussis par la ressource avant la date d'émission du projet d'autorisation de tâches à l'entrepreneur.

   (iii) Pour les exigences relatives aux titres professionnels, la ressource doit détenir le titre ou l'accréditation exigé à la publication du projet d'autorisation de tâches et doit demeurer, le cas échéant, un membre en règle de l'organisme professionnel en question pendant la période d'évaluation et la durée du contrat. Lorsque l'affiliation ou le titre professionnel doit être démontré au moyen d'une certification, d'un diplôme ou d'un grade, ce document doit être à jour, valide et émis par l'entité précisée dans le présent contrat ou, si l'entité n'est pas précisée, par une entité, une institution ou un organisme reconnu ou accrédité au moment où le document a été émis.

   (iv) En ce qui concerne l'expérience de travail, le Canada ne tiendra pas compte de l'expérience acquise dans le cadre d'un programme de formation, sauf s'il s'agit d'expérience acquise dans le cadre d'un programme coopératif officiel dans un établissement postsecondaire.

   (v) Pour les exigences qui demandent un nombre précis d'années d'expérience (p. ex. deux ans), le Canada ne tiendra pas compte de cette expérience si le curriculum vitæ ne donne pas les dates précises (le mois et l'année) de l'expérience alléguée (c.-à-d. la date de début et la date de fin). Le Canada n'évaluera que la période au cours de laquelle la ressource a réellement travaillé au projet ou aux projets (de la date de début indiquée par la ressource jusqu'à la date de fin, plutôt qu'à partir de la date de début et de fin générale d'un projet ou d'un groupe de projets auxquels la ressource a participé).

   (vi) Le curriculum vitæ ne doit pas seulement indiquer le titre du poste occupé par la personne, mais doit également démontrer que cette personne a acquis l'expérience nécessaire en expliquant les responsabilités et les tâches effectuées à ce poste. Le fait

d'énumérer simplement l'expérience en ne fournissant aucune donnée à l'appui pour décrire les responsabilités et les tâches ainsi que leur pertinence par rapport aux exigences, ou le fait de réutiliser les mêmes expressions que le formulaire d'autorisation de tâches, ne sera pas considéré comme la « preuve » d'une expérience aux fins de cette évaluation. L'entrepreneur devrait fournir des détails complets concernant le lieu, les dates (le mois et l'année) et les activités ou responsabilités qui ont permis d'acquérir les qualifications et l'expérience citées. Advenant que la ressource proposée ait travaillé en même temps sur plus d'un projet, la durée de la période de chevauchement de ces projets ne sera prise en considération qu'une seule fois lors de l'évaluation de l'expérience.

3. On évaluera les qualifications et l'expérience des ressources proposées par rapport aux exigences établies à l'appendice C de l'annexe A, afin de déterminer si ces ressources satisfont aux critères obligatoires et cotés. Le Canada peut exiger une preuve selon laquelle la ressource proposée a suivi avec succès une formation officielle, ainsi que des références. Le Canada peut effectuer un contrôle des références pour vérifier l'exactitude des renseignements fournis. Le cas échéant, ce contrôle sera fait par courriel (sauf si la personne citée en référence n'est accessible que par téléphone). Le Canada n'attribuera aucun point à l'entrepreneur ou considérera qu'un critère obligatoire n'est pas satisfait s'il ne reçoit pas de réponse dans les cinq (5) jours ouvrables. Le troisième jour après l'envoi du courriel, si le Canada n'a pas reçu de réponse, il en informera l'entrepreneur par courriel pour que ce dernier puisse rappeler à la personne en question qu'il faut répondre au Canada dans le délai de cinq (5) jours ouvrables prescrit. Si les renseignements fournis par une personne citée en référence diffèrent des renseignements fournis par l'entrepreneur, les renseignements fournis par la personne citée en référence seront les renseignements évalués. On n'accordera aucun point à l'entrepreneur ou l'on considérera qu'un critère obligatoire n'est pas respecté si le client cité en référence n'est pas un client de l'entrepreneur lui-même (par exemple, le client ne peut pas être le client d'une filiale de l'entrepreneur). De même, on n'accordera aucun point à l'entrepreneur ou l'on considérera qu'un critère obligatoire n'est pas respecté si le client est lui-même une filiale ou une autre entité qui a un lien de dépendance avec l'entrepreneur. Des références de l'État seront acceptées.

4. Pendant l'évaluation des ressources proposées, si les références de deux ressources ou plus nécessaires dans le cadre de l'autorisation de tâches ne fournissent pas de réponse ou ne justifient pas les qualifications exigées pour la prestation des services requis, l'offre de prix pourrait être déclarée irrecevable.

5. Seules les offres qui respectent tous les critères obligatoires seront évaluées dans le cadre des critères cotés. Chaque ressource proposée doit obtenir une note minimale requise pour les critères cotés pour la catégorie de ressource applicable. Si la note d'une ressource proposée est inférieure à la note requise, l'offre de prix de l'entrepreneur sera jugée irrecevable.

6. Dès que l'offre de prix aura été acceptée par le responsable technique, le formulaire d'autorisation de tâches sera signé par le Canada et envoyé à l'entrepreneur, qui devra le signer. Le formulaire d'autorisation de tâches doit être dûment signé par le Canada avant le début des travaux. L'entrepreneur ne doit commencer les travaux qu'après avoir reçu un formulaire d'autorisation de tâches (l'autorisation de tâches) approuvé. Tous les travaux réalisés par l'entrepreneur sans formulaire d'autorisation de tâches le seront à ses risques.

APPENDICE B DE L'ANNEXE A

FORMULAIRE D'AUTORISATION DE TÂCHES

FORMULAIRE D'AUTORISATION DE TÂCHES	
Entrepreneur:	Numéro du contrat:
Nº d'autorisation de tâches :	Date:
Code financier:	Nº de modification :

1. ÉNONCÉ DES TRAVAUX (ACTIVITÉS DE TRAVAIL, ATTESTATIONS ET LIVRABLES)

CONTEXTE

TÂCHES

PRODUITS LIVRABLES

RESSOURCES/BESOINS TECHNOLOGIQUES ESSENTIELS

( ) (À déterminer dans l'autorisation de tâches)
( ) (À déterminer dans l'autorisation de tâches)
( ) (À déterminer dans l'autorisation de tâches)
( ) (À déterminer dans l'autorisation de tâches)
( ) (À déterminer dans l'autorisation de tâches)

Le Responsable Technique:
Courriel :

Le responsable technique est le représentant de TC (ou son délégataire) qui est responsable de la gestion de la présente AT. Toute modification apportée à l'AT doit être autorisée par écrit par le représentant de l'équipe d'approvisionnement de TC et par le chargé de projet, s'il y a lieu. L'entrepreneur ne doit pas exécuter de tâches qui ne sont pas prévues dans l'AT ou qui dépassent la portée de l'AT, à la suite de demandes d'instructions orales ou écrites provenant de membres du personnel du gouvernement autre que le représentant susmentionné.

VEUILLEZ TRANSMETTRE LES FACTURES À LA PERSONNE SUIVANTE :

Le Responsable Technique:
Courriel :

Le responsable technique (ou son délégataire) est responsable de toutes les questions reliées aux aspects techniques des travaux prévus dans la présente AT. Toutes les modifications proposées à l'égard de la portée des travaux doivent faire l'objet de discussions avec le responsable technique, mais ne sont applicables et exécutoires que si elles sont confirmées par écrit dans un avis écrit de modification d'AT délivré par le responsable technique ou par l'autorité contractante de TPSGC.

2. PÉRIODE	**DE (**DATE):	**À (**DATE):

3. LIEU DE TRAVAIL	
4. EXIGENCES RELATIVES AUX DÉPLACEMENTS	
5. EXIGENCES LINGUISTIQUES	
6. COTE DE SÉCURITÉ REQUISE	

7. COÛT

CATÉGORIE	NOM DE LA RESSOURCE	TARIF JOURNALIER	NOMBRE ESTIMATIF DE JOURS	COÛT TOTAL
				$
			COÛT ESTIMATIF	**$**
			TAXES APPLICABLES	$
			SOUS-TOTAl	$
			FRAIS DE DÉPLACEMENT ET DE SUBSISTANCE (INCLUANT LES TAXES APPLICABLES)	$
			TOTAL	$

8 SIGNATURES

Responsable Technique:	**Signature:** **Au dossier**	**Date:**
Autorité contractante	**Signature:**	**Date:**

Cocher l'un des énoncés suivants :

___ L'entrepreneur accepte la présente autorisation de tâches

___ L'entrepreneur n'accepte pas la présente autorisation de tâches

Nom du signataire autorisé de l'entrepreneur (caractères d'imprimerie)	**Titre du poste du signataire autorisé de l'entrepreneur (caractères d'imprimerie)**	**Date:**
Signature:		

APPENDICE C DE L'ANNEXE A

CRITÈRES D'ÉVALUATION DES RESSOURCES ET TABLEAU DE RÉPONSE

Pour faciliter l'évaluation des ressources, les entrepreneurs doivent préparer et soumettre leur réponse à un projet d'autorisation de tâches en utilisant les tableaux fournis dans la présente annexe. Aux fins de l'établissement des grilles de ressources, les entrepreneurs devraient fournir des renseignements précis démontrant le respect des critères établis et un renvoi au numéro de page approprié du curriculum vitæ, de façon à ce que le Canada puisse vérifier ces renseignements. Les tableaux ne devraient pas renfermer toutes les données du projet provenant du curriculum vitæ. Seule la réponse demandée doit être fournie.

Pour démontrer la conformité à tous les critères, l'entrepreneur doit inclure les renseignements suivants :

- le nom du projet;
- (*) l'organisation cliente;
  des renseignements sur le client (*), dont le nom de l'organisation, le nom, le titre, l'adresse, le numéro de téléphone et l'adresse courriel de la personne-ressource.

  (*) La personne-ressource doit être une personne étant ou ayant été employé de l'organisation cliente et pouvant confirmer tous les renseignements;
- les dates de début et de fin du projet et la durée de celui-ci;
- la description du projet;
- la description du rôle et des tâches exécutées par la ressource.

La terminologie suivante est utilisée dans les critères d'évaluation :

***démontrer :** le candidat doit clairement démontrer dans son CV la façon dont il ou elle satisfait aux critères. Le simple fait d'énoncer qu'il ou elle y satisfait ne suffira pas pour remplir les critères.

***Expérience pratique :** lorsque ce terme est employé pour définir un critère, cela signifie que la ressource a personnellement exécuté une activité ou une tâche de façon autonome. La ressource n'a pas collaboré ni participé à la tâche, elle ne l'a pas non plus dirigée ni supervisée (ou l'utilisation de verbes de signification semblable), sauf mention contraire explicitement énoncée dans le critère. La ressource a travaillé à l'exécution directe de l'activité avec la technologie « au clavier ».

NOTE À L'INTENTION DE L'ENTREPRENEUR : les termes indiqués en ***caractères gras italiques*** sont définis dans le glossaire.

1.0 CRITÈRES OBLIGATOIRES D'ÉVALUATION DES RESSOURCES :

(Volet 6 : Services de Cyber Protection de SPICT

C.1 — Conseiller en protection et en planification stratégiques de la sécurité des technologies de l'information – niveau 2

Catégorie de ressource : C.1 — Conseiller en protection et en planification stratégiques de la sécurité des technologies de l'information – niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O1.1	L'entrepreneur doit démontrer que la ressource a acquis une expérience au cours des cinq (5) dernières années de l'exécution d'un (1) projet impliquant le développement de logiciel et la sécurité des applications, et l'un des domaines suivants : • sécurité infonuagique; • sécurité des points terminaux; • gestion de l'identité et de l'accès. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O1.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, au moins quatre (4) années d'expérience au cours desquelles il a effectué toutes les tâches suivantes : • fournir des services de consultation et de planification stratégique sur la sécurité informatique; • réaliser des études de faisabilité, des évaluations des technologies et des analyses de rentabilité, et proposer des plans de mise en œuvre des systèmes liés à la sécurité informatique; • soutenir le développement d'une vision, de stratégies et de concepts relatifs à l'architecture de sécurité stratégique informatique; • soutenir le développement de programmes et la conception de services en matière de sécurité informatique. Remarque : L'expérience requise est un total combiné, cependant un minimum de 1 an doit être démontré pour chaque tâche. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

Catégorie de ressource : C.1 — Conseiller en protection et en planification stratégiques de la sécurité des technologies de l'information – niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O1.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, une expérience de travail avec les directives du CSEC en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33*) pour la génération d'exigences de sécurité propre à un projet pour deux (2) projets GI-TI ayant impliqué le traitement de **données protégées.** Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.1 Conseiller en planification et protection stratégiques de la sécurité des technologies de l'information, niveau 3

Catégorie de ressource : C.1 Conseiller en protection et en planification stratégique de la sécurité des TI, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O2.1	L'entrepreneur doit démontrer que la ressource proposée a acquis une expérience, au cours des cinq (5) dernières années, de l'exécution de deux (2) projets impliquant le développement de logiciels et la sécurité des applications, et l'un des domaines suivants : • sécurité infonuagique; • sécurité des points terminaux; • gestion de l'identité et de l'accès. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O2.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, au moins sept (7) années d'expérience au cours desquelles elle a effectué toutes les tâches suivantes : • fournir des services de consultation et de planification stratégique sur la sécurité informatique;	

Catégorie de ressource : C.1 Conseiller en protection et en planification stratégique de la sécurité des TI, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• réaliser des études de faisabilité, des évaluations des technologies et des analyses de rentabilité, et proposer des plans de mise en œuvre des systèmes liés à la sécurité informatique; • soutenir le développement d'une vision, de stratégies et de concepts relatifs à l'architecture de sécurité stratégique informatique; • soutenir le développement de programmes et la conception de services en matière de sécurité informatique. Remarque : L'expérience requise est un total combiné, cependant un minimum de 1 an doit être démontré pour chaque tâche. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O2.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, une expérience de travail avec les directives du CSEC en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)* pour la génération d'exigences de sécurité propre à un projet pour trois (3) projets GI-TI ayant impliqué le traitement de ***données protégées*.** Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des TI, niveau 2

Catégorie de ressource : C.6 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des TI, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O3.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, au moins quatre (4) années d'expérience au cours desquelles elle a exécuté des	

Catégorie de ressource : C.6 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des TI, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	activités de gestion de risques associés aux TI (*) impliquant trois des domaines suivants : • développement de logiciels et sécurité des applications; • sécurité infonuagique; • sécurité des points terminaux; • gestion de l'identité et de l'accès; • sécurité des réseaux et des communications. (*) Voir les directives en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI du CSTC : Une méthode axée sur le cycle de vie (ITSG-33)* Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O3.2	L'entrepreneur doit démontrer que la ressource proposée a acquis douze (12) mois d'expérience de l'exécution d'évaluations des menaces et des risques liés à la sécurité informatique pour des systèmes de TI **sécurisés** en utilisant la méthodologie harmonisée d'évaluation des menaces et des risques (EMR) (EMR-1) ainsi que les directives en matière de sécurité des technologies de l'information *La gestion de risques liés à la sécurité des TI du CSTC : Une méthode axée sur le cycle de vie* (ITSG-33). Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information, niveau 3

Catégorie de ressource : Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O4.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des quinze (15) dernières années, au moins sept (7) années d'expérience au cours desquelles elle a exécuté	

Catégorie de ressource : Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	des activités de gestion de risques associés aux TI (*) impliquant les domaines suivants : • développement de logiciels et sécurité des applications; • sécurité infonuagique; • sécurité des points terminaux; • gestion de l'identité et de l'accès; • sécurité des réseaux et des communications. (*) Voir les directives en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI du CSTC : Une méthode axée sur le cycle de vie (ITSG-33)* Remarque : L'expérience requise est un total combiné, cependant un minimum de six (6) mois doit être démontré pour chaque activité. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O4.2	L'entrepreneur doit démontrer que la ressource proposée a acquis trois (3) années d'expérience de l'exécution d'évaluations des menaces et des risques liés à la sécurité informatique pour des systèmes de TI **sécurisés** en utilisant la méthodologie harmonisée d'évaluation des menaces et des risques (EMR) du CSTC (EMR-1) ainsi que les directives du *CSTC* en matière de sécurité des technologies de l'information *La gestion de risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33). Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.7 Spécialiste en conception de la sécurité des technologies de l'information, niveau 2

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O5.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, au moins quatre (4) années d'expérience pratique (*) dans la planification, le développement et la mise en œuvre d'architectures de sécurité informatique ou de concepts de sécurité informatique pour des applications ou des systèmes d'information complexes (**) impliquant les domaines suivants : • développement de logiciels et sécurité des applications; • sécurité infonuagique; • sécurité des points terminaux; • gestion de l'identité et de l'accès; • sécurité des réseaux et des communications. (*) L'expérience requise est un total combiné, cependant un minimum de 1 an est exigé en développement de logiciels et sécurité des applications. (**) On entend par « complexe » un groupe de systèmes en interaction et interreliés. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O5.2	L'entrepreneur doit démontrer que la ressource proposée a acquis une expérience pratique dans le cadre d'au moins deux (2) projets au cours desquels elle a développé au moins trois (3) des types d'artefacts d'ingénierie des systèmes suivants : • documents sur l'architecture; • spécifications des exigences du système; • spécifications de la conception du système; • documents sur la conception et la configuration; • concept des opérations (CONOPS); • plans de mise en œuvre du système; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.7 Spécialiste en conception de la sécurité des technologies de l'information, niveau 3

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O6.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des quinze (15) dernières années, au moins sept (7) années d'expérience pratique (*) de la planification, du développement et de la mise en œuvre d'architectures de sécurité informatique ou de concepts de sécurité informatique pour des applications ou des systèmes d'information complexes (**) impliquant les domaines suivants : • développement de logiciels et sécurité des applications; • sécurité infonuagique; • sécurité des points terminaux; • gestion de l'identité et de l'accès; • sécurité des réseaux et des communications. (*) L'expérience requise est un total combiné, cependant un minimum de deux (2) années d'expérience sont exigées en développement de logiciels et sécurité des applications. (**) On entend par « complexe » un groupe de systèmes en interaction et interreliés. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O6.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des six (6) dernières années, au moins une (1) année d'expérience pratique dans l'élaboration et la livraison de stratégies, de solutions et de propositions en matière de sécurité informatique visant à résoudre des problèmes en matière des TI et de sécurité affectant plusieurs parties prenantes et architectures de sécurité. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O6.3	L'entrepreneur doit démontrer que la ressource proposée a acquis une expérience pratique dans le cadre d'au moins deux (2) projets au cours desquels elle a développé au moins trois (3) des types d'artefacts d'ingénierie des systèmes suivants : • documents sur l'architecture; • spécifications des exigences du système • spécifications de la conception du système; • documents sur la conception et la configuration; • concept des opérations (CONOPS)	

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité, niveau 3 Nom de la ressource proposée : _____		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• plans de mise en œuvre du système; • plans et rapports de mise à l'essai; • plans de soutien du cycle de vie. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.8 Analyste de la sécurité des réseaux (niveau 2)

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux (niveau 2) Nom de la ressource proposée : _____		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O7.1	L'entrepreneur doit démontrer que la ressource proposée a acquis cinq (5) années d'expérience pratique au cours desquelles elle a effectué toutes les activités suivantes : • ***configuration***[2] et soutien de logiciels de gestion automatisée de la sécurité informatique; • ***configuration***[2] et soutien en matière de pare-feu, de routeurs et d'équilibreurs de charge; • conception et soutien en matière de basculement et de reprise de réseaux à l'aide d'une infrastructure sous forme de code : • ***configuration***[2] et soutien en matière d'informatique élastique. • ***configuration***[2] et soutien de groupes de sécurité et de listes de contrôle d'accès. • conception de routes définies par l'utilisateur pour forcer une tunnelisation. • ***configuration***[2] et intégration d'infrastructures de réseaux à l'aide d'une ***configuration***[1] en nuage hybride Remarque : Les projets ne nécessitent pas toutes les activités, cependant une expérience dans l'exécution de **toutes** les activités doit être démontrée. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux (niveau 2) **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O7.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, six (6) mois d'expérience pratique de la ***configuration[2]*** et du soutien d'environnements ***sécurisés*** de production ***infonuagiques***. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O7.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des huit (8) dernières années, dix-huit mois (18) mois d'expérience du déploiement et du soutien de la sécurité de réseaux sur une infrastructure de ***nuage public*** externalisé. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
07.4	L'entrepreneur doit démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « Systems Security Certified Professional (SSCP) »; • « Information Technology Infrastructure Library (ITIL) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA » Cloud+; • « CompTIA Network+ »; • « CompTIA Security+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.	

C.8 Analyste de la sécurité des réseaux, niveau 3

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O8.1	L'entrepreneur doit démontrer que la ressource proposée a acquis sept (7) années d'expérience pratique au cours desquelles il a effectué toutes les activités suivantes : • ***configuration***[2] et soutien de logiciels de gestion automatisée de la sécurité informatique; • ***configuration***[2] et soutien en matière de pare-feu, de routeurs et d'équilibreurs de charge; • conception et soutien en matière de basculement et de reprise de réseaux à l'aide d'une infrastructure sous forme de code : • ***configuration***[2] et soutien en matière d'informatique élastique. • ***configuration***[2] et soutien de groupes de sécurité et de listes de contrôle d'accès. • conception de routes définies par l'utilisateur pour forcer une tunnelisation. • ***configuration***[2] et intégration d'infrastructures de réseaux à l'aide d'une ***configuration***[1] de nuage hybride Remarque : Les projets ne nécessitent pas toutes les activités, cependant une expérience dans l'exécution de **toutes** les activités doit être démontrée. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O8.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, dix-huit (18) mois d'expérience pratique de la conception ou de l'évaluation d'architecture de sécurité des réseaux ou de produits de sécurité pour des environnements ***sécurisés*** de production ***infonuagiques***. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O8.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des huit (8) dernières années, trois (3) années d'expérience du déploiement et du soutien de la sécurité de réseaux sur une infrastructure de fournisseurs de services de ***nuages publics*** externalisés.	

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O8.4	L'entrepreneur doit démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « Systems Security Certified Professional (SSCP) »; • « Information Technology Infrastructure Library (ITIL) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Network+ »; • « CompTIA Security+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.	

C.9. Opérateur de systèmes de sécurité des technologies de l'information, Niveau 2

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O9.1	L'entrepreneur doit démontrer que la ressource proposée a acquis cinq (5) années d'expérience pratique au cours desquelles elle a effectué toutes les activités suivantes : • utilisation d'outils de gestion des incidents et événements de sécurité;	

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• utilisation d'outils de surveillance en nuage y compris le « AWS Security Hub »ou Azure Sentinel. (*) L'expérience requise est un total combiné, cependant un minimum de dix-huit (18) mois est obligatoire pour chacune des activités. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O9.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, six (6) mois d'expérience pratique de la surveillance de la sécurité d'environnements ***sécurisés*** de production ***infonuagiques***. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O9.3	L'entrepreneur doit démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « Systems Security Certified Professional (SSCP) »; • « Information Technology Infrastructure Library (ITIL) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Cloud+ »; • « CompTIA Network+ »; • « CompTIA Security+ »; • « CompTIA Server+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur; • « Certified Windows Security Administrator »; • « Certified UNIX Security Administrator »; • « Certified Detection Analyst »; • « Certified Incident Handler ».	

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**

C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes niveau 3

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes - niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O10.1	L'entrepreneur doit démontrer que la ressource proposée a acquis dix (10) années d'expérience pratique au cours desquelles elle a effectué les activités suivantes : • utilisation d'outils de gestion des incidents et événements de sécurité; • utilisation d'outils de surveillance en nuage y compris le « AWS Security Hub » ou Azure Sentinel. (*) L'expérience requise est un total combiné, cependant un minimum de trois (3) années est obligatoire pour chacune des activités. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O10.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, dix-huit (18) mois d'expérience pratique de la surveillance de la sécurité d'environnements ***sécurisés*** de production ***infonuagiques***. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O10.3	L'entrepreneur doit démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »;	

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes - niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « Systems Security Certified Professional (SSCP) »; • « Information Technology Infrastructure Library (ITIL) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Cloud+ »; • « CompTIA Network+ »; • « CompTIA Security+ »; • « CompTIA Server+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur; • « Certified Windows Security Administrator »; • « Certified UNIX Security Administrator »; • « Certified Detection Analyst »; • « Certified Incident Handler ».	

C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 2

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O11.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des cinq (5) dernières années, au moins deux (2) années d'expérience de la conduite d'***analyses des vulnérabilités*** et d'***essais de pénétration*** en matière de sécurité informatique.	
O11.2	L'entrepreneur doit démontrer que la ressource proposée possède une certification professionnelle actuelle dans l'une des suivantes :	

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• « AWS Certified Security Specialty »; • « Microsoft Azure Security Technologies »; • « MCSE: Cloud Platforms and Infrastructure »; • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) » d'ISC2; • « CompTIA » Security+; • « CompTIA » Network+; • « CompTIA » Cloud+; • « CompTIA » CySA+; • « CompTIA » PenTest+; • « Certified Wireless Security Professional (CWSP) »; • « GIAC » toute certification « Cloud Security »; • « GIAC » toute certification « Cyber Defense »; • « GIAC » toute certification « Offensive Operations »; • « GIAC Security Expert (GSE) Certification »; • « Certified Windows Security Administrator »; • « Certified UNIX Security Administrator »; • « Certified Vulnerability Assessor (CVA) »; • « EC Council Certified Ethical Hacker ».	
O11.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des trois (3) dernières années, une expérience pratique de l'exécution d'***analyses des vulnérabilités*** et d'***essais de pénétration*** pour un environnement, un service ou une solution informatique en ***nuage public sécurisé*** pour le compte d'une ***organisation du secteur public***, y compris **toutes** les activités suivantes : • effectuer une évaluation des actifs et des données concernés; • effectuer des analyses des vulnérabilités exhaustives et des essais de pénétration pour cerner les vulnérabilités susceptibles de rendre l'organisation ou les données vulnérables aux menaces ou au vol; • utiliser des outils automatisés d'évaluation de vulnérabilité; • dresser une liste, par ordre de priorité, des lacunes pouvant donner à des mesures avec explications et recommandations techniques.	

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	Afin d'être retenu, un projet doit comprendre toutes les activités.	

C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 3

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O12.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des huit (8) dernières années, au moins cinq (5) années d'expérience pratique de la conduite d'***analyses des vulnérabilités*** et d'***essais de pénétration*** en matière de sécurité informatique.	
O12.2	L'entrepreneur doit démontrer que la ressource proposée possède une certification professionnelle actuelle dans l'une des catégories suivantes : • « AWS Certified Security Specialty »; • « Microsoft Azure Security Technologies »; • « MCSE: Cloud Platforms and Infrastructure »; • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) » d'ISC2; • « CompTIA » Security+; • « CompTIA » Network+; • « CompTIA » Cloud+; • « CompTIA » CySA+; • « CompTIA » PenTest+; • « Certified Wireless Security Professional (CWSP) »; • « GIAC » toute certification « Cloud Security »; • « GIAC » toute certification « Cyber Defense »; • « GIAC » toute certification « Offensive Operations »; • « GIAC Security Expert (GSE) Certification »;	

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• « Certified Windows Security Administrator »; • « Certified UNIX Security Administrator »; • « Certified Vulnerability Assessor (CVA) »; • « EC Council Certified Ethical Hacker » • « SANS Mobile Device Security and Ethical Hacking ».	
O12.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des trois (3) dernières années, une (1) année d'expérience pratique de l'exécution d'***analyses des vulnérabilités*** et d'***essais de pénétration*** pour des environnements, des services ou des solutions informatiques en ***nuage public sécurisé*** pour le compte d'au moins deux (2) organisations distinctes du secteur public (*), y compris **toutes** les activités suivantes : • effectuer une évaluation des actifs et des données concernés; • effectuer des ***analyses des vulnérabilités*** exhaustives et des ***essais de pénétration*** pour cerner les vulnérabilités susceptibles d'exposer l'organisation ou les données aux menaces ou au vol; • utiliser des outils automatisés d'évaluation de vulnérabilité; • dresser une liste, par ordre de priorité, des lacunes pouvant donner à des mesures avec explications et recommandations techniques. Afin d'être retenu, un projet doit comprendre toutes les activités. (*) Voir ***organisations du secteur public*** dans le glossaire	

C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 2

Catégorie de ressource : C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O13.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des quinze (15) dernières années, au moins quatre (4) années d'expérience pratique (*) de la planification, du développement et de la mise en œuvre d'architectures de sécurité informatique ou de concepts de sécurité informatique pour des applications ou des systèmes d'information complexes (**) impliquant trois des domaines suivants : • développement de logiciels et sécurité des applications; • infrastructure et plateformes en nuage; • sécurité des points terminaux; • gestion de l'identité et de l'accès; • sécurité des réseaux et des communications. (*) L'expérience requise est un total combiné, cependant un minimum de dix-huit (18) mois d'expérience sont exigées en développement de logiciels et sécurité des applications. (**) On entend par « complexe » un groupe de systèmes en interaction et interreliés. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O13.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des six (6) dernières années, un minimum de six (6) mois d'expérience pratique dans la recherche, l'évaluation, la conception ou la mise à l'essai de solutions intégrées sécurisées (*) impliquant à la fois des ***données protégées*** et des ***technologies émergentes***. (*) Comprend des prototypes fonctionnels. Les solutions doivent à tout le moins avoir été développées et mises en œuvre jusqu'à la phase de mise à l'essai impliquant des données de production. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O13.3	L'entrepreneur doit démontrer que la ressource proposée compte au moins une (1) année d'expérience au cours de laquelle elle a effectué des travaux de recherche, conseillé et guidé des architectes et développeurs de solutions relativement à l'intégration et à l'application, à même des solutions, d'améliorations en matière de sécurité.	

Catégorie de ressource : C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 2 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 3

Catégorie de ressource : C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
O14.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des quinze (15) dernières années, au moins sept (7) années d'expérience pratique (*) de la planification, du développement et de la mise en œuvre d'architectures de sécurité informatique ou de concepts de sécurité informatique pour des applications ou des systèmes d'information complexes (**) impliquant les domaines suivants : • développement de logiciels et sécurité des applications; • infrastructure et plateformes en nuage; • sécurité des points terminaux; • gestion de l'identité et de l'accès; • sécurité des réseaux et des communications. (*) L'expérience requise est un total combiné, cependant un minimum de trois (3) années d'expérience sont exigées en développement de logiciels et sécurité des applications. (**) On entend par « complexe » un groupe de systèmes en interaction et interreliés. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O14.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des six (6) dernières années, un minimum de deux (2) années d'expérience pratique dans la recherche, l'évaluation, la conception et la mise à l'essai de solutions	

Catégorie de ressource : C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 3 **Nom de la ressource proposée : _____**		
Critère	**Exigence obligatoire**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	intégrées sécurisées (*) impliquant à la fois des ***données protégées*** et des ***technologies émergentes***. (*) Comprend des prototypes fonctionnels. Les solutions doivent à tout le moins avoir été développées et mises en oeuvre jusqu'à la phase de mise à l'essai impliquant des données de production. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O14.3	L'entrepreneur doit démontrer que la ressource proposée compte au moins cinq (5) années d'expérience au cours desquelles elle a effectué des travaux de recherche, conseillé et guidé des architectes et développeurs de solutions relativement à l'intégration et à l'application, à même des solutions, d'améliorations en matière de sécurité. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 2

Catégorie de ressource : C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 2 **Nom de la ressource proposée : _____**		
O15.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des dix (10) dernières années, au moins quatre (4) années d'expérience au cours desquelles elle a effectué des évaluations des facteurs relatifs à la vie privée (EFVP). Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O15.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des six (6) dernières années, au moins dix-huit (18) mois d'expérience au cours desquels il a effectué toutes les tâches suivantes : • effectuer des évaluations des facteurs relatifs à la vie privée (EFVP) sur des infrastructures et systèmes informatiques pour le compte d'un client du secteur public du Canada (fédéral, provincial, territorial, municipal, ou société d'État) ou d'un important (*) client commercial établi au Canada;	

Catégorie de ressource : C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 2 **Nom de la ressource proposée : _____**		
	• cerner et atténuer les menaces et risques associés au traitement de différents types de renseignements dont des renseignements personnels, commerciaux et financiers et autres données sensibles; • appliquer des politiques et des procédures concernant l'accès, la rétention, le stockage, l'utilisation, le transfert et l'élimination de documentation relative à des renseignements permettant d'identifier une personne; • développer et mener des évaluations des facteurs relatifs à la vie privée en fonction de pratiques exemplaires; • cerner les risques d'atteinte à la vie privée associés à l'intégration d'ensemble de données provenant de différents systèmes afin d'obtenir, de récupérer et de synchroniser des renseignements aux fins de travaux d'exploration et de recherche de données; • appliquer la législation et les règlements sur la vie privée tels que : o la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP); o la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP); o la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ). • appliquer des concepts en matière de sécurité et de vie privée; appliquer des processus d'authentification des utilisateurs et déterminer, définir et attribuer des rôles en matière de sécurité. (*) S'entend par « important » une organisation comptant 500 employés ou plus. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 3

Catégorie de ressource : C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 3 **Nom de la ressource proposée : _____**		
O16.1	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des douze (12) dernières années, au moins sept (7) années d'expérience au cours desquelles elle a effectué des évaluations des facteurs relatifs à la vie privée (EFVP).	

Catégorie de ressource : C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 3 **Nom de la ressource proposée : _____**		
	Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	
O16.2	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des six (6) dernières années, au moins trois (3) années d'expérience au cours desquelles il a effectué toutes les tâches suivantes : • effectuer des évaluations des facteurs relatifs à la vie privée (EFVP) sur des infrastructures et systèmes informatiques pour le compte d'un client du secteur public du Canada (fédéral, provincial, territorial, municipal, ou société d'État) ou d'un important (*) client commercial établi au Canada; • cerner et atténuer les menaces et risques associés au traitement de différents types de renseignements dont des renseignements personnels, commerciaux et financiers et autres données sensibles; • appliquer des politiques et des procédures concernant l'accès, la rétention, le stockage, l'utilisation, le transfert et l'élimination de documentation relative à des renseignements permettant d'identifier une personne; • développer et mener des évaluations des facteurs relatifs à la vie privée en fonction de pratiques exemplaires; • cerner les risques d'atteinte à la vie privée associés à l'intégration d'ensembles de données provenant de différents systèmes afin d'obtenir, de récupérer et de synchroniser des renseignements aux fins de travaux d'exploration et de recherche de données; • appliquer la législation et les règlements sur la vie privée tels que : o la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP); o la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP); o la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ). • appliquer des concepts en matière de sécurité et de vie privée; appliquer des processus d'authentification des utilisateurs et déterminer, définir et attribuer des rôles en matière de sécurité. (*) S'entend par « important » une organisation comptant 500 employés ou plus. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	

2.0 CRITÈRES COTÉS D'ÉVALUATION DES RESSOURCES

Volet 6 : Services de Cyber Protection de SPICT

C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 2

Catégorie de ressource : C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C1.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	15	Aucun diplôme = 0 point Diplôme = 15 points **Note maximale : 15 points**	
C1.2	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified ISO 27001 Lead Implementer »; • « Certified Information Systems Auditor (CISA) »; • « Certified Information Security Manager (CISM) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Cloud Security Alliance Cloud Security Knowledge (CCSK) »;	20	Pas de certification = 0 point Une certification = 10 points Deux certifications ou plus = 20 points **Note maximale : 20 points**	

Catégorie de ressource : C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• « GIAC »/toute certification intermédiaire ou avancée en cybersécurité « GIAC »/toute certification intermédiaire ou avancée en cyberdéfense; • « Payment Card Industry – Qualified Security Assessor (PCI-QSA) »; • « System Security Certified Practitioner (SSCP) »; • « Control Objectives for Information & related Technology (COBIT) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA CySA+ »; • « Sherwood Applied Business Security Architecture (SABSA) ».			
C1.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Information Technology Infrastructure Library (ITIL) »; • « Information Technology Service Management (ITSM) » ; • Gestion de projets.	5	Pas de certification = 0 point Certification = 5 points **Note maximale : 5 points**	

Catégorie de ressource : C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
Maximum de points possibles				40
Nombre minimal de points requis (65 %)				26
La note de l`entrepreneur				

C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 3

Catégorie de ressource : C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C2.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C2.2	L'entrepreneur devrait démontrer que la ressource proposée détient : • une maîtrise en sécurité des technologies de l'information, en cybersécurité et renseignement sur les menaces ou dans une discipline similaire, d'une université canadienne reconnue; OU • une ***évaluation canadienne des diplômes d'études*** équivalents,	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 3

Nom de la ressource proposée : _____

Nº	Exigence cotée	Nombre maximal de points	Échelle de points	Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV
	s'ils sont obtenus à l'extérieur du Canada.			
C2.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified ISO 27001 Lead Implementer »; • « Certified Information Systems Auditor (CISA) »; • « Certified Information Security Manager (CISM) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Cloud Security Alliance Cloud Security Knowledge (CCSK) »; • « GIAC »/toute certification intermédiaire ou avancée en cybersécurité; • « GIAC »/toute certification intermédiaire ou avancée en cyberdéfense; • « Payment Card Industry – Qualified Security Assessor (PCI-QSA) »; • « System Security Certified Practitioner (SSCP) »; • « Control Objectives for Information & related Technology (COBIT) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA CySA+ » • « Sherwood Applied Business Security Architecture (SABSA) ».	30	Pas de certification = 0 point 1 certification = 10 points 2 certifications = 20 points 3 certifications ou plus = 30 points Maximum de 30 points **Note maximale : 30 points**	

Catégorie de ressource : C.1 Consultant en protection et en planification stratégique de la sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C2.4	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications suivantes : • « Information Technology Infrastructure Library (ITIL) »; • « Information Technology Service Management (ITSM); • Gestion de projets.	5	Pas de certification = 0 point Certification = 5 points **Note maximale : 5 points**	
Maximum de points possibles				55
Nombre minimal de points requis (65 %)				35
La note de l`entrepreneur				

C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 2

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C3.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C3.2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience pratique au cours des cinq (5) dernières années et qu'elle a préparé les produits livrables suivants :	30	Les points seront attribués une fois pour chaque type de produit répondant aux critères :	

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 2

Nom de la ressource proposée : _____

Nº	Exigence cotée	Nombre maximal de points	Échelle de points	Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV
	- (ES) Énoncés de sensibilité pour les systèmes informatiques traitant des renseignements protégés ou classifiés selon la méthodologie harmonisée d'évaluation des menaces et des risques (EMR) du CSTC (EMR1). - (EMR) Évaluations de la menace et des risques pour la sécurité des TI à l'appui des systèmes de TI traitant des renseignements protégés ou classifiés à l'aide de la méthodologie harmonisée d'évaluation de la menace et des risques (EMR) du CSTC (EMR-1). - (ESA / C et A) Trousses d'évaluation et autorisation de sécurité / de certification et d'attestation pour les systèmes de TI traitant des renseignements protégés ou classifiés selon la méthodologie et la terminologie d'ESA des directives en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI* du CSTC : *une méthode axée sur le cycle de vie* (ITSG-33). - (EST-P) Examens de sécurité technique* de produits matériels ou logiciels commerciaux. *Chaque EST-P peut être défini comme contenant tous les éléments suivants : - renseignements fonctionnels sur le produit; - renseignements techniques sur le produit; - évaluation de la sécurité des caractéristiques de sécurité offertes par le produit; - évaluation de la vulnérabilité; et - recommandations. - (TI-ARS) Rapports d'analyse concernant les répercussions sur la sécurité* pour les solutions informatiques. *On peut définir les rapports d'analyse concernant les répercussions sur la		ES = 5 points EMR = 5 points ESA / C et A = 5 points EST-P = 5 points TI-ARS = 5 points TIES-Nuage = 5 points **Note maximale : 30 points**	

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	sécurité comme des documents contenant tous les éléments suivants : - type de produits livrables de sécurité; - estimation des efforts à fournir; - estimation des coûts. - (TIES-nuage) Évaluations de la sécurité des TI sur des solutions informatiques configurées à l'aide d'un modèle ***infonuagique***.			
C3.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications valides suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA CySA+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.	10	Pas de certification = 0 point 1 certification = 5 points 2 certifications ou plus = 10 points **Note maximale : 10 points**	
C3.4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience des activités de gestion des	15	5 points par projet	

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	risques sur des applications infonuagiques pour des projets et des initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves; • infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité infonuagique; • expérience multisensorielle ou mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.		**Note maximale : 15 points**	
Maximum de points possibles				65
Nombre minimal de points requis (65 %)				42
La note de l`entrepreneur				

C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 3

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C4.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.			
C4.2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience pratique acquise au cours des cinq (5) dernières années et qu'elle a préparé au moins deux des produits livrables suivants : - (ES) Énoncés de sensibilité pour les systèmes informatiques traitant des renseignements protégés ou classifiés selon la méthodologie harmonisée d'évaluation des menaces et des risques (EMR) du CSTC (EMR1). - (EMR) Évaluations de la menace et des risques pour la sécurité des TI à l'appui des systèmes de TI traitant des renseignements protégés ou classifiés à l'aide de la méthodologie harmonisée d'évaluation de la menace et des risques (EMR) du CSTC (EMR-1). - (ESA / C et A) Trousses d'évaluation et autorisation de sécurité / de certification et d'attestation pour les systèmes de TI traitant des renseignements protégés ou classifiés selon la méthodologie et la terminologie d'ESA des directives en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI* du CSTC : *une méthode axée sur le cycle de vie* (ITSG-33). - (EST-P) Examen de la sécurité technique* des produits matériels ou logiciels commerciaux. *Chaque EST-P peut être défini comme contenant tous les éléments suivants : - renseignements fonctionnels sur le produit;	30	Les points seront attribués pour deux ou plusieurs de chaque type de produit livrable satisfaisant aux critères, jusqu'à concurrence du nombre maximal de points pour ce type de produit livrable : ES = 5 points EMR = 5 points ESA / C et A = 5 points EST-P = 5 points TI-ARS = 5 points TIES-Nuage = 5 points **Note maximale : 30 points**	

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	- renseignements techniques sur le produit; - évaluation de la sécurité des caractéristiques de sécurité offertes par le produit; - évaluation de la vulnérabilité; - recommandations. - (TI-ARS)* Rapports d'analyse concernant les répercussions sur la sécurité des TI pour les solutions informatiques. *On peut définir les rapports d'analyse concernant les répercussions sur la sécurité comme des documents contenant tous les éléments suivants : - type de produits livrables de sécurité; - estimation des efforts à fournir; - estimation des coûts. - (TIES-nuage) Une évaluation de la sécurité des TI sur des solutions informatiques configurées à l'aide d'un modèle ***infonuagique***.			
C4.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications valides suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) » ; • « Information Systems Security Architecture Professional (ISSAP) »;	15	Pas de certification = 0 point 1 certification = 5 points 2 certifications = 10 points 3 certifications ou plus = 15 points **Note maximale : 15 points**	

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA CySA+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.			
C4.4	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience des activités de gestion des risques sur des applications infonuagiques pour des projets et des initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves; • infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité infonuagique; • expérience multisensorielle ou mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	10	2 points par projet **Note maximale : 10 points**	

Catégorie de ressource : C.3 Analyste de la C et A et des EMR en sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
Maximum de points possibles				65
Nombre minimal de points requis (65 %)				42
La note de l`entrepreneur				

C.7 Spécialiste en conception de la sécurité – niveau 2

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C5.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C5.2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience pratique (*) au cours des sept (7) dernières années en matière de conception, d'architecture ou d'ingénierie de composants et d'architectures de sécurité informatique, tout en travaillant avec les directives en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI* du CSTC : *Une méthode axée sur le cycle de vie* (ITSG-33). (*) Pour être admissible, au moins un (1) an doit avoir été consacré au traitement de données ayant une classification de sécurité du type Protégé B ou supérieure.	10	De 0 à <1 an = 0 point De 1 à <2 ans = 2 points De 2 à <3 ans = 4 points De 3 à <4 ans = 6 points De 4 à <5 ans = 8 points Plus de 5 ans = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.			
C5.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications valides suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA CySA+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.	10	Pas de certification = 0 point Une certification = 5 points Deux certifications ou plus = 10 points **Note maximale : 10 points**	
C5.4	L'entrepreneur devrait démontrer que la ressource proposée a une expérience pratique de la conception de la sécurité pour les applications infonuagiques pour les projets/initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves;	4	2 points par projet **Note maximale : 4 points**	

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité – niveau 2 Nom de la ressource proposée : _____				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV**
	• infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité infonuagique; • expérience multisensorielle ou mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés; • pipelines analytiques Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.			
Maximum de points possibles				34
Nombre minimal de points requis (65 %)				22
La note de l`entrepreneur				

C.7 Spécialiste en conception de la sécurité – niveau 3

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité – niveau 3 Nom de la ressource proposée : _____				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV**
C6.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C6.2	L'entrepreneur devrait démontrer que la ressource proposée détient : • une maîtrise en sécurité des technologies de l'information, en cybersécurité et renseignement sur les menaces ou dans une discipline similaire, d'une université canadienne reconnue; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C6.3	L'entrepreneur devrait démontrer que la ressource proposée a acquis au cours des sept (7) dernières années une expérience pratique (*) des activités suivantes : • la conception, l'architecture ou l'ingénierie de composants et d'architectures de sécurité informatique pour les ***solutions d'entreprise***; OU • la conception, l'architecture ou l'ingénierie de composants et d'architectures de sécurité informatique liée aux ***technologies émergentes***; tout en travaillant avec les directives en matière de sécurité des technologies de l'information *La gestion des risques liés à la sécurité des TI* du CSTC: *Une méthode axée sur le cycle de vie* (ITSG-33). (*) Pour être admissible, au moins un (1) an doit avoir été consacré au traitement de données ayant une classification de sécurité du type Protégé B ou supérieure. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	10	De 0 à <1 an = 0 point De 1 à <2 ans = 2 points De 2 à <3 ans = 4 points De 3 à <4 ans = 6 points De 4 à <5 ans = 8 points Plus de 5 ans = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C6.4	L'entrepreneur devrait démontrer que la ressource proposée détient au moins deux (2) des certifications suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA CySA+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.	20	Pas de certification = 0 point 2 certifications = 10 points 3 certifications ou plus = 20 points **Note maximale : 20 points**	
C6.5	L'entrepreneur devrait démontrer que la ressource proposée a une expérience pratique de la conception de la sécurité pour les applications infonuagiques pour les projets/initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves; • infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité	10	2 points par projet **Note maximale : 10 points**	

Catégorie de ressource : C.7 Spécialiste en conception de la sécurité – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	infonuagique; • expérience multisensorielle ou mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés; • pipelines analytiques Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.			
Maximum de points possibles				60
Nombre minimal de points requis (65 %)				42
La note de l`entrepreneur				

C.8 Analyste de la sécurité des réseaux – niveau 2

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C7.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux – niveau 2

Nom de la ressource proposée : _____

Nº	Exigence cotée	Nombre maximal de points	Échelle de points	Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV
C7.2	L'entrepreneur devrait démontrer qu'il possède au moins une des certifications suivantes : • une certification actuelle et valide d'administrateur de pare-feu d'un fournisseur de ***pare-feu de prochaine génération*** (p. ex. Cisco, Fortinet, Palo Alto, etc.); • « AWS Certified Advanced Networking Specialty »; • « Microsoft Certified: Azure Administrator Associate » ET l'atelier facultatif « Azure Enterprise-Class Networking » (compte pour une certification); • « MCSE: Cloud Platforms and Infrastructure ».	10	Pas de certification = 0 point 1 certification = 5 points 2 certifications ou plus = 10 points **Note maximale : 10 points**	
C7.3	L'entrepreneur devrait démontrer que la ressource proposée a acquis une expérience de la sécurité des réseaux dans le cadre de projets et d'initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves; • infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité infonuagique; • mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés; • pipelines analytiques Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	12	4 points par projet **Note maximale : 12 points**	

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
Maximum de points possibles				32
Nombre minimal de points requis (65 %)				20
La note de l`entrepreneur				

C.8 Analyste de la sécurité des réseaux – niveau 3

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C8.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C8.2	L'entrepreneur devrait démontrer qu'il possède au moins une des certifications suivantes : • une certification actuelle et valide d'administrateur de pare-feu d'un fournisseur de ***pare-feu de prochaine génération*** (p. ex. Cisco, Fortinet, Palo Alto, etc.); • « AWS Certified Advanced Networking Specialty »; • « Microsoft Certified: Azure Administrator Associate » ET l'atelier facultatif « Azure Enterprise-Class Networking » (compte pour une certification); • « MCSE: Cloud Platforms and Infrastructure ».	10	Pas de certification = 0 point 1 certification = 5 points 2 certifications ou plus = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C8.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins deux (2) des certifications de la liste ci-dessous : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.	10	0 à 1 certification = 0 point 2 certifications ou plus = 10 points **Note maximale : 10 points**	
C8.4	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience de la sécurité des réseaux pour des projets et des initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves; • infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité	10	2 points par projet **Note maximale : 10 points**	

Catégorie de ressource : C.8 Analyste de la sécurité des réseaux – niveau 3 Nom de la ressource proposée : _____				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV**
	infonuagique; • mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés; • pipelines analytiques. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.			
Maximum de points possibles				40
Nombre minimal de points requis (65 %)				26
La note de l`entrepreneur				

C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes – niveau 2

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes – niveau 2 Nom de la ressource proposée : _____				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV**
C9.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C9.2	L'entrepreneur doit indiquer si la ressource proposée est titulaire d'une	5	Pas de certification = 0 point	

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	certification valide d'administrateur de pare-feu d'un fournisseur de ***pare-feu de prochaine génération*** (p. ex. Cisco, Fortinet, Palo Alto, etc.).		1 certification = 5 points **Note maximale : 5 points**	
C9.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins deux certifications de la liste ci-dessous : • « AWS Certified Security Specialty »; • « Microsoft Azure Security Technologies »; • « MCSE: Cloud Platforms and Infrastructure »; • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) » • Bibliothèque de l'infrastructure des technologies de l'information « (ITIL) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA Server+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur; • « Certified Windows Security	10	0 à 1 certification = 0 point 2 certifications ou plus = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	Administrator »; • « Certified UNIX Security Administrator »; • « Certified Detection Analyst »; • « Certified Incident Handler ».			
Maximum de points possibles				25
Nombre minimal de points requis (65 %)				15
La note de l`entrepreneur				

C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes - niveau 3

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C10.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C10.2	L'entrepreneur devrait démontrer si la ressource proposée est titulaire d'une certification actuelle et valide d'administrateur de pare-feu d'un fournisseur de ***pare-feu de prochaine***	5	Pas de certification = 0 point 1 certification = 5 points **Note maximale : 5 points**	

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	génération (p. ex. Cisco, Fortinet, Palo Alto, etc.).			
C10.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins deux certifications de la liste ci-dessous : • « AWS Certified Security Specialty »; • « Microsoft Azure Security Technologies »; • « MCSE: Cloud Platforms and Infrastructure »; • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) » • Bibliothèque de l'infrastructure des technologies de l'information « (ITIL) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA Server+ » ; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) » ; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur; • « Certified Windows Security Administrator »;	15	Pas de certification = 0 point 2 certifications = 10 points 3 certifications ou plus = 15 points **Note maximale : 15 points**	

Catégorie de ressource : C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• « Certified UNIX Security Administrator »; • « Certified Detection Analyst »; • « Certified Incident Handler ».			
Maximum de points possibles				30
Nombre minimal de points requis (65 %)				19
La note de l`entrepreneur				

C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 2

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C11.1	L'entrepreneur devrait démontrer que la ressource proposée possède de l'expérience pratique dans la mise à l'essai d'applications de sécurité Web et / ou mobiles pour l'« ***OWASP Top 10*** Most Critical Application Security Risks » et dans l'offre d'aide aux développeurs pour assurer un niveau élevé de sécurité des applications.	20	0 à <1 an = 0 point De 1 à 3 ans = 10 points 3 ans = 20 points **Note maximale : 20 points**	
C11.2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience pratique de la réalisation d'***analyses de vulnérabilité*** et d'***essais de pénétration*** pour les environnements, les services ou les solutions ***infonuagiques*** publics, qui comprennent toutes les activités suivantes : • réalisation d'***analyses de vulnérabilité*** et d'***essais de pénétration*** approfondis pour cerner les vulnérabilités qui peuvent exposer l'organisation ou les	20	5 points par projet **Note maximale : 20 points**	

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	données à des menaces ou des vols; et • production d'une liste réalisable et prioritaire des lacunes, avec des explications et des recommandations techniques.			
C11.3	L'entrepreneur devrait démontrer que la ressource proposée a acquis au cours des trois dernières années une expérience pratique de la réalisation de projets d'analyse de vulnérabilité technique pour les systèmes de gestion de bases de données (SGBD).	5	5 points par projet **Note maximale : 5 points**	
C11.4	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en informatique ou dans une discipline connexe en technologie de l'information, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
Maximum de points possibles				55
Nombre minimal de points requis (65 %)				35
La note de l`entrepreneur				

C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 3

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C12.1	L'entrepreneur devrait démontrer que la ressource proposée possède de	20	De 0 à <3 ans = 0 point	

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	l'expérience pratique dans la mise à l'essai d'applications de sécurité Web et mobiles pour l'« ***OWASP Top 10*** Most Critical Application Security Risks » et dans l'offre d'aide aux développeurs pour assurer un niveau élevé de sécurité des applications.		De 3 à 5 ans = 10 points Plus de 5 ans = 20 points **Note maximale : 20 points**	
C12.2	L'entrepreneur devrait démontrer que la ressource proposée possède une expérience pratique au cours des trois dernières années, en évaluant la conception de l'architecture ***infonuagique*** en fonction des exigences de sécurité de base du CSTC pour les zones de sécurité de réseau du gouvernement du Canada (ITSG-22) et l'établissement des zones de sécurité du CSTC (ITSG-38).	5	1 projet = 1 point 2 projets = 2 points 3 projets = 3 points 4 projets ou plus = 5 points **Note maximale : 5 points**	
C12.3	L'entrepreneur devrait démontrer que la ressource proposée a une expérience pratique au cours des trois dernières années dans la réalisation de projets d'analyse de vulnérabilité technique pour les systèmes de gestion de bases de données (SGBD).	5	1 projet = 1 point 2 projets = 3 points 3 projets ou plus = 5 points **Note maximale : 5 points**	
C12.4	L'entrepreneur devrait démontrer que la ressource proposée possède au moins deux certifications professionnelles valide de la liste ci-dessous : • « AWS Certified Security Specialty »; • « Microsoft Azure Security Technologies »; • « MCSE: Cloud Platforms and Infrastructure »; • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »;	10	De 0 à 1 certification = 0 point 2 certifications ou plus = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• « System Security Certified Practitioner (SSCP) » d'ISC2; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « CompTIA CySA+ »; • « CompTIA PenTest+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC » toute certification « Cloud Security »; • « GIAC » toute certification « Cyber Defense »; • « GIAC » toute certification « Offensive Operations »; • « GIAC Security Expert (GSE) Certification »; • « Certified Windows Security Administrator »; • « Certified UNIX Security Administrator »; • « Certified Vulnerability Assessor (CVA) »; • « EC Council Certified Ethical Hacker »; • « SANS Mobile Device Security and Ethical Hacking ».			
C12.5	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en informatique ou dans une discipline connexe en technologie de l'information, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.11 Spécialiste des analyses de vulnérabilité de la sécurité des TI – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
Maximum de points possibles				50
Nombre minimal de points requis (65 %)				32
La note de l`entrepreneur				

C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (EM) – niveau 2

Catégorie de ressource : C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (EM) – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C13.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	
C13.2	L'entrepreneur devrait démontrer que la ressource proposée détient : • une maîtrise en sécurité des technologies de l'information, en cybersécurité et renseignement sur les menaces, en génie logiciel ou dans une discipline similaire, d'une université canadienne reconnue; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	5	Aucun diplôme = 0 point Diplôme = 5 points **Note maximale : 5 points**	

Catégorie de ressource : C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (EM) – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C13.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications valides suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) »; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de niveau supérieur.	10	Pas de certification = 0 point 1 certification = 5 points 2 certifications ou plus = 10 points **Note maximale : 10 points**	
C13.4	L'entrepreneur devrait démontrer que la ressource proposée a une expérience pratique de la conception de la sécurité pour les applications infonuagiques pour les projets/initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves; • infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité infonuagique;	15	5 points par projet Maximum de 15 points **Note maximale : 15 points**	

Catégorie de ressource : C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (EM) – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	• expérience multisensorielle ou mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés; • pipelines analytiques. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.			
Maximum de points possibles				40
Nombre minimal de points requis (65 %)				26
La note de l`entrepreneur				

C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (PME) – niveau 3

Catégorie de ressource : C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (PME) – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C14.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme d'études universitaires ou postsecondaires en technologie de l'information, en informatique ou en génie électrique, d'une université ou d'un collège canadien reconnus; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme = 10 points **Note maximale : 10 points**	

Catégorie de ressource : C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (PME) – niveau 3

Nom de la ressource proposée : _____

Nº	Exigence cotée	Nombre maximal de points	Échelle de points	Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV
C14.2	L'entrepreneur devrait démontrer que la ressource proposée détient : • une maîtrise en sécurité des technologies de l'information, en cybersécurité et renseignement sur les menaces, en génie logiciel ou dans une discipline similaire, d'une université canadienne reconnue; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	5	Aucun diplôme = 0 point Diplôme = 5 points **Note maximale : 5 points**	
C14.3	L'entrepreneur devrait démontrer que la ressource proposée détient au moins une (1) des certifications valides suivantes : • « Certified Cloud Security Professional (CCSP) »; • « Certified Information System Security Professional (CISSP) »; • « Certified Information Security Manager (CISM) »; • « Certified Information Systems Auditor (CISA) »; • « Certified in Risk and Information Systems Control (CRISC) »; • « Certified Cyber Forensics Professional (CCFP) »; • « System Security Certified Practitioner (SSCP) » ; • « Information Systems Security Architecture Professional (ISSAP) »; • « CompTIA Security+ »; • « CompTIA Network+ »; • « CompTIA Cloud+ »; • « Certified Wireless Security Professional (CWSP) »; • « GIAC (Global Information Assurance Certification) »; • « SABSA Chartered Security Architect Foundation (SCF) » ou de	15	Pas de certification = 0 point 1 certification = 5 points 2 certifications = 10 points 3 certifications ou plus = 15 points **Note maximale : 15 points**	

Catégorie de ressource : C.14 Spécialiste de la recherche et développement en sécurité des technologies de l'information (PME) – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	niveau supérieur.			
C14.4	L'entrepreneur devrait démontrer que la ressource proposée a une expérience pratique de la conception de la sécurité pour les applications infonuagiques pour les projets/initiatives du gouvernement impliquant l'un des éléments suivants : • identification biométrique; • authentification multifactorielle, traitement sécuritaire des enclaves; • infrastructure-service de ***nuage public;*** • gestion de l'accès de l'identité infonuagique; • expérience multisensorielle ou mobile; • ***intelligence artificielle*** ou ***apprentissage automatique;*** • automatisation de processus robotisés; • pipelines analytiques. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	10	2 points par projet **Note maximale : 10 points**	
Maximum de points possibles				40
Nombre minimal de points requis (65 %)				26
La note de l`entrepreneur				

C.16 Spécialiste de l'évaluation des incidences sur la vie privée – niveau 2

Catégorie de ressource : C.16 Spécialiste de l'évaluation des incidences sur la vie privée – niveau 2 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
C15.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme universitaire dans n'importe quelle discipline, d'une université canadienne reconnue; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme universitaire = 10 points **Note maximale : 10 points**	
C15.2	L'entrepreneur devrait démontrer que l'expérience de la ressource proposée est supérieure (*) au minimum requis au titre du critère O15.1 pour cette catégorie de ressources. (*) Les années d'expérience supplémentaires ne doivent pas avoir été acquises au cours des 10 dernières années. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	10	Expérience totale : De 0 à 4 ans = 0 point De 4 à 5 ans = 3 points De 5 à 6 ans = 6 points De 6 à 7 ans = 8 points Plus de 7 ans = 10 points **Note maximale : 10 points**	
C15.3	L'entrepreneur devrait démontrer que la ressource proposée est titulaire d'une certification de « Holistic Information Security Practitioner (HISP) » ou de « Certified Information Privacy Professional (CIPP) » valide et à jour.	10	Pas de certification = 0 point 1 certification = 10 points **Note maximale : 10 points**	
C15.4	L'entrepreneur devrait démontrer que la ressource proposée a une expérience, acquise au cours des cinq (5) dernières	5	5 points par projet	

Catégorie de ressource : C.16 Spécialiste de l'évaluation des incidences sur la vie privée – niveau 2 Nom de la ressource proposée : _____				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV**
	années précédant la date de délivrance de l'AT, de la détermination des risques pour la vie privée associés à l'utilisation de la biométrie ou d'autres ***technologies émergentes***. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.		**Note maximale : 5 points**	
Maximum de points possibles				35
Nombre minimal de points requis (65 %)				21
La note de l`entrepreneur				

C.16 Spécialiste de l'évaluation des incidences sur la vie privée – niveau 3

Catégorie de ressource : C.16 Spécialiste de l'évaluation des incidences sur la vie privée – niveau 3 Nom de la ressource proposée : _____				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée Renvoi à la proposition / projet no /Resume ou CV**
C16.1	L'entrepreneur devrait démontrer que la ressource proposée satisfait aux critères suivants : • un diplôme universitaire dans n'importe quelle discipline, d'une université canadienne reconnue; OU • une ***évaluation canadienne des diplômes d'études*** équivalents, s'ils sont obtenus à l'extérieur du Canada.	10	Aucun diplôme = 0 point Diplôme universitaire = 10 points **Note maximale : 10 points**	
C16.2	L'entrepreneur devrait démontrer que l'expérience de la ressource proposée est supérieure (*) au minimum requis au titre du critère O1 pour cette catégorie de ressources. (*) Les années d'expérience supplémentaires ne doivent pas avoir été	10	Expérience totale : De 0 à 7 ans = 0 point De 7 à 8 ans = 3 points	

Catégorie de ressource : C.16 Spécialiste de l'évaluation des incidences sur la vie privée – niveau 3 **Nom de la ressource proposée : _____**				
Nº	**Exigence cotée**	**Nombre maximal de points**	**Échelle de points**	**Expérience démontrée** **Renvoi à la proposition / projet no /Resume ou CV**
	acquises au cours des 12 dernières années. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.		De 8 à 9 ans = 6 points De 9 à 10 ans = 8 points Plus de 10 ans = 10 points **Note maximale : 10 points**	
C16.3	L'entrepreneur devrait démontrer que la ressource proposée est titulaire d'une certification de « Holistic Information Security Practitioner (HISP) » ou de « Certified Information Privacy Professional (CIPP) » valide et à jour.	10	Pas de certification = 0 point 1 certification = 10 points **Note maximale : 10 points**	
C16.4	L'entrepreneur devrait démontrer que la ressource proposée est titulaire d'une certification de « Certified Internal Auditor (CIA) » ou de «Certified Information Systems Auditor (CISA) » valide et à jour.	10	Pas de certification = 0 point 1 certification = 5 points 2 certifications = 10 points **Note maximale : 10 points**	
C16.5	L'entrepreneur devrait démontrer que la ressource proposée a de l'expérience, au cours des cinq (5) dernières années, de la détermination des risques pour la vie privée associés à l'utilisation de la biométrie ou d'autres ***technologies émergentes***. Remarque : Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.	5	5 points par projet **Note maximale : 5 points**	
Maximum de points possibles				45
Nombre minimal de points requis (65 %)				27
La note de l`entrepreneur				

APPENDICE D DE L'ANNEXE A
ATTESTATIONS À L'ÉTAPE DE L'AUTORISATION DE TÂCHES

Les attestations ci-après doivent être utilisées, le cas échéant. Si elles s'appliquent, elles doivent être signées et jointes à l'offre de prix de l'entrepreneur au moment de sa soumission au Canada.

1. ATTESTATION D'ÉTUDES ET D'EXPÉRIENCE

L'entrepreneur atteste par la présente que tous les renseignements fournis dans les curriculum vitæ et autres documents soumis pour l'exécution des travaux, plus particulièrement l'information relative aux études, aux réalisations, à l'expérience et aux antécédents professionnels ont été vérifiés par ses soins et qu'ils sont complets et exacts. De plus, l'entrepreneur garantit que chaque personne qu'il propose pour l'exigence est capable d'effectuer les travaux décrits dans l'autorisation de tâches.

_____ _____

Nom en caractères d'imprimerie et signature de la personne autorisée Date

2. ATTESTATION DE LA DISPONIBILITÉ DU PERSONNEL

L'entrepreneur atteste que, s'il est autorisé à fournir des services dans le cadre de cette autorisation de tâches, les personnes proposées dans la proposition de prix pourront commencer les travaux dans un délai raisonnable suivant la date d'émission de l'autorisation de tâches approuvée, ou dans le délai précisé dans le formulaire d'autorisation de tâches, et qu'elles demeureront disponibles pour réaliser les travaux requis.

_____ _____

Nom en caractères d'imprimerie et signature de la personne autorisée Date

3. ATTESTATION DU STATUT DU PERSONNEL

Si l'entrepreneur a proposé une personne qui n'est pas un de ses employés, il atteste qu'il a la permission de la personne d'offrir ses services pour l'exécution des travaux liés à cette autorisation de tâches et de soumettre son curriculum vitæ au Canada. En tout temps pendant la durée du contrat, l'entrepreneur doit, à la demande de l'autorité contractante, fournir une confirmation écrite, signée par la personne concernée, de la permission donnée à l'entrepreneur ainsi que de sa disponibilité. Le non-respect de la demande peut être considéré comme un manquement au contrat en vertu des conditions générales.

_____ _____

Nom en caractères d'imprimerie et signature de la personne autorisée Date

4. ATTESTATION LINGUISTIQUE – [anglais ou bilingue ou français]

L'entrepreneur atteste que chaque ressource proposée en réponse au présent projet d'autorisation de tâches :

[Option 1 – Unilingue anglais] maîtrise l'anglais. Les personnes proposées doivent communiquer en anglais tant à l'oral qu'à l'écrit, sans aide, et en faisant peu d'erreurs.

[Option 2 – Bilingue] maîtrise les deux langues officielles du Canada (français et anglais). Les personnes proposées doivent être en mesure de communiquer en français et en anglais tant à l'oral qu'à l'écrit, sans aide, et en faisant peu d'erreurs.

[Option 3 – Unilingue français] maîtrise le français. Les personnes proposées doivent être en mesure de communiquer en français tant à l'oral qu'à l'écrit, sans aide, et en faisant peu d'erreurs.

_____ _____

Nom en caractères d'imprimerie et signature de la personne autorisée Date

ANNEXE B

BASE DE PAIEMENT

Période de contrat 1

Periode de contrat initiale

Date de l'attribution du contrat pour 1 an (insérer a l`attribution du contrat)

Categorie de Resources	Niveau d'expertise	Taux quotidien ferme
Volet 6 : Services de Cyber Protection de SPICT		
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	2	
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	3	
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	2	
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	3	
C.7 Spécialiste en conception de sécurité des technologies de l'information	2	
C.7 Spécialiste en conception de sécurité des technologies de l'information	3	
C.8 Analyste de la sécurité des réseaux	2	
C.8 Analyste de la sécurité des réseaux	3	
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	2	
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	3	
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2	
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	3	

Categorie de Resources	Niveau d'expertise	Taux quotidien ferme
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2	
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	3	
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2	
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	3	

PÉRIODE OPTIONNELE

Période Option 1

Commence a la fin de la période option 1 pour 1 an
(insérer a l`attribution du contrat)

Categorie de Resources	Niveau d'expertise	Taux quotidien ferme
Volet 6 : Services de Cyber Protection de SPICT		
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	2	
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	3	
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	2	
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	3	
C.7 Spécialiste en conception de sécurité des technologies de l'information	2	
C.7 Spécialiste en conception de sécurité des technologies de l'information	3	
C.8 Analyste de la sécurité des réseaux	2	
C.8 Analyste de la sécurité des réseaux	3	

Categorie de Resources	Niveau d'expertise	Taux quotidien ferme
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	2	
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	3	
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2	
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	3	
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2	
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	3	
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2	
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	3	

Période Option 2

Commence a la fin de la période option 2 pour 1 an
(insérer a l`attribution du contrat)

Categorie de Resources	Niveau d'expertise	Taux quotidien ferme
Volet 6 : Services de Cyber Protection de SPICT		
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	2	
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	3	
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	2	

Categorie de Resources	Niveau d'expertise	Taux quotidien ferme
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	3	
C.7 Spécialiste en conception de sécurité des technologies de l'information	2	
C.7 Spécialiste en conception de sécurité des technologies de l'information	3	
C.8 Analyste de la sécurité des réseaux	2	
C.8 Analyste de la sécurité des réseaux	3	
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	2	
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	3	
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2	
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	3	
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2	
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	3	
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2	
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	3	

ANNEXE C

LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ

Voir le document SRCL/LVERS dans la section Pieces Jointes sur Achatset ventes.gc.ca

ANNEXE C1
GUIDE DE CLASSIFICATION DE SÉCURITÉ

Services avec diverses catégories sera nécessaire.

Catégorie de ressource	Niveau de ressource	Cote de sécurité minimale
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	Niveau 2	Secret
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	Niveau 3	Secret
C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information	Niveau 2	Secret
C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information	Niveau 3	Secret
C.7 Spécialiste en conception de sécurité des technologies de l'information	Niveau 2	Secret
C.7 Spécialiste en conception de sécurité des technologies de l'information	Niveau 3	Secret
C.8 Analyste de la sécurité des réseaux	Niveau 2	Secret
C.8 Analyste de la sécurité des réseaux	Niveau 3	Secret
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	Niveau 2	Secret
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	Niveau 3	Secret
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	Niveau 2	Secret
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	Niveau 3	Secret
C.14 Spécialiste de la R et D en sécurité des technologies de l'information	Niveau 2	Secret
C.14 Spécialiste de la R et D en sécurité des technologies de l'information	Niveau 3	Secret
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	Niveau 2	Secret
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	Niveau 3	Secret

Toutes les ressources affectées à ce contrat sans exception doit être autorisée au minimum au niveau « Secret ».

PIÈCE JOINTE 1.1

Liste des modifications importantes apportées à cette demande de propositions. Le Canada ne sera pas tenu responsable de l'omission par inadvertance de tout changement.

Nº de pièce, article et sous-article de la présente DP	Changements de fond
Exigences de Sécurité	Supprimé LVERS #23 Remplacer par LVERS #19
Annexe A, Énonce des travaux, section 2	L'Agence des services frontaliers du Canada (ASFC) veut retenir les services d'une organisation pour fournir des ressources professionnelles de cybersécurité en GI-TI possédant une expertise particulière dans le domaine de la conformité et de la sécurité du nuage public et des technologies émergentes, conformément à la description détaillée du présent énoncé des travaux.
Annexe A, Énonce des travaux, section 5 (a)	i. Évaluer les équipes des opérations de sécurité; fournir des avis sur la capacité des secteurs responsables de gérer et de remplir leurs responsabilités; élaborer et mettre au point des mesures de gestion précises à l'égard des besoins en matière d'outils, de formation, de personnel, de collaboration et de communication. ii. Rédiger des rapports, par exemple : pour l'analyse de sécurité des données, les concepts d'opération, les énoncés de sensibilité, les évaluations de la menace, les évaluations des facteurs relatifs à la vie privée, les évaluations des vulnérabilités non techniques, les évaluations des risques et la présentation des menaces, vulnérabilités et risques liés à la sécurité des TI. iii. Mener les activités de certification et d'accréditation. iv. Mener des évaluations techniques de la sécurité par rapport aux biens de l'ASFC, y compris les suivants : • charges de travail de niveau Protégé B/Intégrité moyenne/Disponibilité moyenne (PBMM) et non classifiées; • données et environnements de développement et d'essai (masquage, brouillage ou chiffrement de données); • solutions déployées en tant que modèles IaaS, PaaS ou SaaS — à l'intérieur et à l'extérieur du Canada; • adaptation de profils de contrôle de sécurité; • examen et intégration de données probantes sur l'évaluation provenant de sources tierces (CCC, SOC, FedRAMP, ISO, etc.).
Annexe A, Énonce des travaux, section 5 (c)	ii. S'occuper de la surveillance des systèmes de sécurité et de l'intervention en cas d'incident; mener des enquêtes sur des incidents; préparer des séances d'information, des rapports et des plans d'action sur la sécurité. iii. Surveiller la conformité afin d'assurer l'observation et la vigilance continues.
Annexe A, Énonce des travaux, section 5 (d)	d) Fournir des conseils techniques, un soutien, une ingénierie et une recherche dans la conception, le développement et la sécurisation de solutions fondées sur des technologies émergentes ou en évolution (comme des réseaux infonuagiques publics, des applications mobiles, la biométrie, l'automatisation robotisée de processus, les interfaces API, l'intelligence artificielle/l'apprentissage machine et la technologie IRF) :
Annexe A, Énonce des travaux,	iii. examiner et donner des conseils sur la conception, le développement (y compris l'examen des codes), la configuration et les opérations de solutions;

<table>
<tr><th>Nº de pièce, article et sous-article de la présente DP</th><th>Changements de fond</th></tr>
<tr><td>section 5 (d)</td><td>iv. fournir à l'ASFC des analyses instructives, des conseils et du soutien en matière d'ingénierie et de conception sur les moyens réalisables de permettre et de faciliter l'adoption et l'utilisation de technologies novatrices tout en renforçant la posture de sécurité de l'Agence ou en l'aidant à atténuer l'exposition aux menaces inhérentes à ces technologies;
v. tenir l'Agence au courant de l'évolution des risques en matière de sécurité liés à la technologie;
vi. fournir des conseils sur la façon dont l'ASFC peut évaluer et mettre en œuvre des mesures pour s'adapter constamment aux nouvelles technologies et au développement dans le domaine de la cybersécurité.</td></tr>
<tr><td>Annexe A, Énonce des travaux, section 6</td><td>Aux fins de la prise en charge des aspects décrits dans la section 5, le fournisseur doit mettre à la disposition de l'ASFC des ressources professionnels de cybersécurité des TI dans les catégories de SPICT suivantes (mais sans s'y limiter), au besoin, sur présentation d'autorisations de tâche (AT).
<table>
<tr><th>Catégories de ressources</th><th>Niveaux</th></tr>
<tr><td>C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque</td><td>2, 3</td></tr>
<tr><td>C.3. Analyste de la certification et accréditation et des évaluations de la menace et des risques en sécurité des technologies de l'information</td><td>2, 3</td></tr>
<tr><td>C.7 Spécialiste en conception de sécurité des technologies de l'information</td><td>2, 3</td></tr>
<tr><td>C.8 Analyste de la sécurité des réseaux</td><td>2, 3</td></tr>
<tr><td>C.9. Opérateur de systèmes de sécurité des technologies de l'information</td><td>2, 3</td></tr>
<tr><td>C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information</td><td>2, 3</td></tr>
<tr><td>C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information</td><td>2, 3</td></tr>
<tr><td>C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée</td><td>2, 3</td></tr>
</table></td></tr>
<tr><td>Annexe A, Énonce des travaux, section 6</td><td>(Supprimé)
Volet 1: Services à l'entreprise
6.1 Analyste des activités, niveaux 2 et 3 (et activités connexes)
Volet 2:Services de cyberprotection
6.4 C.6 Ingénieur en sécurité des technologies de l'information, niveaux 2 et 3 (et activités connexes)</td></tr>
<tr><td>Annexe A, Énonce des travaux, section 6</td><td>(Les suivants ont été renumérotés)</td></tr>
</table>

Nº de pièce, article et sous-article de la présente DP	Changements de fond
	6.1 C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque, niveaux 2 & 3 6.2 C.3. Analyste de la certification et accréditation et des évaluations de la menace et des risques en sécurité des technologies de l'information, niveaux 2 & 3 6.3 C.7 Spécialiste en conception de sécurité des technologies de l'information, niveaux 2 & 3 6.4 C.8 Analyste de la sécurité des réseaux, niveaux 2 & 3 6.5 C.9. Opérateur de systèmes de sécurité des technologies de l'information, niveaux 2 & 3 6.6 C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveaux 2 & 3 6.7 C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information, niveaux 2 & 3 6.8 C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveaux 2 & 3 6.9 Tâches communes
Annexe A, Énonce des travaux, section 6.8	(Ajouté) h. Effectuer une analyse pour déterminer les risques d'entrave à la vie privée et démontrer la conformité avec les exigences en matière de respect de la confidentialité des données des partenaires internationaux du Canada, le cas échéant.
Annexe A, Énonce des travaux, section 6.9	(Supprimé) • Effectuer des analyses des fonctions opérationnelles et des analyses des répercussions sur les opérations
Annexe A, Énonce des travaux, section 7	(Ajouté) d. un rapport trimestriel d'utilisation des autorisations de tâches. (Ajouté) 21. documentation sur la gestion du changement; 22. documentation sur la gestion des configurations 46. notes de conversation
Annexe A, Énonce des travaux, section 9	Le personnel du fournisseur peut être appelé à travailler sur place dans les locaux de l'ASFC dans la RCN, ou dans les locaux du fournisseur à l'extérieur. Le lieu où les services seront fournis sera indiqué dans chaque autorisation de tâche (AT). Certains services, en particulier le (5) b), pourraient être dispensés en partie à l'extérieur des environnements de l'ASFC grâce à l'équipement du fournisseur et/ou de l'ASFC. Toutefois, à aucun moment des données protégées ne devront être stockées à l'extérieur de l'infrastructure de l'ASFC. Les autres services et tâches se dérouleront dans les environnements de l'ASFC et seront intégrés à ceux-ci grâce à l'équipement de l'ASFC.
Annexe A, Énonce des travaux, section 14	(Ajouté) Tous les travaux doivent être réalisés au Canada et toutes les technologies et l'information de l'ASFC doivent demeurer au Canada.
Annexe A1,	(Definition supprimé)

Nº de pièce, article et sous-article de la présente DP	Changements de fond
Glossaire	Services de sécurité gérés en matière de GI-TI (MSS) / Fournisseur de services de sécurité gérés en matière de GI-TI (MSSP) (Definition ajouté) Évaluation de sécurité Examen d'évaluation et d'autorisation de sécurité (EAS)
Pièce jointe 4.1, Critères techniques obligatoires	(Ajouté) Lorsqu'une copie du contrat ou de la documentation relative aux autorisations de tâches est requise pour vérifier les renseignements fournis par le soumissionnaire afin de démontrer sa conformité à un critère, les documents suivants suffisent : 1. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou 2. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou 3. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.
Pièce jointe 4.1, Critères techniques obligatoires, section 1.0	(Supprimé) EO1
Pièce jointe 4.1, Critères techniques obligatoires, section 1.0	(Renumérotés EO2 à EO1, contenu révisé) **Services facturables ($) par le soumissionnaire (*) pour la prestation de services professionnels de *cybersécurité* en GI-TI dans une infrastructure en nuage public.** Le soumissionnaire doit fournir un maximum de dix (10) contrats de référence d'une valeur cumulative minimale de 10 000 000 $ CA (taxes en sus) pour la prestation de services professionnels de ***cybersécurité*** en GI-TI dans une infrastructure en ***nuage public*** au cours des cinq dernières années à compter de la date de publication de la présente demande de proposition et dans le cadre duquel les tâches liées à **TOUS** les services suivants ont été exécutées individuellement ou collectivement : a) analyses des ***vulnérabilités techniques*** et ***essais de pénétration*** dans des environnements conçus pour répondre à l'un des profils de contrôle de sécurité suivants : a) Protégé B, intégrité moyenne, disponibilité moyenne (PBMM) ou un niveau supérieur,

Nº de pièce, article et sous-article de la présente DP	Changements de fond
	b) FEDRAMP modéré ou élevé, c) ISO 27001 et ISO 27017, d) NIST SP 800-53 modéré ou élevé; b) ***évaluation des risques pour la sécurité des entreprises informatiques***, ***vérifications de sécurité*** ou ***Examen d'évaluation et d'autorisation de sécurité***; c) conseils techniques, soutien, ingénierie et recherche dans le développement de solutions ***sécurisées***; d) opérations touchant la sécurité : surveillance du système de technologie de l'information, gestion des incidents de sécurité, enquêtes et réaction. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EO1**. • Les projets n'ont pas à comprendre tous les services, mais chacun des services doit être justifié. • Chaque projet doit consister en la prestation de services professionnels de ***cybersécurité*** dans une infrastructure en ***nuage public*** et comprendre au moins un service établi. • Le soumissionnaire doit fournir une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis. **(*) Dans l'évaluation de l'expérience de l'entreprise pour ce critere, le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire tel que défini dans :** **Partie 3, Section 3.2** **Section i ; Soumission Technique** **Justification de la conformité technique** **Paragraphe C (page 17)**
Pièce jointe 4.1, Critères techniques obligatoires, section 1.0	(Renumérotés EO3 à EO2, contenu révisé) **Fourniture par le soumissionnaire de services professionnels de *cybersécurité* en GI-TI simultanément** Le soumissionnaire doit s'être vu attribuer, au cours des cinq (5) années précédant la date de publication de la présente DP, un (1) contrat visant à fournir des services professionnels de ***cybersécurité*** en GI-TI pour lesquels : • le soumissionnaire a fourni au moins cinq (5) ressources simultanément dans n'importe laquelle des catégories de ressources, ou catégories de ressources équivalentes (*) sous différents titres, énumérées dans le tableau ci-dessous pendant six (6) mois consécutifs; • chacune des ressources doit avoir offert des services professionnels de ***cybersécurité*** en GI-TI pendant au moins 90 jours facturables au cours d'une période de six (6) mois consécutifs. Catégorie de ressources C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque

Nº de pièce, article et sous-article de la présente DP	Changements de fond

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information
C.7 Spécialiste en conception de sécurité des technologies de l'information
C.8 Analyste de la sécurité des réseaux
C.9 Opérateur de systèmes de sécurité des technologies de l'information
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information
C.14 Spécialiste de la R et D en sécurité des technologies de l'information
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée

(*) Dans le cas où le titre d'une catégorie de ressources mentionné dans le contrat de référence n'est pas identique (**) à celui de la catégorie de ressources indiqué dans le tableau ci-dessus, le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend les tâches connexes (***), à l'exception des tâches communes énumérées à l'annexe A — Énoncé des travaux, pour la catégorie de ressources précisée, comme il est indiqué ci-dessous :

C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque (section 6.1, 5 tâches, y compris les tâches e et h).

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information (section 6.2, 3 tâches, y compris les tâches d et f).

C.7 Spécialiste en conception de la sécurité des technologies de l'information (section 6.3, 6 tâches, y compris les tâches e et i).

C.8 Analyste de la sécurité des réseaux (section 6.4, 5 tâches, y compris les tâches b et f).

C.9 Opérateur de systèmes de sécurité des TI (section 6.5, 3 tâches, y compris les tâches c et d)

C.11 Spécialiste des analyses des vulnérabilités de la sécurité des technologies de l'information (section 6.6, 3 tâches, y compris les tâches a et b).

C.14 Spécialiste de la R et D en sécurité des technologies de l'information (section 6.7, 3 tâches, y compris les tâches a et c).

C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée (section 6.8, 4 tâches, y compris les tâches b et f).

(**) Les titres des catégories de ressources seront aussi considérés comme identiques à ceux indiqués dans le tableau susmentionné si :

- ils contiennent des sigles au lieu de la forme longue des termes utilisés dans les catégories de ressources exigées (p. ex. TI ou GI-TI pour technologie de l'information; AV pour analyse des vulnérabilités; R et D pour recherche et développement; EFVP pour évaluation des facteurs relatifs à la vie privée) et que tout le reste concorde;
- ils contiennent la forme longue des termes au lieu des sigles utilisés dans les catégories de ressources exigées (p. ex. évaluation de la menace et des risques pour EMR; certification et accréditation pour C et A) et que tout le reste concorde;
- ils ne contiennent pas le numéro de catégorie des SPICT (p. ex. C.1), mais le reste du titre est identique ou conforme aux considérations ci-dessus.

(***) Dans le but de démontrer l'équivalence des tâches accomplies par les ressources pour un autre pays, pour lesquelles il est fait référence aux politiques,

Nº de pièce, article et sous-article de la présente DP	Changements de fond
	lignes directrices et autres documents du Canada dans l'énoncé des travaux pour une catégorie de ressources particulière, le soumissionnaire peut citer en lieu et place les politiques, lignes directrices et autres documents applicables du pays concerné. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EO2**. • Les jours facturables doivent être liés à la prestation de services professionnels de ***cybersécurité***. • Le travail facturé pour une catégorie de ressources donnée doit comprendre les tâches associées équivalentes des catégories de ressources décrites ci-dessus. • Le soumissionnaire doit fournir une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis.
Pièce jointe 4.1, Critères techniques obligatoires, section 1.0	(Nouveau EO3) Le soumissionnaire doit démontrer qu'il a établi un des partenariats d'entreprise suivants : • partenaire AWS Consulting; • partenaire Microsoft. Le soumissionnaire doit joindre la documentation appropriée de Microsoft ou d'AWS montrant le niveau de partenariat décrit et sa validité actuelle.
Attachment 4.2 Point-Rated Technical Criteria	(Ajouté) Lorsqu'une copie du contrat ou de la documentation relative aux autorisations de tâches est requise pour vérifier les renseignements fournis par le soumissionnaire afin de démontrer sa conformité à un critère, les documents suivants suffisent : 1. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou 2. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou 3. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.
Pièce jointe 4.2 Critères techniques cotés, section 2.0	(Supprimé) EC1 Renumérotés EC2 à EC4 Renumérotés EC3 à EC5 Renumérotés EC4 à EC6

Nº de pièce, article et sous-article de la présente DP	Changements de fond	
	(Supprimé) EC5 (Ajouté) EC7	
Pièce jointe 4.2 Critères techniques cotés, section 2.0 EC1	Le soumissionnaire obtiendra jusqu'à 20 points pour les contrats supplémentaires répondant à toutes les exigences de l'EO2. Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère et il ne peut s'agir du contrat utilisé pour démontrer la conformité à l'exigence obligatoire EO2. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC1**	Dix (10) points pour chaque contrat admissible. **Note maximale : 20 points**
Pièce jointe 4.2 Critères techniques cotés, section 2.0 EC2	Le soumissionnaire obtiendra jusqu'à 25 points pour les ressources en ***cybersécurité*** simultanées en sus des cinq (5) ressources obligatoires dans le cadre du même contrat et pendant la même période de six mois consécutifs utilisés pour démontrer la conformité au critère obligatoire EO2. Pour obtenir des points, toutes les conditions d'admissibilité indiquées à l'EO2 doivent être respectées par ces ressources additionnelles. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC2**.	Nombre de ressources travaillant simultanément pendant la période de six mois. 5 ressources = 0 point 6 ressources = 5 points 7 ressources = 10 points 8 ressources = 15 points 9 ressources = 20 points 10 ressources = 25 points **Note maximale : 25 points**
Pièce jointe 4.2 Critères techniques cotés, section 2.0 EC3	Le soumissionnaire obtiendra jusqu'à 15 points pour le nombre de catégories de ressources utilisées pour démontrer la conformité au critère obligatoire EO2 et aux exigences cotées EC1 et EC2. Les catégories de ressources doivent provenir de la liste fournie à l'EO2. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC3**	Le nombre de catégories de ressources utilisées pour démontrer la conformité à l'EO2, à l'EC1 et à l'EC2 : 1 catégorie = 2 points 2 catégories = 5 points 3 catégories = 8 points 4 catégories = 11 points 5 catégories = 13 points 6 catégories et + = 15 points **Note maximale : 15 points**

Nº de pièce, article et sous-article de la présente DP	Changements de fond	
Pièce jointe 4.2 Critères techniques cotés, section 2.0 EC4	Le soumissionnaire obtiendra jusqu'à 10 points si le client de l'un des contrats admissibles utilisés pour démontrer la conformité aux exigences organisationnelles obligatoires EO1, EO2 ou à l'EC1 est le gouvernement du Canada(*). (*) Le gouvernement du Canada est défini comme tout ministère, organisme ou société d'État du gouvernement du Canada. Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC4**	Contrat(s) du gouvernement du Canada utilisé(s) pour l'EO1 et l'EO2 ou l'EC1 . 1 ou 2 = 5 points 3 et + = 10 points3 plus = 10 points **Note maximale : 10 points**
Pièce jointe 4.2 Critères techniques cotés, section 2.0 EC5	Le soumissionnaire (*) obtiendra jusqu'à 20 points si l'un des services de ***cybersécurité*** fournis dans le cadre des contrats admissibles utilisés pour démontrer la conformité aux exigences organisationnelles obligatoires EO1, EO2 ou l'EC1 est lié à une ***technologie émergente***(*). Remarque : Pour être admissible, la technologie émergente doit être explicitement identifiée dans l'énoncé des travaux du contrat ou de l'autorisation de tâches. Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC5** **(*) Dans l'évaluation de l'expérience de l'entreprise pour ce critere, le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire tel que défini dans :** **Partie 3, Section 3.2** **Section i ; Soumission Technique** **Justification de la conformité technique** **Paragraphe C (page 17)**	Dix (10) points sont accordés pour chaque contrat utilisé pour démontrer la conformité à l'EO1, l'EO2 ou l'EC1 et lié à une technologie émergente décrite dans les critères. **Note maximale : 20 points**
Pièce jointe 4.2 Critères techniques cotés, section 2.0 EC6	Le soumissionnaire obtiendra des points supplémentaires pour avoir démontré les partenariats actuels et valides ou les certifications suivants : • Partenariat Microsoft « Silver » ou « Gold »; • « AWS Partner Network » « Sélect », « Advanced » ou « Premier ».	Jusqu'à cinq (5) points pour chaque partenariat actuel et valide, comme suit : • partenaire Microsoft « Silver » ou « Gold » (5 points)

Nº de pièce, article et sous-article de la présente DP	Changements de fond	
	Le soumissionnaire doit joindre la documentation appropriée montrant la certification ou le niveau de partenariat décrit et sa validité actuelle	• réseau Partenaires AWS « Sélect », « Advanced » ou « Premier » (5 points) **Note maximale : 10 points**
Pièce jointe 4.2 Critères techniques cotés, section 2.0 EC7	<u>Plan de gestion des talents</u> Le soumissionnaire devrait décrire le plan de gestion des talents qu'il propose de mettre en œuvre dans le contrat subséquent. Ce plan devrait décrire comment le soumissionnaire prévoit : a) composer avec le roulement des ressources et le minimiser; b) maintenir les connaissances et l'expertise liées aux exigences de l'Agence des services frontaliers du Canada pendant toute la durée du contrat subséquent, pendant et entre les autorisations de tâche; c) veiller à ce que les ressources se tiennent à jour des changements technologiques tout au long du contrat; d) veiller à ce qu'il soit en mesure de proposer à l'Agence des services frontaliers du Canada des ressources qualifiées dans les cinq (5) jours suivant la réception d'une demande. La soumission du soumissionnaire devrait être pertinente aux exigences de l'ASFC, et elle ne devrait pas dépasser 2 000 mots.	Cinq (5) points seront attribués pour chacun des éléments donnés ci-dessous : Pas de démonstration = 0 point 1. Les processus qu'utilise le soumissionnaire pour maintenir son inventaire des ressources actives à jour et comment l'addition et la validation de l'expertise des nouvelles ressources sont effectuées; 2. L'identification des personnes devant maintenir les connaissances liées aux exigences de l'ASFC, la fréquence selon laquelle ces connaissances sont maintenues, et le moyen de les communiquer dans l'entreprise; 3. Une explication de la façon dont le soumissionnaire garde le contact avec le client pour connaître son degré de satisfaction au sujet des résultats ou des produits livrables attendus; 4. Une explication de la façon dont le soumissionnaire garde le contact avec les ressources utilisées dans le

Nº de pièce, article et sous-article de la présente DP	Changements de fond	
		cadre du contrat; 5. Les processus qu'utilise le soumissionnaire pour s'assurer de pouvoir proposer rapidement des ressources qualifiées de remplacement qui ont les connaissances et l'expertise spécialisées requises; 6. Une explication de la façon dont le soumissionnaire s'assure que les connaissances et les compétences de ses ressources qui sont liées aux produits livrables du contrat sont tenues à jour pendant toute la durée du contrat. **Note maximale : 30 points**
Pièce jointe 4.2 Critères techniques cotés, section 2.0	Total des points disponibles130 Note minimale requise (~65 %) 85	
Formulaires	Suppressions et ajouts aux formulaires reflétant les modifications apportées aux pièces jointes 4.1 et 4.2	
Appendice C de l'Annexe A section 1.0	(Supprimé) Volet de travail 1 : Services à l'entreprise (Supprimé) B.1 Analyste des activities, niveau 2 (Supprimé) B.1 Analyste des activities, niveau 3 (Supprimé) Volet de travail 2 (titre)	
Appendice C de l'Annexe A section 1.0 O1.2	Remarque : L'expérience requise est un total combiné, cependant un minimum de 1 an doit être démontré pour chaque tâche.	
Appendice C de l'Annexe A section 1.0 O2.2	Remarque : L'expérience requise est un total combiné, cependant un minimum de 1 an doit être démontré pour chaque tâche.	
Appendice C de l'Annexe A section 1.0	Remarque : L'expérience requise est un total combiné, cependant un minimum de six (6) mois doit être démontré pour chaque tâche.	

Nº de pièce, article et sous-article de la présente DP	Changements de fond
O4.1	
Appendice C de l'Annexe A section 1.0	(Supprimé) C.6 Ingénieur en sécurité des technologies de l'information, niveau 2 (O5.1 à O5.4) (Supprimé) C.6 Ingénieur en sécurité des technologies de l'information, niveau 3 (O6.1 à O6.4) Renuméroter les critères restants pour les ressources comme suit : C.7 Spécialiste en conception de sécurité des technologies de l'information, niveau 2 (O5.x) C.7 Spécialiste en conception de sécurité des technologies de l'information, niveau 3 (O6.x) C.8 Analyste de la sécurité des réseaux, niveau 2 (O7.x) C.8 Analyste de la sécurité des réseaux, niveau 3 (O8.x) C.9 Opérateur de systèmes de sécurité des technologies de l'information, niveau 2 (O9.x) C.9 Opérateur de systèmes de sécurité des technologies de l'information, niveau 3 (O10.x) C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 2 (O11.x) C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 3 (O12.x) C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 2 (O13.x) C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 3 (O14.x) C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 2 (O15.x) C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 3 (O16.x)
Appendice C de l'Annexe A section 1.0 O5.1	(*) L'expérience requise est un total combiné, cependant un minimum de 1 an est exigé en développement de logiciels et sécurité des applications
Appendice C de l'Annexe A section 1.0 O6.1	(*) L'expérience requise est un total combiné, cependant un minimum de deux (2) années d'expérience sont exigées en développement de logiciels et sécurité des applications.
Appendice C de l'Annexe A section 1.0 O7.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des huit (8) dernières années, dix-huit mois (18) mois d'expérience du déploiement et du soutien de la sécurité de réseaux sur une infrastructure de nuage public externalisé. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.

Nº de pièce, article et sous-article de la présente DP	Changements de fond
Appendice C de l'Annexe A section 1.0 O8.1	L'entrepreneur doit démontrer que la ressource proposée a acquis sept (7) années d'expérience pratique au cours desquelles il a effectué toutes les activités suivantes : • ***configuration***[2] et soutien de logiciels de gestion automatisée de la sécurité informatique; • ***configuration***[2] et soutien en matière de pare-feu, de routeurs et d'équilibreurs de charge; • conception et soutien en matière de basculement et de reprise de réseaux à l'aide d'une infrastructure sous forme de code : • ***configuration***[2] et soutien en matière d'informatique élastique. • ***configuration***[2] et soutien de groupes de sécurité et de listes de contrôle d'accès. • conception de routes définies par l'utilisateur pour forcer une tunnelisation. • ***configuration***[2] et intégration d'infrastructures de réseaux à l'aide d'une ***configuration***[1] de nuage hybride Remarque : Les projets ne nécessitent pas toutes les activités, cependant une expérience dans l'exécution de **toutes** les activités doit être démontrée. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois.
Appendice C de l'Annexe A section 1.0 O8.3	L'entrepreneur doit démontrer que la ressource proposée a acquis, au cours des huit (8) dernières années, trois (3) années d'expérience du déploiement et du soutien de la sécurité de réseaux sur une infrastructure de fournisseurs de services de ***nuages publics*** externalisés. Pour être admissible, un projet doit avoir une durée minimale de quatre (4) mois
Appendice C de l'Annexe A section 1.0 O9.1	(*) L'expérience requise est un total combiné, cependant un minimum de dix-huit (18) mois est obligatoire pour chacune des activités.
Appendice C de l'Annexe A section 1.0 O10.1	(*) L'expérience requise est un total combiné, cependant un minimum de trois (3) années est obligatoire pour chacune des activités.
Appendice C de l'Annexe A section 1.0 M13.1	(*)The experience required is a combined total, however a minimum of eighteen (18) months is required with Software Development & Application Security.
Appendice C de l'Annexe A section 1.0 O13.1	(*) L'expérience requise est un total combiné, cependant un minimum de dix-huit (18) mois d'expérience sont exigées en développement de logiciels et sécurité des applications.

Nº de pièce, article et sous-article de la présente DP	Changements de fond
Appendice C de l'Annexe A section 1.0 O14.1	(*) L'expérience requise est un total combiné, cependant un minimum de trois (3) années d'expérience sont exigées en développement de logiciels et sécurité des applications
Appendice C de l'Annexe A section 2.0	(Supprimé) Volet de travail 1 : Services à l'entreprise (Supprimé) B.1 Analyste des activities, niveau 2 (Supprimé) B.1 Analyste des activities, niveau 3 (Supprimé) Volet de travail 2 (titre)
Appendice C de l'Annexe A section 2.0	(Supprimé) C.6 Ingénieur en sécurité des technologies de l'information, niveau 2 (C5.1 à C5.4) (Supprimé) C.6 Ingénieur en sécurité des technologies de l'information, niveau 3 (C6.1 à C6.4) Renuméroter les critères restants pour les ressources comme suit : C.7 Spécialiste en conception de sécurité des technologies de l'information, niveau 2 (C5.x) C.7 Spécialiste en conception de sécurité des technologies de l'information, niveau 3 (C6.x) C.8 Analyste de la sécurité des réseaux, niveau 2 (C7.x) C.8 Analyste de la sécurité des réseaux, niveau 3 (C8.x) C.9 Opérateur de systèmes de sécurité des technologies de l'information, niveau 2 (C9.x) C.9 Opérateur de systèmes de sécurité des technologies de l'information, niveau 3 (C10.x) C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 2 (C11.x) C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information, niveau 3 (C12.x) C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 2 (C13.x) C.14 Spécialiste de la R et D en sécurité des technologies de l'information, niveau 3 (C14.x) C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 2 (C15.x) C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée, niveau 3 (C16.x)

PIÈCE JOINTE 3.1

FORMULAIRE DE PRÉSENTATION DE LA SOUMISSION

FORMULAIRE DE PRÉSENTATION DE LA SOUMISSION		
Dénomination sociale du soumissionnaire		
Représentant autorisé du soumissionnaire aux fins d'évaluation (p. ex. pour obtenir des précisions)	Nom	
	Titre	
	Adresse	
	Numéro de téléphone	
	Numéro de télécopieur	
	Adresse électronique	
Agent de sécurité d'entreprise	Nom	
	Titre	
	Adresse	
	Numéro de téléphone	
	Numéro de télécopieur	
	Adresse électronique	
Numéro d'entreprise-approvisionnement (NEA) du soumissionnaire [voir les instructions et conditions uniformisées 2003] **[Remarque à l'intention des soumissionnaires : Le NEA donné doit correspondre à la dénomination sociale utilisée dans la soumission. Si ce n'est pas le cas, le soumissionnaire sera déterminé en fonction de la dénomination sociale fournie plutôt qu'en fonction du NEA, et le soumissionnaire devra fournir le NEA qui correspond à la dénomination sociale du soumissionnaire.]**		
Compétence du contrat : Province ou territoire du Canada choisi par le soumissionnaire et qui aura les compétences sur tout contrat subséquent (si différent de celui précisé dans la demande)		

Sites ou locaux proposés par le soumissionnaire nécessitant des mesures de protection Consulter les directives à la Partie 3.	Adresse du site ou des locaux proposés : _____ Ville : _____ Province : _____ Code postal : _____ Pays : _____
Anciens fonctionnaires Pour obtenir une définition d'« ancien fonctionnaire », voir la clause intitulée « Ancien fonctionnaire », dans la Partie 2 de la demande de soumissions.	Le soumissionnaire est-il un ancien fonctionnaire touchant une pension tel qu'il est défini dans la demande de soumissions? Oui ____ Non ____ Si oui, fournir les renseignements demandés à l'article intitulé « Ancien fonctionnaire » dans la Partie 2.
	Le soumissionnaire est-il un ancien fonctionnaire qui a reçu un paiement forfaitaire en vertu des dispositions d'un programme de réduction des effectifs? Oui ____ Non ____ Si oui, fournir les renseignements demandés à l'article intitulé « Ancien fonctionnaire » dans la Partie 2.
Niveau d'attestation de sécurité du soumissionnaire [Indiquer le niveau et la date d'attribution] **[Remarque à l'intention des soumissionnaires : Le nom dans l'attestation de sécurité doit correspondre à la dénomination sociale du soumissionnaire. Si ce n'est pas le cas, l'attestation n'est pas valide pour le soumissionnaire.]**	
En apposant ma signature ci-après, j'atteste, au nom du soumissionnaire, que j'ai lu la demande de soumissions en entier, y compris les documents incorporés par renvoi dans la demande et que : 1. le soumissionnaire considère que lui-même et les ressources qu'il propose peuvent répondre aux exigences obligatoires décrites dans la demande de soumissions; 2. la soumission est valide pour la période indiquée dans la demande de soumissions; 3. tous les renseignements fournis dans cette soumission sont complets et exacts; 4. si un contrat est attribué au soumissionnaire, ce dernier acceptera toutes les modalités déterminées dans les clauses du contrat subséquent comprises dans la demande de soumissions.	
Signature du représentant autorisé du soumissionnaire	

PIÈCE JOINTE 3.2

INSTRUMENTS DE PAIEMENT ÉLECTRONIQUE

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$)

PIÈCE JOINTE 4.1

CRITÈRES TECHNIQUES OBLIGATOIRES

REMARQUE À L'INTENTION DES SOUMISSIONNAIRES : Les termes qui apparaissent en ***caractères gras et en italiques*** sont définis dans le glossaire

Lorsqu'une copie du contrat ou de la documentation relative aux autorisations de tâches est requise pour vérifier les renseignements fournis par le soumissionnaire afin de démontrer sa conformité à un critère, les documents suivants suffisent :

4. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou
5. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou
6. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.

1.0 EXIGENCES ORGANISATIONNELLES OBLIGATOIRES

Critères	Exigences obligatoires	Réponse du soumissionnaire
EO1 (PC)	**Services facturables ($) par le soumissionnaire (*) pour la prestation de services professionnels de *cybersécurité* en GI-TI dans une infrastructure en nuage public.** Le soumissionnaire **(*)** doit fournir un maximum de dix (10) contrats de référence d'une valeur cumulative minimale de 10 000 000 $ CA (taxes en sus) pour la prestation de services professionnels de ***cybersécurité*** en GI-TI dans une infrastructure en ***nuage public*** au cours des cinq dernières années à compter de la date de publication de la présente demande de proposition et dans le cadre duquel les tâches liées à **TOUS** les services suivants ont été exécutées individuellement ou collectivement : a) analyses des ***vulnérabilités techniques*** et ***essais de pénétration*** dans des environnements conçus pour répondre à l'un des profils de contrôle de sécurité suivants : a. Protégé B, intégrité moyenne, disponibilité moyenne (PBMM) ou un niveau supérieur, b. FEDRAMP modéré ou élevé, c. ISO 27001 et ISO 27017, d. NIST SP 800-53 modéré ou élevé; b) ***évaluation des risques pour la sécurité des entreprises informatiques***, ***vérifications de sécurité*** ou ***Examen d'évaluation et d'autorisation de sécurité***; c) conseils techniques, soutien, ingénierie et recherche dans le développement de solutions ***sécurisées***; d) opérations touchant la sécurité : surveillance du système de technologie de l'information, gestion des incidents de sécurité, enquêtes et réaction.	

<table>
<tr><th>Critères</th><th>Exigences obligatoires</th><th>Réponse du soumissionnaire</th></tr>
<tr><td></td><td>Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le Formulaire EO1.

• Les projets n'ont pas à comprendre tous les services, mais chacun des services doit être justifié.
• Chaque projet doit consister en la prestation de services professionnels de cybersécurité dans une infrastructure en nuage public et comprendre au moins un service établi.
• Le soumissionnaire doit fournir une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis.

(*) Dans l'évaluation de l'expérience de l'entreprise pour ce critere, le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire tel que défini dans :

Partie 3, Section 3.2
Section i ; Soumission Technique
Justification de la conformité technique
Paragraphe C (page 17)</td><td></td></tr>
<tr><td>EO2</td><td>Fourniture par le soumissionnaire de services professionnels de cybersécurité en GI-TI simultanément

Le soumissionnaire doit s'être vu attribuer, au cours des cinq (5) années précédant la date de publication de la présente DP, un (1) contrat visant à fournir des services professionnels de cybersécurité en GI-TI pour lesquels :

• le soumissionnaire a fourni au moins cinq (5) ressources simultanément dans n'importe laquelle des catégories de ressources, ou catégories de ressources équivalentes (*) sous différents titres, énumérées dans le tableau ci-dessous pendant six (6) mois consécutifs;
• chacune des ressources doit avoir offert des services professionnels de cybersécurité en GI-TI pendant au moins 90 jours facturables au cours d'une période de six (6) mois consécutifs.

<table>
<tr><th>Catégorie de ressources</th></tr>
<tr><td>C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque</td></tr>
<tr><td>C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information</td></tr>
<tr><td>C.7 Spécialiste en conception de sécurité des technologies de l'information</td></tr>
<tr><td>C.8 Analyste de la sécurité des réseaux</td></tr>
<tr><td>C.9 Opérateur de systèmes de sécurité des technologies de l'information</td></tr>
<tr><td>C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information</td></tr>
<tr><td>C.14 Spécialiste de la R et D en sécurité des technologies de l'information</td></tr>
<tr><td>C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée</td></tr>
</table>

(*) Dans le cas où le titre d'une catégorie de ressources mentionné</td><td></td></tr>
</table>

Critères	Exigences obligatoires	Réponse du soumissionnaire
	dans le contrat de référence n'est pas identique (**) à celui de la catégorie de ressources indiqué dans le tableau ci-dessus, le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend les tâches connexes (***), à l'exception des tâches communes énumérées à l'annexe A - Énoncé des travaux, pour la catégorie de ressources précisée, comme il est indiqué ci-dessous : C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque (section 6.1, 5 tâches, y compris les tâches e et h). C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information (section 6.2, 3 tâches, y compris les tâches d et f). C.7 Spécialiste en conception de la sécurité des technologies de l'information (section 6.3, 6 tâches, y compris les tâches e et i). C.8 Analyste de la sécurité des réseaux (section 6.4, 5 tâches, y compris les tâches b et f). C.9 Opérateur de systèmes de sécurité des TI (section 6.5, 3 tâches, y compris les tâches c et d) C.11 Spécialiste des analyses des vulnérabilités de la sécurité des technologies de l'information (section 6.6, 3 tâches, y compris les tâches a et b). C.14 Spécialiste de la R et D en sécurité des technologies de l'information (section 6.7, 3 tâches, y compris les tâches a et c). C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée (section 6.8, 4 tâches, y compris les tâches b et f). (**) Les titres des catégories de ressources seront aussi considérés comme identiques à ceux indiqués dans le tableau susmentionné si : • ils contiennent des sigles au lieu de la forme longue des termes utilisés dans les catégories de ressources exigées (p. ex. TI ou GI-TI pour technologie de l'information; AV pour analyse des vulnérabilités; R et D pour recherche et développement; EFVP pour évaluation des facteurs relatifs à la vie privée) et que tout le reste concorde; • ils contiennent la forme longue des termes au lieu des sigles utilisés dans les catégories de ressources exigées (p. ex. évaluation de la menace et des risques pour EMR; certification et accréditation pour C et A) et que tout le reste concorde; • ils ne contiennent pas le numéro de catégorie des SPICT (p. ex. C.1), mais le reste du titre est identique ou conforme aux considérations ci-dessus. (***) Dans le but de démontrer l'équivalence des tâches accomplies par les ressources pour un autre pays, pour lesquelles il est fait référence aux politiques, lignes directrices et autres documents du Canada dans l'énoncé des travaux pour une catégorie de ressources particulière, le soumissionnaire peut citer en lieu et place les politiques, lignes directrices et autres documents applicables du pays concerné.	

Critères	Exigences obligatoires	Réponse du soumissionnaire
	Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EO2**. • Les jours facturables doivent être liés à la prestation de services professionnels de ***cybersécurité***. • Le travail facturé pour une catégorie de ressources donnée doit comprendre les tâches associées équivalentes des catégories de ressources décrites ci-dessus. • Le soumissionnaire doit fournir une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis.	
EO3	Le soumissionnaire doit démontrer qu'il a établi un des partenariats d'entreprise suivants : • partenaire AWS Consulting; • partenaire Microsoft. Le soumissionnaire doit joindre la documentation appropriée de Microsoft ou d'AWS montrant le niveau de partenariat décrit et sa validité actuelle.	

PIÈCE JOINTE 4.2

CRITÈRES TECHNIQUES COTÉS

REMARQUE À L'INTENTION DES SOUMISSIONNAIRES : Les termes qui apparaissent en ***caractères gras et en italiques*** sont définis dans le glossaire.

Lorsqu'une copie du contrat ou de la documentation relative aux autorisations de tâches est requise pour vérifier les renseignements fournis par le soumissionnaire afin de démontrer sa conformité à un critère, les documents suivants suffisent :

1. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou
2. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou
3. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.

2.0 EXIGENCES ORGANISATIONNELLES COTÉES

EC	Critères techniques cotés	Attribution des points	Réponse du soumissionnaire
EC1	Le soumissionnaire obtiendra jusqu'à 20 points pour les contrats supplémentaires répondant à toutes les exigences de l'EO2. Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère et il ne peut s'agir du contrat utilisé pour démontrer la conformité à l'exigence obligatoire EO2. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC1**.	Dix (10) points pour chaque contrat admissible. **Note maximale : 20 points**	
EC2	Le soumissionnaire obtiendra jusqu'à 25 points pour les ressources en ***cybersécurité*** simultanées en sus des cinq (5) ressources obligatoires dans le cadre du même contrat et pendant la même période de six mois consécutifs utilisés pour démontrer la conformité au critère obligatoire EO2. Pour obtenir des points, toutes les conditions d'admissibilité indiquées à l'EO2 doivent être respectées par ces ressources additionnelles.	Nombre de ressources travaillant simultanément pendant la période de six mois. 5 ressources = 0 point 6 ressources = 5 points 7 ressources = 10 points 8 ressources = 15 points 9 ressources = 20 points 10 ressources = 25 points	

	Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC2**.	**Note maximale : 25 points**	
EC3	Le soumissionnaire obtiendra jusqu'à 15 points pour le nombre de catégories de ressources utilisées pour démontrer la conformité au critère obligatoire EO2 et aux exigences cotées EC1 et EC2. Les catégories de ressources doivent provenir de la liste fournie à l'EO2. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC3**.	Le nombre de catégories de ressources utilisées pour démontrer la conformité à l'EO2, à l'EC1 et à l'EC2 : 1 catégorie = 2 points 2 catégories = 5 points 3 catégories = 8 points 4 catégories = 11 points 5 catégories = 13 points 6 catégories et + = 15 points **Note maximale : 15 points**	
EC4	Le soumissionnaire obtiendra jusqu'à 10 points si le client de l'un des contrats admissibles utilisés pour démontrer la conformité aux exigences organisationnelles obligatoires EO1, EO2 ou à l'EC1 est le gouvernement du Canada(*). (*) Le gouvernement du Canada est défini comme tout ministère, organisme ou société d'État du gouvernement du Canada. Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère. Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC4**.	Contrat(s) du gouvernement du Canada utilisé(s) pour l'EO1 et l'EO2 ou l'EC1. 1 ou 2 = 5 points 3 et + = 10 points **Note maximale : 10 points**	
EC5	Le soumissionnaire (*) obtiendra jusqu'à 20 points si l'un des services de ***cybersécurité*** fournis dans le cadre des contrats admissibles utilisés pour démontrer la conformité aux exigences organisationnelles obligatoires EO1, EO2 ou l'EC1 est lié à une ***technologie émergente***(*). Remarque : Pour être admissible, la technologie émergente doit être explicitement identifiée dans l'énoncé des travaux du contrat ou de l'autorisation de tâches. Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère.	Dix (10) points sont accordés pour chaque contrat utilisé pour démontrer la conformité à l'EO1, l'EO2 ou l'EC1 et lié à une technologie émergente décrite dans les critères. **Note maximale : 20 points**	

	Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC5**. **(*) Dans l'évaluation de l'expérience de l'entreprise pour ce critere, le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire tel que défini dans :** **Partie 3, Section 3.2** **Section i ; Soumission Technique** **Justification de la conformité technique** **Paragraphe C (page 17)**		
EC6	Le soumissionnaire obtiendra des points supplémentaires pour avoir démontré les partenariats actuels et valides ou les certifications suivants : • Partenariat Microsoft « Silver » ou « Gold »; • « AWS Partner Network » « Sélect », « Advanced » ou « Premier ». Le soumissionnaire doit joindre la documentation appropriée montrant la certification ou le niveau de partenariat décrit et sa validité actuelle.	Jusqu'à cinq (5) points pour chaque partenariat actuel et valide, comme suit : • partenaire Microsoft « Silver » ou « Gold » (5 points) • réseau Partenaires AWS « Sélect », « Advanced » ou « Premier » (5 points) **Note maximale : 10 points**	
EC7	<u>Plan de gestion des talents</u> Le soumissionnaire devrait décrire le plan de gestion des talents qu'il propose de mettre en œuvre dans le contrat subséquent. Ce plan devrait décrire comment le soumissionnaire prévoit : a) composer avec le roulement des ressources et le minimiser; b) maintenir les connaissances et l'expertise liées aux exigences de l'Agence des services frontaliers du Canada pendant toute la durée du contrat subséquent, pendant et entre les autorisations de tâche; c) veiller à ce que les ressources se tiennent à jour des changements technologiques tout au long du contrat; d) veiller à ce qu'il soit en mesure de proposer à l'Agence des services frontaliers du Canada des ressources qualifiées dans les cinq (5) jours suivant la réception d'une demande.	Cinq (5) points seront attribués pour chacun des éléments donnés ci-dessous : Pas de démonstration = 0 point 7. Les processus qu'utilise le soumissionnaire pour maintenir son inventaire des ressources actives à jour et comment l'addition et la validation de l'expertise des nouvelles ressources sont effectuées; 8. L'identification des personnes devant maintenir les connaissances liées aux exigences de l'ASFC, la fréquence selon laquelle ces connaissances sont maintenues, et le moyen de les communiquer dans	

	La soumission du soumissionnaire devrait être pertinente aux exigences de l'ASFC, et elle ne devrait pas dépasser 2 000 mots.	l'entreprise; 9. Une explication de la façon dont le soumissionnaire garde le contact avec le client pour connaître son degré de satisfaction au sujet des résultats ou des produits livrables attendus; 10. ne explication de la façon dont le soumissionnaire garde le contact avec les ressources utilisées dans le cadre du contrat; 11. es processus qu'utilise le soumissionnaire pour s'assurer de pouvoir proposer rapidement des ressources qualifiées de remplacement qui ont les connaissances et l'expertise spécialisées requises; 12. ne explication de la façon dont le soumissionnaire s'assure que les connaissances et les compétences de ses ressources qui sont liées aux produits livrables du contrat sont tenues à jour pendant toute la durée du contrat. **Note maximale : 30 points**	
Total des points disponibles			**130**
Note minimale requise (~65 %)			**85**
Note du soumissionnaire			

PIÈCE JOINTE 4.3

FORMULAIRES DE RÉPONSE DU SOUMISSIONNAIRE AUX EXIGENCES ORGANISATIONNELLES

EXIGENCE ORGANISATIONNELLE OBLIGATOIRE EO1

Services facturables ($) par le soumissionnaire (*) pour la prestation de services professionnels de *cybersécurité* en GI-TI dans une infrastructure en nuage public.

Le soumissionnaire (*) doit fournir un maximum de dix (10) contrats de référence d'une valeur cumulative minimale de 10 000 000 $ CA (taxes en sus) pour la prestation de services professionnels de ***cybersécurité*** en GI-TI dans une infrastructure en ***nuage public*** au cours des cinq dernières années à compter de la date de publication de la présente demande de proposition et dans le cadre duquel les tâches liées à **TOUS** les services suivants ont été exécutées individuellement ou collectivement :

a) analyses des ***vulnérabilités techniques*** et ***essais de pénétration*** dans des environnements conçus pour répondre à l'un des profils de contrôle de sécurité suivants :
   a. Protégé B, intégrité moyenne, disponibilité moyenne (PBMM) ou un niveau supérieur,
   b. FEDRAMP modéré ou élevé,
   c. ISO 27001 et ISO 27017,
   d. NIST SP 800-53 modéré ou élevé;
b) ***évaluation des risques pour la sécurité des entreprises informatiques***, ***vérifications de sécurité*** ou ***Examen d'évaluation et d'autorisation de sécurité***;
c) conseils techniques, soutien, ingénierie et recherche dans le développement de solutions ***sécurisées***;
d) opérations touchant la sécurité : surveillance du système de technologie de l'information, gestion des incidents de sécurité, enquêtes et réaction.

- Les projets n'ont pas à comprendre tous les services, mais chacun des services doit être justifié.
- Chaque projet doit consister en la prestation de services professionnels de ***cybersécurité*** dans une infrastructure en ***nuage public*** et comprendre au moins un service établi.
- Le soumissionnaire doit fournir une copie du contrat ou de l'autorisation de tâches pour justifier les détails fourni

(*) Dans l'évaluation de l'expérience de l'entreprise pour ce critere, le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire tel que défini dans :

Partie 3, Section 3.2
Section i : Soumission Technique
Justification de la conformité technique
Paragraphe C (page 17)

Copier et remplir pour chaque contrat de référence

FORMULAIRE EO1
A) Nº de référence du contrat ou de l'autorisation de tâches (AT) : _____

B) Renseignements sur le client (*) (*) La personne-ressource doit être une personne qui est ou était au moment du projet un employé de l'organisation cliente et qui peut confirmer tous les renseignements.	
Nom de l'organisation	
Nom et titre de la personne-ressource	
Adresse	
Téléphone	
Adresse électronique	

C) Valeur facturée du contrat ou de l'autorisation de tâches (*) (*) Valeur facturée, taxes en sus, pour les services professionnels ***de cybersécurité*** dans une infrastructure en ***nuage public*** et pour au moins un sous-critère établi.	
Valeur facturée du contrat ou de l'AT	

D) Description du projet	
Nom du projet	
Description du projet : tel que définie dans l'énoncé des travaux du contrat ou de l'autorisation de tâches	
Dates de début et de fin du projet Si le projet est en cours, indiquer la date de clôture de la présente demande de proposition.	
Portée des services de cybersécurité fournis : Description du travail entrepris et des services fournis, y compris la façon dont le travail répond aux critères.	
Lesquels des services suivants sont démontrés par ce projet: Infrastructure en ***nuage public*** et : a) analyses des ***vulnérabilités techniques*** et ***essais de pénétration*** dans des environnements conçus pour répondre à l'un des profils de contrôle de sécurité suivants : a. Protégé B, intégrité moyenne, disponibilité moyenne (PBMM) ou un niveau supérieur, b. FEDRAMP modéré ou élevé, c. ISO 27001 et ISO 27017, d. NIST SP 800-53 modéré ou élevé; b) ***évaluation des risques pour la sécurité des entreprises informatiques***,	

vérifications de sécurité ou ***Examen d'évaluation et d'autorisation de sécurité***; c) conseils techniques, soutien, ingénierie et recherche dans le développement de solutions ***sécurisées***; d) opérations touchant la sécurité : surveillance du système de technologie de l'information, gestion des incidents de sécurité, enquêtes et réaction.	

Documentation à l'appui
S'assurer d'inclure une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis. Ce qui suit est suffisant : 1. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou 2. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou 3. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.

EXIGENCE ORGANISATIONNELLE OBLIGATOIRE EO2

Fourniture par le soumissionnaire de services professionnels de *cybersécurité* en GI-TI simultanément

Le soumissionnaire doit s'être vu attribuer, au cours des cinq (5) années précédant la date de publication de la présente DP, un (1) contrat visant à fournir des services professionnels de ***cybersécurité*** en GI-TI pour lesquels :

- le soumissionnaire a fourni au moins cinq (5) ressources simultanément dans n'importe laquelle des catégories de ressources, ou catégories de ressources équivalentes (*) sous différents titres, énumérées dans le tableau ci-dessous pendant six (6) mois consécutifs;
- chacune des ressources doit avoir offert des services professionnels de ***cybersécurité*** en GI-TI pendant au moins 90 jours facturables au cours d'une période de six (6) mois consécutifs.

Catégorie de ressources
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque
C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information
C.7 Spécialiste en conception de sécurité des technologies de l'information
C.8 Analyste de la sécurité des réseaux
C.9 Opérateur de systèmes de sécurité des technologies de l'information
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information
C.14 Spécialiste de la R et D en sécurité des technologies de l'information
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée

(*) Dans le cas où le titre d'une catégorie de ressources mentionné dans le contrat de référence n'est pas identique (**) à celui de la catégorie de ressources indiqué dans le tableau ci-dessus, le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend les tâches connexes (***), à l'exception des tâches communes énumérées à l'annexe A- Énoncé des travaux, pour la catégorie de ressources précisée, comme il est indiqué ci-dessous :

C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque (section 6.1, 5 tâches, y compris les tâches e et h).

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information (section 6.2, 3 tâches, y compris les tâches d et f).

C.7 Spécialiste en conception de la sécurité des technologies de l'information (section 6.3, 6 tâches, y compris les tâches e et i).

C.8 Analyste de la sécurité des réseaux (section 6.4, 5 tâches, y compris les tâches b et f).

C.9 Opérateur de systèmes de sécurité des TI (section 6.5, 3 tâches, y compris les tâches c et d)

C.11 Spécialiste des analyses des vulnérabilités de la sécurité des technologies de l'information (section 6.6, 3 tâches, y compris les tâches a et b).

C.14 Spécialiste de la R et D en sécurité des technologies de l'information (section 6.7, 3 tâches, y compris les tâches a et c).

C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée (section 6.8, 4 tâches, y compris les tâches b et f).

(**) Les titres des catégories de ressources seront aussi considérés comme identiques à ceux indiqués dans le tableau susmentionné si :

- ils contiennent des sigles au lieu de la forme longue des termes utilisés dans les catégories de ressources exigées (p. ex. TI ou GI-TI pour technologie de l'information; AV pour analyse des vulnérabilités; R et D pour recherche et développement; EFVP pour évaluation des facteurs relatifs à la vie privée) et que tout le reste concorde;
- ils contiennent la forme longue des termes au lieu des sigles utilisés dans les catégories de ressources exigées (p. ex. évaluation de la menace et des risques pour EMR; certification et accréditation pour C et A) et que tout le reste concorde;

- ils ne contiennent pas le numéro de catégorie des SPICT (p. ex. C.1), mais le reste du titre est identique ou conforme aux considérations ci-dessus.

(***) Dans le but de démontrer l'équivalence des tâches accomplies par les ressources pour un autre pays, pour lesquelles il est fait référence aux politiques, lignes directrices et autres documents du Canada dans l'énoncé des travaux pour une catégorie de ressources particulière, le soumissionnaire peut citer en lieu et place les politiques, lignes directrices et autres documents applicables du pays concerné.

- Les jours facturables doivent être liés à la prestation de services professionnels de ***cybersécurité***.
- Le travail facturé pour une catégorie de ressources donnée doit comprendre les tâches associées équivalentes des catégories de ressources décrites ci-dessus.
- Le soumissionnaire doit fournir une copie du contrat ou de l'autorisation de tâches pour justifier les détails fourni

FORMULAIRE EO2 (3 Parties)

PARTIE 1
A) Nº de référence du contrat ou de l'autorisation de tâches : _____

B) Renseignements sur le client (*) (*) La personne-ressource doit être une personne qui est ou était au moment du projet un employé de l'organisation cliente et qui peut confirmer tous les renseignements.	
Nom de l'organisation	
Nom et titre de la personne-ressource	
Adresse	
Téléphone	
Adresse électronique	

C) Renseignements sur le contrat	
Date de début	
Date de fin	

D) S'agit-il ou s'agissait-il d'un contrat des Services professionnels en informatique centrés sur les tâches (SPICT)? Oui ____ Non ____

E) Description du projet	
Nom du projet	
Description du projet : tel que définie dans l'énoncé des travaux du contrat ou de l'autorisation de tâches	

Dates de début et de fin du projet Si le projet est en cours, indiquer la date de clôture de la présente demande de proposition.	
Portée des services de ***cybersécurité*** fournis Description du travail entrepris et des services fournis, y compris la façon dont le travail répond aux critères.	

Remplir avec détails des ressources

PARTIE 2
Nº de référence du contrat : _____

F) Période de 6 mois consécutifs à évaluer	
Date de début	
Date de fin	

G) SECTION 1 : RENSEIGNEMENTS SUR LES RESSOURCES	
Ressource Nº 1 :	**Nom** :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 2 :	**Nom :**
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 3 :	**Nom :**
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	

Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 4 :	**Nom** :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 5 :	**Nom** :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	

Pour l'une des ressources inclus dans la partie 2 (G), si leurs titres de catégorie de ressources dans le contrat de référence ne sont pas identiques à ceux qui sont énumérés dans les critères, la partie 3 complètez pour établir l'équivalence de catégorie de ressource comme indiqué dans les critères de EO2.

Cartographie des activités et des tâches

Sélectionnez et remplissez la section appropriée pour la ou les catégories de ressources à cartographier.

PARTIE 3
Nº de référence du contrat : _____

Nº de l'autorisation de tâches : _____

Ressource : _____

C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.1 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
e) Réaliser des études de faisabilité, des évaluations des technologies ainsi que des analyses de rentabilité, en plus de proposer des plans de mise en œuvre des systèmes liés à la sécurité des TI	
h) Examiner et prioriser les programmes en matière de protection de l'infrastructure de l'information et de sécurité des TI.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend trois autres tâches connexes énumérées à la section 6.1 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	

Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.2 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
d) Rédiger des rapports, par exemple pour l'analyse de sécurité des données, les concepts d'opération, les énoncés de sensibilité, les évaluations de la menace, les évaluations des facteurs relatifs à la vie privée, les évaluations des vulnérabilités non techniques, les évaluations des risques et la présentation des menaces, vulnérabilités et risques liés à la sécurité des TI.	
f) Effectuer des activités liées à l'accréditation, notamment : l'examen, par l'accréditeur, des résultats de l'homologation indiqués dans les documents d'examen conceptuel, pour s'assurer que les risques entourant l'exploitation du système seront acceptables et que celui-ci sera en conformité avec les politiques et normes de sécurité pertinentes du Ministère et celles qui lui sont propres; et la détermination des conditions d'exploitation du système (aux fins d'approbation).	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.2 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.7 Spécialiste en conception de sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	

Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.3 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
e) Examiner, analyser ou appliquer l'importance et les conséquences des tendances du marché et de la technologie afin de les appliquer aux feuilles de route pour les architectures et la conception des solutions (p. ex. : sécurité des services Web, sécurité des interfaces API, gestion des incidents, gestion de l'identité).	
i) Assurer la conception d'architectures de sécurité et le soutien technique.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend quatre autres tâches connexes énumérées à la section 6.3 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.8 Analyste de la sécurité des réseaux	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.4 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
b) Analyser les données de sécurité et présenter des avis et des rapports	
f) Déceler et analyser les menaces techniques pesant sur les réseaux et leurs vulnérabilités.	

ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend quatre autres tâches connexes énumérées à la section 6.4 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.9. Opérateur de systèmes de sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.5 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
c) Configurer la gestion de la sécurité des TI.	
d) Configurer des systèmes de détection des intrusions, des coupe-feu et des vérificateurs de contenu, extraire et analyser des rapports et des journaux, et intervenir en cas d'incidents en matière de sécurité.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.5 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____ **Ressource : _____**

C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.6 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
a) Examiner, analyser ou appliquer: • les outils d'analyse des agents de menace et autres nouvelles technologies, notamment les outils de protection des renseignements personnels, l'analyse prédictive, les techniques VoIP, la visualisation et la fusion des données, les dispositifs de sécurité sans fil, les PBX et les coupe-feu pour téléphonie; • les détecteurs d'accès entrant, les perceurs de mots de passe; • les services consultatifs du domaine public sur les vulnérabilités des TI; • les analyseurs réseau et des outils d'analyse des vulnérabilités comme SATAN, ISS, Portscan et NMap; • les protocoles réseau (HTTP, FTP, Telnet); • les protocoles de sécurité Internet, comme TLS, HTTPS, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP et SNMP; • la sécurité des systèmes sans fil; • les systèmes de détection des intrusions, les coupe-feu et les vérificateurs de contenu; • les systèmes de détection et de prévention des intrusions dans les hôtes et les réseaux (gestion des antivirus).	
b) Déceler les menaces pesant sur les réseaux et leurs vulnérabilités techniques.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.6 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____ **Ressource : _____**	
C.14 Spécialiste de la R et D en sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.7 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche de l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
a) Examiner, analyser ou appliquer : • la capacité de recherche et développement sur la sécurité des TI dans l'industrie et les universités canadiennes; • les normes d'annuaire comme X.400, X.500 et SMTP; • les protocoles réseau comme HTTP, FTP et Telnet; • les protocoles de sécurité Internet (TLS, HTTPS, S MIME, IPSec, SSH); • les normes de sécurité des technologies sans fil et Bluetooth; • les protocoles et normes TCP/IP, UDP, DNS, SMTP et SNMP; • les systèmes de détection des intrusions, de coupe-feu et de vérificateurs de contenu; • les algorithmes cryptographiques; • les pratiques exemplaires de sécurité.	
c) Conceptualiser et élaborer des prototypes ainsi que des modèles et essais de validation de principe, y compris à l'égard de fonctionnalités et de technologies émergentes liées à la sécurité.	
<u>ET</u> Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.7 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____ **Ressource : _____**

C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.8 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche de l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
b) Réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) et des évaluations préliminaires des facteurs relatifs à la vie privée (EPFVP) des projets et des concepts, conformément aux exigences énoncées dans : • la Politique d'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor; • les lignes directrices du Conseil du Trésor sur l'EFVP; • d'autres normes, procédures et lignes directrices pertinentes.	
f) Élaborer des recommandations quant aux stratégies possibles d'atténuation des risques d'entrave à la vie privée.	
<u>ET</u> Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend deux autres tâches connexes énumérées à la section 6.8 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Documentation à l'appui

S'assurer d'inclure une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis.

Ce qui suit est suffisant :

1. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou
2. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou
3. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.

EXIGENCE ORGANISATIONNELLE COTÉE EC1

Le soumissionnaire obtiendra jusqu'à 20 points pour les contrats supplémentaires répondant à toutes les exigences de l'EO2.

Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère et il ne peut s'agir du contrat utilisé pour démontrer la conformité à l'exigence obligatoire EO2.

Dix (10) points pour chaque contrat admissible.

Note maximale : 20 points

Formulaire EC1 :

Copier et remplir les parties 1, 2 et 3 (le cas échéant) pour chaque contrat de référence admissible supplémentaire

PARTIE 1

A) Nº de référence du contrat ou de l'Autorisation de tâches : _____

B) Renseignements sur le client (*)

(*) La personne-ressource doit être une personne qui est ou était au moment du projet un employé de l'organisation cliente et qui peut confirmer tous les renseignements.

Nom de l'organisation	
Nom et titre de la personne-ressource	
Adresse	
Téléphone	
Adresse électronique	

C) Renseignements sur le contrat

Date de début	
Date de fin	

D) S'agit-il ou s'agissait-il d'un contrat des Services professionnels en informatique centrés sur les tâches (SPICT)? Oui ____ Non ____

E) Description du projet

Nom du projet	
Description du projet : tel que définie dans l'énoncé des travaux du contrat ou de l'autorisation de tâches	

Dates de début et de fin du projet Si le projet est en cours, indiquer la date de clôture de la présente demande de proposition.	
Portée des services de ***cybersécurité*** fournis Description du travail entrepris et des services fournis, y compris la façon dont le travail répond aux critères.	

Remplir avec détails des ressources

PARTIE 2
Nº de référence du contrat : _____

F) Période de 6 mois consécutifs à évaluer	
Date de début	
Date de fin	

G) SECTION 1 : RENSEIGNEMENTS SUR LES RESSOURCES	
Ressource Nº 1 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 2 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 3 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	

Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 4 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 5 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	

Pour l'une des ressources inclus dans la partie 2 (G), si leurs titres de catégorie de ressources dans le contrat de référence ne sont pas identiques à ceux qui sont énumérés dans les critères, la partie 3 complète pour établir l'équivalence de catégorie de ressource comme indiqué dans les critères de EO2.

Cartographie des activités et des tâches

Sélectionnez et remplissez la section appropriée pour la ou les catégories de ressources à cartographier.

PARTIE 3
Nº de référence du contrat : _____

Nº de l'autorisation de tâches : _____

Ressource : _____

C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.1 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
e) Réaliser des études de faisabilité, des évaluations des technologies ainsi que des analyses de rentabilité, en plus de proposer des plans de mise en œuvre des systèmes liés à la sécurité des TI	
h) Examiner et prioriser les programmes en matière de protection de l'infrastructure de l'information et de sécurité des TI.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend trois autres tâches connexes énumérées à la section 6.1 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	

Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.2 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
d) Rédiger des rapports, par exemple pour l'analyse de sécurité des données, les concepts d'opération, les énoncés de sensibilité, les évaluations de la menace, les évaluations des facteurs relatifs à la vie privée, les évaluations des vulnérabilités non techniques, les évaluations des risques et la présentation des menaces, vulnérabilités et risques liés à la sécurité des TI.	
f) Effectuer des activités liées à l'accréditation, notamment : l'examen, par l'accréditeur, des résultats de l'homologation indiqués dans les documents d'examen conceptuel, pour s'assurer que les risques entourant l'exploitation du système seront acceptables et que celui-ci sera en conformité avec les politiques et normes de sécurité pertinentes du Ministère et celles qui lui sont propres; et la détermination des conditions d'exploitation du système (aux fins d'approbation).	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.2 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.7 Spécialiste en conception de sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	

Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.3 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
e) Examiner, analyser ou appliquer l'importance et les conséquences des tendances du marché et de la technologie afin de les appliquer aux feuilles de route pour les architectures et la conception des solutions (p. ex. : sécurité des services Web, sécurité des interfaces API, gestion des incidents, gestion de l'identité).	
i) Assurer la conception d'architectures de sécurité et le soutien technique.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend quatre autres tâches connexes énumérées à la section 6.3 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.8 Analyste de la sécurité des réseaux	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.4 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
b) Analyser les données de sécurité et présenter des avis et des rapports	
f) Déceler et analyser les menaces techniques pesant sur les réseaux et leurs vulnérabilités.	

ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend quatre autres tâches connexes énumérées à la section 6.4 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.9. Opérateur de systèmes de sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.5 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
c) Configurer la gestion de la sécurité des TI.	
d) Configurer des systèmes de détection des intrusions, des coupe-feu et des vérificateurs de contenu, extraire et analyser des rapports et des journaux, et intervenir en cas d'incidents en matière de sécurité.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.5 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____ **Ressource : _____**	
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.6 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
a) Examiner, analyser ou appliquer: • les outils d'analyse des agents de menace et autres nouvelles technologies, notamment les outils de protection des renseignements personnels, l'analyse prédictive, les techniques VoIP, la visualisation et la fusion des données, les dispositifs de sécurité sans fil, les PBX et les coupe-feu pour téléphonie; • les détecteurs d'accès entrant, les perceurs de mots de passe; • les services consultatifs du domaine public sur les vulnérabilités des TI; • les analyseurs réseau et des outils d'analyse des vulnérabilités comme SATAN, ISS, Portscan et NMap; • les protocoles réseau (HTTP, FTP, Telnet); • les protocoles de sécurité Internet, comme TLS, HTTPS, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP et SNMP; • la sécurité des systèmes sans fil; • les systèmes de détection des intrusions, les coupe-feu et les vérificateurs de contenu; • les systèmes de détection et de prévention des intrusions dans les hôtes et les réseaux (gestion des antivirus).	
b) Déceler les menaces pesant sur les réseaux et leurs vulnérabilités techniques.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.6 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.14 Spécialiste de la R et D en sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.7 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche de l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
a) Examiner, analyser ou appliquer : • la capacité de recherche et développement sur la sécurité des TI dans l'industrie et les universités canadiennes; • les normes d'annuaire comme X.400, X.500 et SMTP; • les protocoles réseau comme HTTP, FTP et Telnet; • les protocoles de sécurité Internet (TLS, HTTPS, S MIME, IPSec, SSH); • les normes de sécurité des technologies sans fil et Bluetooth; • les protocoles et normes TCP/IP, UDP, DNS, SMTP et SNMP; • les systèmes de détection des intrusions, de coupe-feu et de vérificateurs de contenu; • les algorithmes cryptographiques; • les pratiques exemplaires de sécurité.	
c) Conceptualiser et élaborer des prototypes ainsi que des modèles et essais de validation de principe, y compris à l'égard de fonctionnalités et de technologies émergentes liées à la sécurité.	
<u>ET</u> Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.7 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____ **Ressource : _____**

C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.8 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche de l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
b) Réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) et des évaluations préliminaires des facteurs relatifs à la vie privée (EPFVP) des projets et des concepts, conformément aux exigences énoncées dans : • la Politique d'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor; • les lignes directrices du Conseil du Trésor sur l'EFVP; • d'autres normes, procédures et lignes directrices pertinentes.	
f) Élaborer des recommandations quant aux stratégies possibles d'atténuation des risques d'entrave à la vie privée.	
<u>ET</u> Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend deux autres tâches connexes énumérées à la section 6.8 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Documentation à l'appui

S'assurer d'inclure une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis.

Ce qui suit est suffisant :

1. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou
2. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou
3. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.

EXIGENCE ORGANISATIONNELLE COTÉE EC2

Le soumissionnaire obtiendra jusqu'à 25 points pour les ressources en ***cybersécurité*** simultanées en sus des cinq (5) ressources obligatoires dans le cadre du même contrat et pendant la même période de six mois consécutifs utilisés pour démontrer la conformité au critère obligatoire EO2.

Pour obtenir des points, toutes les conditions d'admissibilité indiquées à l'EO2 doivent être respectées par ces ressources additionnelles.

Pour montrer qu'il respecte ce critère, le soumissionnaire doit remplir et transmettre le **Formulaire EC2**.

Nombre de ressources travaillant simultanément pendant la période de six mois.
5 ressources = 0 point
6 ressources = 5 points
7 ressources = 10 points
8 ressources = 15 points
9 ressources = 20 points
10 ressources = 25 points

Note maximale : 25 points

Formulaire EC2 (3 Parties) :

PARTIE 1
A) Nº de référence du contrat ou de l'autorisation de tâches : _____

B) Description du projet	
Nom du projet	
Description du projet : tel que définie dans l'énoncé des travaux du contrat ou de l'autorisation de tâches	
Dates de début et de fin du projet Si le projet est en cours, indiquer la date de clôture de la présente demande de proposition.	
Portée des services de ***cybersécurité*** fournis Description du travail entrepris et des services fournis, y compris la façon dont le travail répond aux critères.	

Remplir avec détails des ressources

PARTIE 2

C) Période de 6 mois consécutifs à évaluer	
Date de début	
Date de fin	

D) SECTION 1 : RENSEIGNEMENTS SUR LES RESSOURCES	
Ressource Nº 6 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 7 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 8 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 9 :	Nom :
N ° d'autorisation de tâche	
Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	
Ressource Nº 10 :	Nom :
N ° d'autorisation de tâche	

Catégorie de ressources selon sa désignation dans le contrat de référence	
Catégorie de ressources selon sa désignation en EO2	
Nombre de jours facturables dans la période visée (minimum 90 jours)	

Pour l'une des ressources inclus dans la partie 2 (D), si leurs titres de catégorie de ressources dans le contrat de référence ne sont pas identiques à ceux qui sont énumérés dans les critères, la partie 3 complète pour établir l'équivalence de catégorie de ressource comme indiqué dans les critères de EO2.

Cartographie des activités et des tâches

Sélectionnez et remplissez la section appropriée pour la ou les catégories de ressources à cartographier.

PARTIE 3
Nº de référence du contrat : _____

Nº de l'autorisation de tâches : _____

Ressource : _____

C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.1 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
e) Réaliser des études de faisabilité, des évaluations des technologies ainsi que des analyses de rentabilité, en plus de proposer des plans de mise en œuvre des systèmes liés à la sécurité des TI	
h) Examiner et prioriser les programmes en matière de protection de l'infrastructure de l'information et de sécurité des TI.	

ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend trois autres tâches connexes énumérées à la section 6.1 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.2 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
d) Rédiger des rapports, par exemple pour l'analyse de sécurité des données, les concepts d'opération, les énoncés de sensibilité, les évaluations de la menace, les évaluations des facteurs relatifs à la vie privée, les évaluations des vulnérabilités non techniques, les évaluations des risques et la présentation des menaces, vulnérabilités et risques liés à la sécurité des TI.	
f) Effectuer des activités liées à l'accréditation, notamment : l'examen, par l'accréditeur, des résultats de l'homologation indiqués dans les documents d'examen conceptuel, pour s'assurer que les risques entourant l'exploitation du système seront acceptables et que celui-ci sera en conformité avec les politiques et normes de sécurité pertinentes du Ministère et celles qui lui sont propres; et la détermination des conditions d'exploitation du système (aux fins d'approbation).	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.2 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.7 Spécialiste en conception de sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.3 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
e) Examiner, analyser ou appliquer l'importance et les conséquences des tendances du marché et de la technologie afin de les appliquer aux feuilles de route pour les architectures et la conception des solutions (p. ex. : sécurité des services Web, sécurité des interfaces API, gestion des incidents, gestion de l'identité).	
i) Assurer la conception d'architectures de sécurité et le soutien technique.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend quatre autres tâches connexes énumérées à la section 6.3 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.8 Analyste de la sécurité des réseaux	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	

Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.4 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
b) Analyser les données de sécurité et présenter des avis et des rapports	
f) Déceler et analyser les menaces techniques pesant sur les réseaux et leurs vulnérabilités.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend quatre autres tâches connexes énumérées à la section 6.4 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.9. Opérateur de systèmes de sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.5 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
c) Configurer la gestion de la sécurité des TI.	
d) Configurer des systèmes de détection des intrusions, des coupe-feu et des vérificateurs de contenu, extraire et analyser des rapports et des journaux, et intervenir en cas d'incidents en matière de sécurité.	

ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.5 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	

Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.6 de l'annexe A, Énoncé des travaux :

La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.

Activité/tâche décrite à l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
a) Examiner, analyser ou appliquer: • les outils d'analyse des agents de menace et autres nouvelles technologies, notamment les outils de protection des renseignements personnels, l'analyse prédictive, les techniques VoIP, la visualisation et la fusion des données, les dispositifs de sécurité sans fil, les PBX et les coupe-feu pour téléphonie; • les détecteurs d'accès entrant, les perceurs de mots de passe; • les services consultatifs du domaine public sur les vulnérabilités des TI; • les analyseurs réseau et des outils d'analyse des vulnérabilités comme SATAN, ISS, Portscan et NMap; • les protocoles réseau (HTTP, FTP, Telnet); • les protocoles de sécurité Internet, comme TLS, HTTPS, S-MIME, IPSec, SSH, TCP/IP, UDP, DNS, SMTP et SNMP; • la sécurité des systèmes sans fil; • les systèmes de détection des intrusions, les coupe-feu et les vérificateurs de contenu; • les systèmes de détection et de prévention des intrusions dans les hôtes et les réseaux (gestion des antivirus).	
b) Déceler les menaces pesant sur les réseaux et leurs vulnérabilités techniques.	

ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.6 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____

Ressource : _____

C.14 Spécialiste de la R et D en sécurité des technologies de l'information	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.7 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche de l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
a) Examiner, analyser ou appliquer : • la capacité de recherche et développement sur la sécurité des TI dans l'industrie et les universités canadiennes; • les normes d'annuaire comme X.400, X.500 et SMTP; • les protocoles réseau comme HTTP, FTP et Telnet; • les protocoles de sécurité Internet (TLS, HTTPS, S MIME, IPSec, SSH); • les normes de sécurité des technologies sans fil et Bluetooth; • les protocoles et normes TCP/IP, UDP, DNS, SMTP et SNMP; • les systèmes de détection des intrusions, de coupe-feu et de vérificateurs de contenu; • les algorithmes cryptographiques; • les pratiques exemplaires de sécurité.	
c) Conceptualiser et élaborer des prototypes ainsi que des modèles et essais de validation de principe, y compris à l'égard de fonctionnalités et de technologies émergentes liées à la sécurité.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend une autre tâche connexe énumérée à la section 6.7 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Nº de l'autorisation de tâches : _____ **Ressource : _____**	
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	
Catégorie de ressources équivalente selon sa désignation dans le contrat de référence à cartographier	
Le soumissionnaire doit fournir une justification selon laquelle les travaux effectués comprennent les tâches connexes suivantes énumérées à la section 6.8 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	
Activité/tâche de l'annexe A : Énoncé des travaux pour la catégorie de ressources de l'exigence EO2	**Tâche exécutée dans le cadre du contrat de référence, y compris la justification**
b) Réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) et des évaluations préliminaires des facteurs relatifs à la vie privée (EPFVP) des projets et des concepts, conformément aux exigences énoncées dans : • la Politique d'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor; • les lignes directrices du Conseil du Trésor sur l'EFVP; • d'autres normes, procédures et lignes directrices pertinentes.	
f) Élaborer des recommandations quant aux stratégies possibles d'atténuation des risques d'entrave à la vie privée.	
ET Le soumissionnaire doit fournir une justification selon laquelle le travail effectué comprend deux autres tâches connexes énumérées à la section 6.8 de l'annexe A, Énoncé des travaux : **La justification ne doit pas être une simple répétition des tâches; elle doit expliquer les responsabilités et démontrer la façon dont le soumissionnaire a effectué les travaux dans le cadre de ses tâches.**	

Documentation à l'appui

S'assurer d'inclure une copie du contrat ou de l'autorisation de tâches pour justifier les détails fournis.

Ce qui suit est suffisant :

1. le contrat, y compris l'énoncé des travaux, excluant les annexes, pièces jointes, formulaires et autres appendices qui ne sont pas nécessaires pour étayer les renseignements fournis; ou
2. le contrat, y compris l'énoncé des travaux comme susmentionné au point 1, avec les renseignements confidentiels caviardés, pourvu que l'on conserve l'information appropriée pour étayer les renseignements démontrant la conformité au critère; ou
3. la signature du client, électronique ou manuscrite (à l'échelon du directeur ou un échelon supérieur), y compris le nom, le titre et les coordonnées, figurant sur le formulaire connexe validant tous les renseignements fournis dans le formulaire. Les renseignements indiqués doivent démontrer parfaitement le respect du critère.

EXIGENCE ORGANISATIONNELLE COTÉE EC3

Le soumissionnaire obtiendra jusqu'à 15 points pour le nombre de catégories de ressources utilisées pour démontrer la conformité au critère obligatoire EO2 et aux exigences cotées EC1 et EC2.

Les catégories de ressources doivent provenir de la liste fournie à l'EO2.

Le nombre de catégories de ressources utilisées pour démontrer la conformité à l'EO2, à l'EC1 et à l'EC2 :

1 catégorie = 2 points
2 catégories = 5 points
3 catégories = 8 points
4 catégories = 11 points
5 catégories = 13 points
6 catégories et + = 15 points

Note maximale : 15 points

Formulaire EC3 :

Catégorie de ressource	No de référence du contrat / de l'autorisation de tâches	Référence des critères
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information/Spécialiste en gestion du risque		
C.3 Analyste de la C et A et des évaluations de la menace et des risques en sécurité des technologies de l'information		
C.7 Spécialiste en conception de sécurité des technologies de l'information		
C.8 Analyste de la sécurité des réseaux		
C.9 Opérateur de systèmes de sécurité des technologies de l'information		
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information		
C.14 Spécialiste de la R et D en sécurité des technologies de l'information		
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée		
# catégories de ressources utilisées		

EXIGENCE ORGANISATIONNELLE COTÉE EC4

Le soumissionnaire obtiendra jusqu'à 10 points si le client de l'un des contrats admissibles utilisés pour démontrer la conformité aux exigences organisationnelles obligatoires EO1, EO2 ou à l'EC1 est le gouvernement du Canada(*).

(*) Le gouvernement du Canada est défini comme tout ministère, organisme ou société d'État du gouvernement du Canada.

Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère.

Contrat(s) du gouvernement du Canada utilisé(s) pour l'EO1 et l'EO2 ou l'EC1.
1 ou 2 = 5 points
3 et + = 10 points

Note maximale : 10 points

Formulaire EC4 :

	Numéro(s) de référence du (des) contrat(s) utilisé(s) pour l'EO1, l'EO2 ou l'EC1	**Organisme client du gouvernement du Canada**
1		
2		
3		

EXIGENCE ORGANISATIONNELLE COTÉE EC5

Le soumissionnaire (*) obtiendra jusqu'à 20 points si l'un des services de cybersécurité fournis dans le cadre des contrats admissibles utilisés pour démontrer la conformité aux exigences organisationnelles obligatoires EO1, EO2 ou l'EC1 est lié à une technologie émergente(*).

Remarque : Pour être admissible, la technologie émergente doit être explicitement identifiée dans l'énoncé des travaux du contrat ou de l'autorisation de tâches.

Un contrat ne peut être compté qu'une seule fois pour l'évaluation de ce critère.

Dix (10) points sont accordés pour chaque contrat utilisé pour démontrer la conformité à l'EO1, l'EO2 ou l'EC1 et lié à une technologie émergente décrite dans les critères.

Note maximale : 20 points

(*) Dans l'évaluation de l'expérience de l'entreprise pour ce critere, le gouvernement du Canada tiendra compte de l'expérience de l'entreprise décrite par le soumissionnaire tel que défini dans :

Partie 3, Section 3.2
Section i ; Soumission Technique
Justification de la conformité technique
Paragraphe C (page 17)

Formulaire EC5 :

Numéro de référence du contrat utilisé pour l'EO1, l'EO2 ou l'EC1	
Explication de la raison pour laquelle ce contrat répond à l'exigence :	

Numéro de référence du contrat utilisé pour l'EO1, l'EO2 ou l'EC1	
Explication de la raison pour laquelle ce contrat répond à l'exigence :	

PIÈCE JOINTE 4.4
BARÈME DE PRIX

Le soumissionnaire doit compléter ce barème de prix et l'inclure dans sa soumission financière.

Les données volumétriques comprises dans ce barème de prix sont fournies uniquement aux fins de la détermination du prix évalué de chaque soumission. Elles ne doivent pas être considérées comme une garantie contractuelle. Leur inclusion dans ce barème de prix ne représente pas un engagement de la part du Canada que son utilisation future des services décrits dans la demande de soumissions correspondra à ces données.

TABLE DE BAREME DE PRIX

		Periode de contrat (1) Date de l'attribution du contrat pour 1 an			Periode du contrat (2) Option 1 : Debute a la fin de la periode 1 pour 1 an			Periode du Contrat (3) Option 2 : Débute a la fin de Periode 2 pour 1 an		
		A	B	C = A*B	D	E	F = D * E	G	H	I = G * H
Catégorie de ressources	**Niveau**	**Nombre estimatif de jours**	**Taux quotidien ferme** *(taux du soumissionnaire)*	**Cout Total Periode de contrat (1)**	**Nombre estimatif de jours**	**Taux quotidien ferme** *(taux du soumissionnaire)*	**Cout Total Periode de contrat (2)**	**Nombre estimatif de jours**	**Taux quotidien ferme** *(taux du soumissionnaire)*	**Cout Total Periode de contrat (3)**
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	2	240			240			60		
C.1 Consultant en protection et en planification stratégique de la sécurité des technologies de l'information / Spécialiste en gestion du risque	3	240			240			60		
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	2	240			240			108		
C.3. Analyste de la certification et accréditation et des évaluation de la menace et des risques en sécurité des technologies de l'information	3	360			360			108		
C.7 Spécialiste en conception de sécurité des technologies de l'information	2	480			480			240		
C.7 Spécialiste en conception de sécurité des technologies de l'information	3	480			480			240		
C.8 Analyste de la sécurité des réseaux	2	480			240			240		
C.8 Analyste de la sécurité des réseaux	3	240			240			240		
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	2	480			480			480		
C.9. Opérateur de systèmes de sécurité des technologies de l'information / Vérificateur de systèmes	3	240			240			240		
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	2	240			240			120		
C.11 Spécialiste des analyses de vulnérabilité de la sécurité des technologies de l'information	3	240			240			120		
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	2	720			720			720		
C.14. Spécialiste de la recherche et développement en sécurité des technologies de l'information	3	720			720			720		
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	2	120			120			60		
C.16 Spécialiste des évaluations des facteurs relatifs à la vie privée	3	120			120			60		
COUT TOTAL POUR INFORMATION SEULEMENT Voir Partie 4, section 4.3 a)		**COUT TOTAL Periode de contrat 1**			**COUT TOTAL Periode de contrat 2**			**COUT TOTAL Periode de contrat 2**		
		COUT TOTAL = Periode de Contrat 1 + Periode de Contract 2 + Periode de contrat 3								

PIÈCE JOINTE 5.1
PROGRAMME DE CONTRATS FÉDÉRAUX POUR L'ÉQUITÉ EN MATIÈRE D'EMPLOI – ATTESTATION

Je, le 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 se réserve le droit d'exiger des renseignements supplémentaires pour vérifier les attestations du soumissionnaire. Le non-respect de toute demande ou exigence imposée par le Canada peut rendre la soumission irrecevable ou constituer un manquement au contrat.

Pour obtenir de plus amples renseignements sur le Programme de contrats fédéraux pour l'équité en matière d'emploi, consulter le site Web du Programme du travail d'Emploi et Développement social Canada.

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

Répondre aux questions A et B.

A. Cocher une seule case :

( ) 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 régi par le gouvernement fédéral assujetti à 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 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 œuvre de l'équité en matière d'emploi valide avec le Programme du travail d'Emploi et Développement social Canada et que cet accord est en vigueur.

OU

( ) A5.2 Le soumissionnaire atteste qu'il a présenté le formulaire « Accord pour la mise en œuvre de l'équité en matière d'emploi » (LAB1168) au Programme du travail d'Emploi et développement social Canada. Comme il s'agit d'une condition d'attribution du contrat, l'entrepreneur doit remplir le formulaire « Accord pour la mise en œuvre de l'équité en matière d'emploi » (LAB1168), le signer en bonne et due forme et le transmettre au Programme du travail d'Emploi et Développement social Canada.

B. Cocher une seule case :

( ) B1. Le soumissionnaire ne fait pas partie d'une coentreprise.

OU

( ) B2. Le soumissionnaire fait partie d'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 » remplie. (Voir la section sur les coentreprises des instructions uniformisées.)